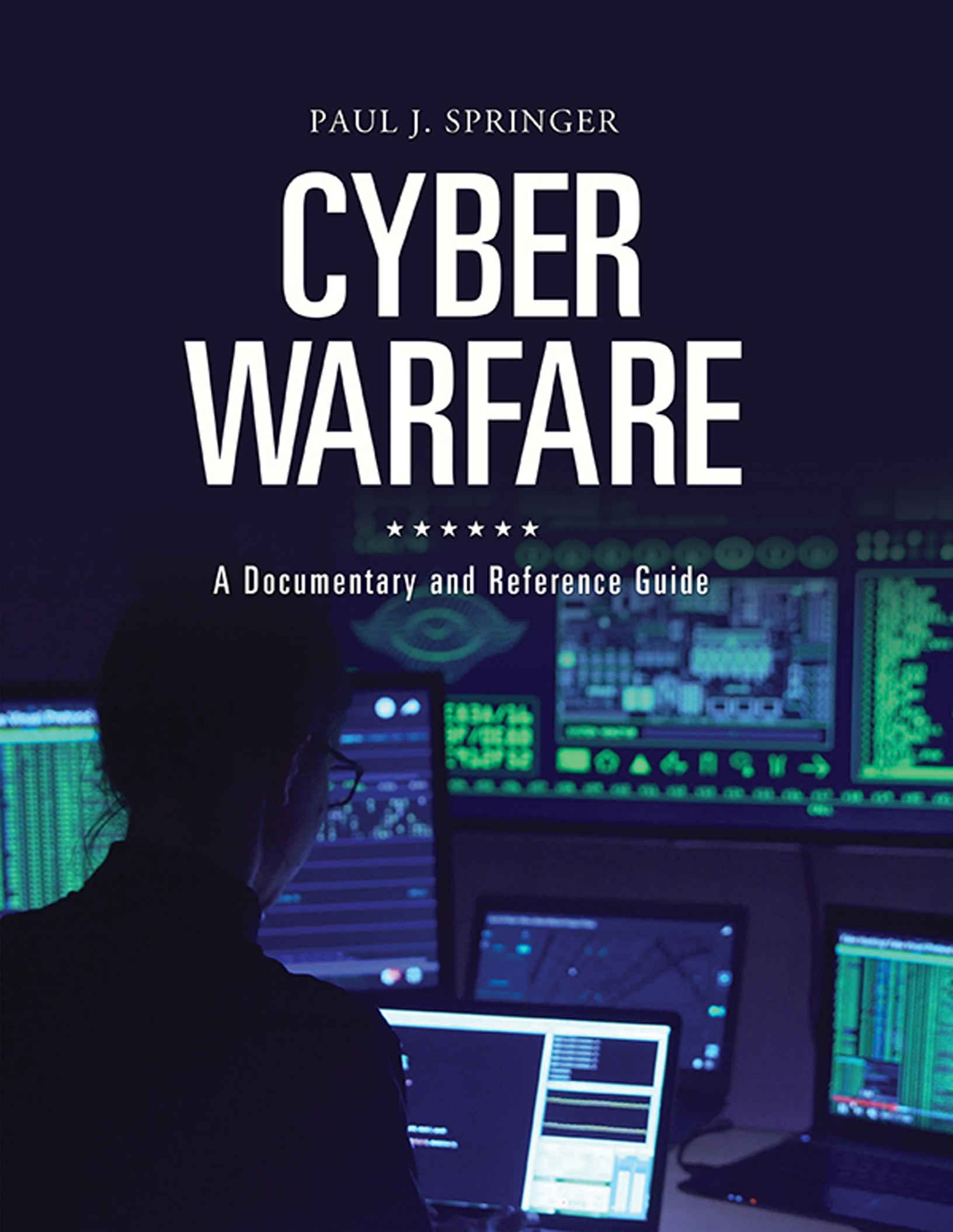
PAUL J. SPRINGER

CYBER WARFARE

★★★★★★

A Documentary and Reference Guide



CYBER WARFARE

Recent Titles in
Documentary and Reference Guides

The Politics of Sexuality: A Documentary and Reference Guide
Raymond A. Smith

U.S. Election Campaigns: A Documentary and Reference Guide
Thomas J. Baldino and Kyle L. Kreider

U.S. Foreign Policy: A Documentary and Reference Guide
Akis Kalaitzidis and Gregory W. Streich

White-Collar and Corporate Crime: A Documentary and Reference Guide
Gilbert Geis

Homelessness: A Documentary and Reference Guide
Neil Larry Shumsky

Victims' Rights: A Documentary and Reference Guide
Douglas E. Beloof

Substance Abuse in America: A Documentary and Reference Guide
James A. Swartz

The Iraq War: A Documentary and Reference Guide
Thomas R. Mockaitis

Animal Rights and Welfare: A Documentary and Reference Guide
Lawrence W. Baker

Water Rights and the Environment in the United States: A Documentary and Reference Guide
John R. Burch Jr.

Endangered Species: A Documentary and Reference Guide
Edward P. Weber

9/11 and the War on Terror: A Documentary and Reference Guide
Paul J. Springer

Vaccination and Its Critics: A Documentary and Reference Guide
Lisa Rosner

Arab-Israeli Conflict: A Documentary and Reference Guide
Priscilla Roberts

Modern Slavery: A Documentary and Reference Guide
Laura J. Lederer

Poverty in the United States: A Documentary and Reference Guide
John R. Burch Jr.

Afghanistan War: A Documentary and Reference Guide
Ryan Wadle

Modern Genocide: A Documentary and Reference Guide
Paul R. Bartrop

CYBER WARFARE

A Documentary and Reference Guide

Paul J. Springer

Documentary and Reference Guides

GREENWOOD™
An Imprint of ABC-CLIO, LLC
Santa Barbara, California • Denver, Colorado

Library of Congress Cataloging-in-Publication Data

Names: Springer, Paul J., author.
Title: Cyber warfare : a documentary and reference guide / Paul J. Springer.
Description: Santa Barbara, California : Greenwood, an imprint of ABC-CLIO, [2020] | Series: Documentary and Reference Guides | Includes bibliographical references and index.
Identifiers: LCCN 2019059457 (print) | LCCN 2019059458 (ebook) | ISBN 9781440872785 (hardcover) | ISBN 9781440872792 (ebook)
Subjects: LCSH: Cyberspace operations (Military science)—United States. | Cyberspace—Government policy—United States—Sources. | Information warfare—United States.
Classification: LCC U167.5.C92 S67 2020 (print) | LCC U167.5.C92 (ebook) | DDC 355.4—dc23
LC record available at https://lccn.loc.gov/2019059457
LC ebook record available at https://lccn.loc.gov/2019059458

ISBN: 978-1-4408-7278-5 (print)
978-1-4408-7279-2 (ebook)

24 23 22 21 20 1 2 3 4 5

This book is also available as an eBook.

Greenwood
An Imprint of ABC-CLIO, LLC

ABC-CLIO, LLC
147 Castilian Drive
Santa Barbara, California 93117
www.abc-clio.com

This book is printed on acid-free paper ♾

Manufactured in the United States of America

CONTENTS

READER'S GUIDE TO RELATED DOCUMENTS

U.S. National Security Strategies

Document 1: *National Security Strategy of the United States* (1987)

Document 5: *A National Security Strategy for a New Century* (1999)

Document 12: *National Security Strategy* (2010)

Document 17: *National Security Strategy* (2015)

Document 20: *National Security Strategy of the United States of America* (2017)

U.S. National Military Strategies

Document 2: *National Military Strategy of the United States of America: A Strategy of Flexible and Selective Engagement* (1995)

Document 3: *National Military Strategy of the United States of America: Shape, Respond, and Prepare Now: A Military Strategy for a New Era* (1997)

Document 8: *The National Military Strategy of the United States of America: A Strategy for Today; a Vision for Tomorrow* (2004)

Document 14: *The National Military Strategy of the United States of America: Redefining America's Military Leadership* (2011)

Document 18: *The National Military Strategy of the United States of America: The United States Military's Contribution to National Security* (2015)

U.S. Quadrennial Defense Reviews

Document 4: *Quadrennial Defense Review* (1997)

Document 6: *Quadrennial Defense Review Report* (2001)

Document 10: *Quadrennial Defense Review Report* (2006)

Document 13: *Quadrennial Defense Review Report* (2010)

Document 16: *Quadrennial Defense Review* (2014)

U.S. National Cyber Strategies

Document 7: *The National Strategy to Secure Cyberspace* (2003)

Document 15: *International Strategy for Cyberspace* (2011)

Document 19: *The Department of Defense Cyber Strategy* (2015)

Document 22: *National Cyber Strategy of the United States* (2018)

Document 23: *Summary, Department of Defense Cyber Strategy* (2018)

U.S. National Defense Strategies

Document 9: *The National Defense Strategy of the United States of America* (2005)

Document 11: *National Defense Strategy* (2008)

Document 21: *Summary of the 2018 National Defense Strategy of the United States of America* (2018)

Documents Pertaining to the Peoples' Republic of China

Document 24: *Military Power of the People's Republic of China* (2009)

Document 25: *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (2009)

Document 26: *Mandiant APT1 Report: Exposing One of China's Cyber Espionage Units* (2013)

Document 28: *China and International Law in Cyberspace* (2014)

Document 29: *Military and Security Developments Involving the People's Republic of China* (2014)

Document 30: *Cybersecurity Law of the People's Republic of China* (2016)

Document 35: *China Military Power* (2019)

Document 45: *U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage* (2014)

Document 58: *Unrestricted Warfare* (1999)

Document 68: *People's Republic of China National Cyberspace Security Strategy* (2016)

Documents Pertaining to the Democratic Peoples' Republic of Korea

Document 27: *Military and Security Developments Involving the Democratic People's Republic of Korea* (2013)

Document 34: *Military and Security Developments Involving the Democratic People's Republic of Korea* (2017)

Document 47: *Executive Order 13687—Imposing Additional Sanctions with Respect to North Korea* (2015)

Documents Pertaining to the Russian Federation

Document 31: *Grizzly Steppe—Russian Malicious Cyber Activity* (2016)

Document 32: *Assessing Russian Activities and Intentions in Recent U.S. Elections* (2017)

Document 33: *Russia Military Power* (2017)

Document 69: *Developments in the Field of Information and Communications Technology in the Context of International Security* (2018)

Executive Documents from the Office of the President of the United States

Document 36: *Presidential Decision Directive/NSC-63* (1998)

Document 38: *The Comprehensive National Cybersecurity Initiative* (2009)

Document 40: *Executive Order 13636—Improving Critical Infrastructure Cybersecurity* (2013)

Document 42: *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience* (2013)

Document 43: *Presidential Policy Directive 21—Critical Infrastructure Security and Resilience* (2013)

Document 48: *Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing* (2015)

Document 51: *Presidential Policy Directive 41: United States Cyber Incident Coordination* (2016)

Document 52: *Executive Order 13800—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (2017)

U.S. Congressional Investigations and Testimony

Document 37: *Cyber Threat Source Descriptions* (2005)

Document 49: *Cyberwarfare and Cyberterrorism: In Brief* (2015)

Document 53: *Information Warfare: Issues for Congress* (2018)

Document 54: *Cybersecurity: Selected Issues for the 115th Congress* (2018)

Document 73: *Statement for the Record of Seán P. McGurk before the U.S. Senate Homeland Security and Governmental Affairs Committee* (2010)

Document 76: *Statement of General Keith B. Alexander before the Senate Committee on Armed Services* (2013)

Document 78: *Michael Rogers, "Testimony before the U.S. House Intelligence Committee"* (2014)

Document 80: *Advance Policy Questions for the Honorable Ashton Carter* (2015)

Document 82: *James Clapper, Testimony before the U.S. Senate Committee on Armed Services* (2015)

Documents Created by U.S. Government Agencies

Document 39: *Resilient Military Systems and the Advanced Cyber Threat* (2013)

Document 41: *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented* (2013)

Document 44: *Deterrence in the Age of Surprise* (2014)

Document 56: *Developments in the Field of Information and Communications Technology in the Context of International Security* (2018)

U.S. Department of Defense Joint Publications and Doctrine

Document 46: *Joint Publication 3-13: Information Operations* (2014)

INTRODUCTION

For as long as humans have organized themselves into societies, there have been conflicts between those societies. The largest and most violent conflicts are collectively termed "wars," and most theorists and philosophers of human interaction consider war to be an inherent part of the human condition. Wars are propagated by individuals, but they are organized and conducted by governments, using all the means at their disposal. As new innovations occur, they are often adapted for military conflict. The development of computer networks and the internet are no exception to this phenomenon. Although to date no humans have been killed as a direct result of cyberattacks, operations throughout the cyber domain have still caused and enabled enormous devastation in the past two decades.

The cyber domain is unique in that it is the first human-made domain through which nations may engage in violence against one another. It has also been utilized to enable crime, espionage, sabotage, and terrorism, all of which are often grouped under the term "cyber warfare." The terminology of warfare has been adapted to fit the digital realm, often by simply adding "cyber" as a prefix to an existing term. Thus, "cybersecurity," "cyberterrorism," and "cyberwar" have all entered the lexicon of human conflict. In general, the same operations that might be launched in the physical domain have their corresponding possibilities in the cyber domain. Thus, the development of economic opportunities through the internet has also enabled the expansion of cybercrime, vastly increasing the amount that skilled thieves might pilfer in a short period of time. The creation of ways to store and secure large volumes of information has triggered a spate of cyberespionage, as hostile states, organizations, and individuals seek to access materials through cyberespionage, despite the efforts of the owners to keep access strictly controlled. The internet has enabled a much greater interconnectivity of devices, including aspects of critical infrastructure, making systems much more effective and efficient. Yet, this networking of physical items has also created an opportunity for cybersabotage, as hostile computer users attempt to hijack and destroy the same systems. Military recruitment and propaganda distribution have both been enabled by computer networks—but so has the recruitment of individuals to join terror organizations.

In short, the development of cyber capabilities has not fundamentally altered the nature of human conflicts, although it has certainly had a substantial impact upon the character of those conflicts. As interconnectivity and computer capabilities continue to advance, so will efforts to utilize those developments for malicious purposes, forcing users to devote increasing resources and efforts to protecting the new systems they come to rely upon. Yet, refusing to accept the cyber revolution will not protect individuals from its effects—rather, those who do not adapt to the changing landscape of human conflict are likely to simply be swept up in the aftereffects, with little opportunity to influence the direction of the social changes brought about by the development of cyber technology.

This work is divided into five parts, based upon the type and source of the documents. Within each section, the documents are presented in chronological order, facilitating efforts to follow the developments of cyber capabilities over time. The first chapter provides the underpinning strategic documents of the United States. Most of the early developments of computer technology, to include the creation of digital protocols to link computers into networks, originated in the United States. Not surprisingly, many of the precedents for cyber operations have also been derived from U.S. behaviors in cyberspace. Reading through the strategic documents that guide the nation's approach to conflict, one can see the growing importance of computer networks and cyber warfare in the United States. The United States has a greater dependence upon cyber capabilities, and a greater capacity to utilize the cyber domain, than any other nation-state—but with that dependence comes a host of vulnerabilities.

Part 2 examines the nations that the United States perceives as adversaries in the cyber domain. It consists of U.S.-created evaluations of those nations' efforts in cyberspace, as well as evaluations of their activities and future capabilities. Part 3 supplies policy documents, military doctrine, and official reports related to cyberwar, as created by members of the U.S. military and other government agencies. Part 4 offers examples of foreign cyber strategies, devised by friends and foes, as well as nongovernmental bodies that have developed the international standing to offer major opinions upon behaviors, conflicts, and norms within cyberspace. Part 5 is a collection of speeches, testimony, and transcripts by prominent individuals who have shaped the global perception of how cyber power has been developed and used.

Readers should adopt a critical stance when considering each of the documents in this collection, regardless of source. Every nation that chooses to publish its position on cyber affairs and then place it in the public sphere does so as part of an effort to shape the future of cyberspace. Likewise, prominent political and military leaders offering their opinions on cyber activities do so with the full knowledge that the precedents for cyber activity are only beginning to create regular modes of behavior in the digital domain. As such, readers should consider the bias of the creators of documents, as well as their underlying purpose for developing and propagating these items.

No project of this magnitude is ever created in a vacuum, and the most important contributions to its success are often made by individuals working behind the scenes to ensure its completion. In particular, the personnel at ABC-CLIO deserve special recognition for their efforts to create and support this work. Padraic (Pat) Carlin is

an outstanding editor and an absolute delight to work with as an author. Robin Tutt is one of the best in the business at editorial operations and obtaining permissions to use materials included in this book. Bridget Austiguy-Preschel and Angel Daphnee were absolutely essential in bringing this project to fruition.

I am proud to serve as a faculty member at the Air Command and Staff College, where I have the opportunity to work with extremely dedicated and talented professionals every day. Our mission is to educate the leaders of tomorrow's joint force, encompassing the military services, civilian agencies, and partner nations. It is to the faculty, staff, and students of the Air Command and Staff College that I gratefully dedicate this volume.

1

U.S. CYBER STRATEGY DOCUMENTS

- ***Document 1:*** *National Security Strategy of the United States*
- ***When:*** 1987
- ***Where:*** Washington, D.C.
- ***Significance:*** The National Security Strategy is the overarching document that lays out an administration's broad approaches to maintaining the territorial integrity and safety of the United States. Each time such a strategy is released, it offers guidance for the formulation of a national defense strategy, a national military strategy, and the like. In 1987, the United States had been locked in a Cold War with the Soviet Union for more than four decades—and at the time, no end to the conflict was in sight. In this document, President Ronald Reagan established his priorities for U.S. national security.

DOCUMENT

Political and Informational Elements of National Power

We are faced with a profound challenge to our national security in the political field. This challenge is to fight the war of ideas and to help support the political infrastructure of world democracies. To accomplish this we must be as committed to the maintenance of our political defense as we are to our military defense.

Public opinion polls consistently find that two-thirds of the American electorate normally take no interest in foreign policy. Moreover, only a bare majority today believes that this country needs to play an active part in world affairs—and that majority is eroding. There is no natural domestic constituency for foreign policy—*we must build one*.

The instruments to implement such an approach include a number of traditional foreign policy agencies such as the Departments of State and Defense, Agency for International Development (AID), and U.S. Information Agency (USIA), plus several less traditional participants including the Departments of Commerce and Treasury and the U.S. Trade Representative (USTR).

Another actor in the field of political, informational and communications activity is the private sector. During the past six years, the private sector has been energized as a key element in the projection of U.S. foreign policy goals. Leading private citizens and groups are taking steps to identify and organize the many local forces throughout the United States that have a direct stake in the nation's relations with the rest of the world. The private voluntary organizations in world affairs are doing an indispensable job of public education. They have our strongest encouragement and support.

While we focus on the needs of an effective political and informational policy, we must keep in mind that the Soviet Union has a most aggressive public deception and propaganda program, using a wide range of techniques aimed not only at the Third World, but also at our alliance partners. The current Soviet regime has increased the range and intensity of Soviet public diplomacy and propaganda efforts. We must actively counter Soviet propaganda and active measures using the full range of U.S. informational programs.

Our political and informational strategy must also reach to the peoples of denied areas, particularly the USSR and Eastern Europe—to encourage hope for change and to educate publics on the benefits of free institutions. This is achieved through the electronic media, written materials, and the increased contact and exchange of ideas that come from such contact. The process of gradual change will take place inside, but the stimulant and the vision of "how things could be" must come from outside in a closed society. This is the vision of a nation which believes that a world of democracies is a safer world, and one where the respect for the dignity of all men has a better chance to be realized.

. . .

Taking Advantage of U.S. Strengths and Soviet Weaknesses

One of the central tenets of our defense policy is that the United States will not seek to match the Soviet Union weapon for weapon. Rather, we will work to overcome Soviet numerical superiority by taking maximum advantage of the inherent strengths of alliances composed of democratic, industrialized, free economy nations.

Technology. The United States and its allies continue to enjoy technological superiority over the Soviet Bloc in most areas of military application. This technological advantage derives from the fundamental nature of the two societies. The spirit of inquiry and the free flow of information which characterize the West will inevitably permit technology and innovation to flourish to a greater degree than it will in a closed society. The United States and its allies enjoy an intrinsic advantage not only in the creation, but in the practical exploitation of advanced technologies. Competitive, free-enterprise societies consistently out-perform centrally planned economies in fostering innovation, growth, and the application of new technology to a wide variety of fields.

Technology affects our national security in two ways. First, the ability to exploit and adapt technology contributes to the overall economic health of the United States and its allies, which is a key element of national power. Second, the exploitation of a technological advantage directly enhances defense. Precision guided munitions, for example, help offset the large Soviet edge in tank forces. Stealth technology helps counter the massive Soviet investment in air defense. Advances in

DID YOU KNOW?

Strategy and Doctrine

"Strategy" is the art of setting larger and long-term goals for an organization. In a military sense, it is largely the purview of general officers and senior political leaders as it involves determining the most effective and/or efficient means of securing a nation's foreign policy interests through the use or threat of force. Strategy requires not only the creation of goals and expectations but also the provision of personnel and resources. "Doctrine" refers to the sum knowledge of one or more military operations, and serves to standardize military behavior by essentially providing the underpinning information necessary for the execution of strategy. Military organizations issue doctrine as a means to disseminate a common understanding of difficult problems such as the conduct of cyber operations.

anti-submarine warfare technologies and in submarine quieting help preserve maritime superiority despite the Soviet Navy's numerical advantages. Perhaps most significantly, the U.S. edge in computer technology and software has military relevance across the entire spectrum of warfare.

The Soviets are, of course, conscious of the Western technological advantage and have undertaken a massive effort to acquire and exploit Western technology. Thus a vital element of our defense policy is to control technology transfer and protect classified information relating to military technologies. With this in mind, we have undertaken a major effort to enhance our National Counter-intelligence and Security Countermeasures plans and capabilities, as I outlined in my November 1986 report to Congress.

Competitive Strategies. Competitive strategies are aimed at exploiting our technological advantages in thoughtful and systematic ways to cause the Soviets to compete less efficiently or less effectively in areas of military application. Such strategies seek to make portions of the tremendous Soviet military machine obsolete and force the Soviets to divert resources in ways they may not prefer, and in a manner that may not necessarily threaten our own forces. Low observable (stealth) technology, for example, can render much of the Soviet investment in air defense obsolete and requires the Soviets to divert resources from offensive forces to defensive forces. The contribution which new technologies can make to our competitive strategies is an explicit consideration in making defense procurement decisions.

Alliances. A third area of U.S. strength and Soviet weakness is alliance relationships. While the Soviet Union presides over an empire that has seen several armed rebellions in the past forty years, the United States is the leader of a voluntary coalition of equal nations. U.S. allies, particularly our NATO partners, contribute a major share of the West's total military strength. Recognizing this contribution, our defense policy is based on the fundamental premise that we will not seek to offset Soviet power alone, but in conjunction with our allies throughout the globe, on a basis of equitable burdensharing.

In NATO, this means continuing our strong support for Alliance efforts to improve the overall Western conventional balance, including appropriate economic and military assistance to allies on NATO's critical southern flank. It means integrating the contribution of our NATO partners into our strategy—indeed, the United States has no separate military strategy for the defense of Europe, but is a partner in the NATO alliance strategy of deterrence and defense. Outside of Europe, the United States seeks strong ties with nations throughout the globe, assisting friendly and allied countries in improving their military capabilities while encouraging them to assume a greater role in their own defense.

The Strength of the Individual. One of our greatest advantages in competing with the Soviet Union is the character of our people. Western societies, with their stress on the importance of the individual, stand in sharp contrast to the repressive nature of the Soviet state. The initiative, enterprise, and motivation of free people is a source of great strength when individuals are put to the supreme test of combat. While intangible, these qualities are an important asset, which the Soviets cannot match. Defense policy recognizes this by stressing unit integrity and leadership,

while our training and tactics place great value on individual initiative, and aggressive exploitation of opportunities.

SOURCE: White House, *The National Security Strategy of the United States* (Washington, D.C.: Government Printing Office, 1987), 13, 20–21, http://nssarchive.us/NSSR/1987.pdf

ANALYSIS

Although the term "cyber" does not appear in this document, many of the fundamental concepts that underpin cyberwarfare in the twenty-first century are evident in its pages.

Although the 1987 iteration of the U.S. National Security Strategy made only tangential mention of information assets, command and control, and the role of computing technology in future conflicts, it had many hints of the future development of cyber weapons and their utilization, both by the United States and its adversaries. In 1987, the internet was a technological anomaly, with relatively few connections and almost no public usage—but the notion of using intelligence assets to target information networks, steal critical data, and leverage it into technological advancement was already well refined. The emphasis upon the open transfer of information throughout Western societies in the 1987 document was a harbinger of future information networks and the rapid transfer of enormous volumes of data. The document is also interesting in that it foreshadows the growing links between national defense policy and the role of the private sector—a relationship that has only grown in importance in the succeeding decades.

- ***Document 2:*** *National Military Strategy of the United States of America: A Strategy of Flexible and Selective Engagement*
- ***When:*** 1995
- ***Where:*** Washington, D.C.
- ***Significance:*** In support of the overarching National Security Strategy documents released by presidential administrations and the National Defense Strategy documents created by the secretary of defense, the Joint Chiefs of Staff create a National Military Strategy that illustrates the broad priorities and principles of the American military establishment. This document allows the chairman of the Joint Chiefs of Staff to provide overarching guidance to the uniformed military that illustrates the roles it will play in the preservation of national security. In 1995, the military was still experiencing substantial change due to the end of the Cold War.

Although the U.S. military had led the coalition effort to expel Iraq from Kuwait, and demonstrated impressive capabilities in the process, it had shifted much of its efforts to humanitarian engagements in the succeeding years. The 1995 National Military Strategy reminded its readers that although the Soviet Union might have collapsed, the nation still faced substantial threats from a resurgent Russian Federation and an emerging People's Republic of China.

DOCUMENT

Fight and Win

The ability of US Armed Forces to fight and win, the third component of our strategy, serves as the ultimate guarantor of our vital interests. This ability is crucial to deter aggression and prevent conflict, and if challenged, it assures that we will in fact prevail. Being ready to fight and win remains our foremost responsibility and the prime consideration governing all our military activities. It is for this reason, fundamentally, that our Nation has raised and sustained its Armed Forces.

In war, our use of military force will follow the principles outlined below.

Clear Objectives—Decisive Force

In any application of force, military objectives will be clearly defined to support our national political aims in the conflict. We intend to commit sufficient force to achieve these objectives in a prompt and decisive manner.

Wartime Power Projection

If we have forces deployed to the threatened area when crisis turns to conflict, these forces will assist our regional allies in creating a viable defense to halt the invasion rapidly and will form the basis for the subsequent buildup of combat power needed to defeat the aggressor decisively. But we anticipate that, for the most part, we will project air, land, and sea forces from the United States and, in some cases, from overseas areas, to augment forward deployed forces or to establish US presence in the theater of operations. This power projection could ultimately entail the transport of large numbers of personnel and their equipment. Such an effort requires detailed plans to provide the necessary intelligence, logistics, and communications support, as well as capabilities to protect our forces during deployment.

We continue to build on the lessons learned in Operation Desert Storm to strengthen our power projection capabilities. During the September 1994 deployment of forces to Haiti, roll-on/roll-off shipping was proved exceptionally ready and significantly more reliable as a result of post-Gulf War improvements. Early access to combat, combat support, and combat service support capabilities in the Reserve component is also vital to meet our power projection requirements for any major regional contingency. We have demonstrated in recent operations in both Haiti

and Kuwait that we have the ability to gain this prompt access to the Reserves, clearly indicating improved wartime capabilities.

Fight Combined and Fight Joint

While we maintain the unilateral capability to wage decisive campaigns to protect US and multinational security interests, our Armed Forces will most often fight in concert with regional allies and friends, as coalitions can decisively increase combat power and lead to a more rapid and favorable outcome to the conflict. Combined operations capitalize on our peacetime training, help generate and sustain international support, and enable our forces to provide the high-leverage capabilities required to achieve decisive outcomes against any adversary.

Modern warfare requires US forces to fight as a joint team whether operating unilaterally or as part of an international coalition. Accordingly, each of the Services provides trained and ready forces to support the combatant commanders' warfighting plans and operations. Success in joint and combined military operations requires bringing to bear, at the right times and places, the unique and complementary capabilities of each of the Services.

Each Service has both a role and primary and collateral functions to execute, for which it must train, organize, and equip its forces. Land forces are mainly involved with prompt and sustained combat operations on land; naval and marine forces with operations at or from the sea; air forces with military operations in the air. Each of our Services leverages the benefits of unhindered access to space.

Land forces must be capable of deploying rapidly and, if necessary, executing forcible entry to seize the initiative and close with and destroy enemy forces through synchronized maneuver and precision fire throughout the breadth and depth of the battle area. They must be capable of achieving operational and tactical freedom of maneuver and be sufficiently agile to achieve their objectives before opponents can effect countermeasures. Land forces must possess the capabilities necessary to dominate the land battle. In addition, they must provide the combat support and combat service support necessary to sustain the land battle as well as provide critical elements of support to joint forces deployed in theater. Ultimately, land forces can occupy territory, control populations, and provide on-the-scene assurance that political objectives will be met.

Naval and marine forces must be capable of conducting naval and amphibious warfighting operations. Forward-deployed naval expeditionary forces can respond immediately to a crisis, execute forcible entry or reinforce other forward-deployed

DID YOU KNOW?

Michael Hayden

General Michael V. Hayden (1945–), USAF, retired, is the only person to have led both the Central Intelligence Agency (CIA) and the National Security Agency (NSA). He joined the U.S. Air Force in 1967, commencing a four-decade career as an intelligence officer. In 1999, he was named the director of the NSA, and during his tenure, he shifted the agency from its Cold War posture to a more agile orientation with a focus upon counterterrorism. In the aftermath of the September 11 attacks, Hayden expanded the NSA's data collection efforts, including a controversial domestic surveillance program that eavesdropped upon American citizens without warrants. His organization also began to collect metadata, allowing the government to obtain personal information from major technology companies such as Google and Facebook. In 2006, Hayden became the director of the CIA, presiding over a period of substantial increases in covert military operations, especially drone strikes. During his tenure, the CIA became far more aggressive throughout cyberspace, and Hayden continually warned political leaders that the United States is ill prepared to respond to sophisticated cyberattacks. Hayden publicly worried that the Stuxnet attacks, by which a cyber intrusion caused physical damage to a critical system, might establish a dangerous precedent for future cyber warfare.

elements, and through prompt action help halt an enemy offensive and enable the flow of follow-on ground and land-based air contingents. These forces assist in providing protective cover from air, land, sea, or missile intrusion. By ensuring freedom of the seas and controlling strategic choke points, naval and marine forces provide strategic freedom of maneuver and thus enhance deployment and sustainment of joint forces in theater.

Air forces must be capable of conducting military operations to gain and maintain control of the skies, holding vital enemy capabilities at risk throughout the theater, and helping to destroy the enemy's ability to wage war. Air superiority is essential so we can quickly move forces into theater and attack the enemy at will. Air control provides the joint force numerous operational and tactical advantages while facilitating land and naval maneuver. Air forces provide sustained, precise firepower, reconnaissance and surveillance, critical refueling, and global lift to rapidly deploy and sustain joint forces in theater.

Space forces play an increasingly important role in prosecuting modern warfare. They provide global and battlefield surveillance, ballistic missile warning, precise navigation, secure communications, weather, and intelligence information. Space assets facilitate effective command and control and enhance the joint utilization of our land, sea, and air forces.

Special operations forces from all three military departments provide combatant commanders and deployed forces with unique capabilities to conduct direct action, special reconnaissance, unconventional warfare, counterterrorism, psychological operations, and civil affairs activities. Properly employed, special operations forces provide commanders capabilities that extend their vision of the battlefield, increase their flexibility, and enhance their initiative. These forces will be fully integrated into military operations by the combatant commanders.

Win the Information War

The remarkable leverage attainable from modern reconnaissance, intelligence collection and analysis, and highspeed data processing and transmission warrants special emphasis. The Services and combatant commands require such fused information systems. These systems enhance our ability to dominate warfare. We must assure that this leverage works for us and against our adversaries. New doctrine is being developed, and training and control programs are underway, to ensure that advantages, built on the early success in Operation Desert Storm, are being exploited.

Countering Weapons of Mass Destruction

Potential adversaries should recognize our capability to dominate any escalation of conflict should weapons of mass destruction be employed against us. In addition, we will maintain and strengthen our defensive capabilities against such weapons. We continue efforts to prevent the use of mass destruction weapons and make preparations to operate effectively in environments marked by biological, chemical, or radioactive contamination.

Two Major Regional Contingency Focus

When entering any regional conflict, we will fully apply all the principles addressed above to ensure decisive victory. At the same time, however, we will remain aware

that risks and dangers remain in other regions. While projecting forces to one contingency, we will be enhancing the readiness of other assets to handle a challenge elsewhere. Some high-leverage capabilities could be used in one major regional contingency and then reallocated and redeployed to another as conditions permit. Other capabilities essential to fighting and winning the first conflict will remain in the theater where they are committed.

Force Generation

We will quickly generate combat power in wartime. Active forces engaged overseas in lower priority missions may be recalled, reorganized, retrained, and redeployed. Normally our Armed Forces will withdraw from operations other than war when the security situation is stabilized and other organizations are prepared to assume responsibility for relief or security. In times of crisis, we will need to accelerate this process. As our first forces react to a major regional crisis, we will begin actions to ensure forces are ready to meet a second contingency should it arise. Activities not involving critical US interests will be turned over to the United Nations or other responsible regional security organizations while we attend to higher priority taskings.

Substantial Reserve forces will be committed to combat and combat support missions early in any major regional contingency. To backfill active forces elsewhere and to prepare for unforeseen contingencies, some Reserve component forces can expect to be mobilized immediately and to remain on active duty throughout the conflict, even though they are not directly involved in operations.

Win the Peace

In the wake of any major theater conflict, our forces will likely encounter numerous demands to attend to the needs of the indigenous population. This may well include activities such as providing humanitarian relief and nation assistance that are included in the peacetime engagement component strategy. Planning for post-conflict operations will begin prior to and continue throughout any conflict. Close coordination between military and other governmental and nongovernmental agencies will be particularly critical during the transition period following war as some functions are transferred to non-military organizations and while our forces are being redeployed and reconstituted.

SOURCE: Joint Chiefs of Staff, *National Military Strategy of the United States of America: A Strategy of Flexible and Selective Engagement* (Washington, D.C.: Government Printing Office, 1995), 13–16, https://history.defense.gov/Portals/70/Documents/nms/nms1995.pdf?ver=2014-06-25-123428-503

ANALYSIS

Even the subtitle of this iteration of the National Military Strategy is illustrative—by calling for a flexible engagement capability, but one that would only be employed on a selective basis—the joint chiefs were effectively reminding the political leadership of the nation that the military might not be the best tool for humanitarian operations, peacekeeping efforts, diplomatic overtures, or other nontraditional activities.

Rather, this version of the National Military Strategy called for a modernization effort, particularly in terms of front-line equipment, that would allow the military to retrench itself as a heavy-combat force capable of deterring or destroying enemy forces in conventional theaters. It is also important to note that even though the importance of information operations were extremely clear to the authors, there was little evidence that they thought of the cyber domain as a separate avenue for military operations at that point. Some major cyber developments occurred shortly after the publication of this document, which proved to many uniformed strategists that the military could no longer take secure communications for granted in future combat scenarios.

- ***Document 3:*** *National Military Strategy of the United States of America: Shape, Respond, and Prepare Now: A Military Strategy for a New Era*
- ***When:*** 1997
- ***Where:*** Washington, D.C.
- ***Significance:*** The Goldwater-Nichols Department of Defense Reorganization Act of 1986 established the requirements for creating a National Security Strategy, National Defense Strategy, and National Military Strategy. Although it did not specify precisely how often such strategic documents should be devised and publicized, at no time did the development of strategic guidance become an annual event. Typically, new iterations were released every three to four years, making the 1997 version a very rapid follow-on to the 1995 document, particularly given the fact that the United States had not faced a major crisis in the intervening two years, and General John Shalikashvili served as the chairman of the Joint Chiefs of Staff during the production of both documents.

DOCUMENT

The Strategic Environment—Opportunities and Challenges

Asymmetric Challenges

Some state or nonstate actors may resort to asymmetric means to counter the US military. Such means include unconventional or inexpensive approaches that circumvent our strengths, exploit our vulnerabilities, or confront us in ways we cannot match in kind. Of special concern are terrorism, the use or threatened use of WMD, and information warfare. These three risks in particular have the potential to threaten the US homeland and population directly and to deny us access to critical overseas infrastructure. Other challenges include exploiting commercial and foreign space capabilities, interrupting the flow of critical information, denying our

access to strategic resources, and environmental sabotage. Hostile actors may use such means by themselves or in conjunction with conventional military force. Such asymmetric challenges are legitimate military concerns. We must increase our capabilities to counter these threats and adapt our military doctrine, training, and equipment to ensure a rapid and effective joint and interagency response.

. . .

The Strategy—Shape, Respond, Prepare Now

Preparing Now for an Uncertain Future

As we move into the next century, it is imperative that the United States maintain the military superiority essential to our global leadership. To be able to respond effectively in the future, we must transform US combat capabilities and support structures, but while we do so, our forces must remain engaged worldwide and ready to fight and win two nearly simultaneous major theater wars. Success demands a stabilized investment program in robust modernization that exploits the RMA [Revolution in Military Affairs]. It also requires fundamental reengineering of our infrastructure and streamlining of our support structures through the RBA [Revolution in Budgetary Affairs] to realize the cost efficiencies necessary to recapitalize the force. Though difficult to accomplish, such tasks are essential to reaching new levels of joint warfighting effectiveness.

Joint Vision 2010 is the conceptual template for joint operations and warfighting in the future. It provides the azimuth for the Services' visions, thus ensuring the future interoperability of the joint force. Because we will often act in concert with like-minded nations, as we implement *JV 2010*, we must also retain interoperability with our allies and potential coalition partners. This vision of future capabilities guides our warfighting requirements and procurement, and focuses technological development. *JV 2010*'s key enablers of information superiority and technological innovation will transform the current concepts of maneuver, strike, protection, and logistics into the new operational concepts of dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. Turning these concepts into reality will help us to conduct decisive operations in any environment, a characteristic *JV 2010* calls "full spectrum dominance." *JV 2010* rests on the foundations of information superiority and technological innovation.

Information Superiority.

Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of precise and reliable information, while exploiting or denying an adversary's ability to do the same. While it is dependent upon superior technology, systems integration, organization and doctrine, it is not an inherent quality

DID YOU KNOW?

ILOVEYOU Virus

The ILOVEYOU malware program was a worm that propagated itself through a vulnerability in the Microsoft Outlook email system. On May 4, 2000, two Filipino hackers launched the worm via email, with an attachment entitled "LOVE-LETTER-FOR-YOU.txt.vbs." Unwitting recipients who opened the file launched a Visual Basic script that quickly sent itself to all Outlook contacts on the user's machine. After taking this basic step to expand its infiltration, the worm then overwrote random files, damaging the host computer. The virus was one of the fastest-growing malware events in history, infecting more than one million computers per day and eventually damaging more than 45 million machines and causing over $5 billion in damages. The two creators of the worm, Onel de Guzman and Reomel Ramones, were not prosecuted for their activity, as it did not violate any laws in the Philippines at the time of their actions. Thus, one of the most damaging cyberattacks in history went completely unpunished, even though those responsible were clearly identified, demonstrating the effect of laws falling behind the pace of developing technology.

but, like air superiority, must be achieved in the battlespace throughout offensive and defensive information operations. Information superiority yields battlespace awareness, an interactive, shared and highly accurate picture of friendly and enemy operations as they occur. Information superiority allows our commanders to employ widely dispersed joint forces in decisive operations, engage and reengage with the appropriate force, protect the force throughout the battlespace, and conduct tailored logistical support.

Technological Innovation.

As we reshape our forces to meet the challenges of a changing world, we will leverage emerging technologies to enhance the capabilities of our servicemen and women through development of new doctrine, organizations, materiel, and training. Development and acquisition of new systems and equipment will improve our ability to conduct decisive operations and achieve full spectrum dominance. However, they are not a panacea. We must recognize that each includes inherent vulnerabilities; each must be applicable across the range of human operations; and each must enhance the human capability of our forces.

. . .

The Joint Force

Capabilities

Information Operations

Success in any operation depends on our ability to quickly and accurately integrate critical information and deny the same to an adversary. We must attain information superiority through the conduct of both offensive and defensive information operations. Information operations are, however, more than discrete offensive and defensive actions; they are also the collection and provision of that information to the warfighters. Superiority in these areas will enable commanders to contend with information threats to their forces, including attacks which may originate from outside their area of operations. It also limits an adversary's freedom of action by disabling his critical information systems. We are developing joint doctrine for offensive and defensive information operations that assigns appropriate responsibilities to all agencies and commands for assuring committed forces gain and maintain information superiority. This emerging joint doctrine must fully integrate interagency participation allowing us to leverage all existing information systems.

SOURCE: Joint Chiefs of Staff, *National Military Strategy of the United States of America: Shape, Respond, Prepare Now: A Military Strategy for a New Era* (Washington, D.C.: Government Printing Office, 1997), 9, 17–18, 27, https://history.defense.gov/Portals/70/Documents/nms/nms1997.pdf?ver=2014-06-25-123438-080

ANALYSIS

The 1997 National Military Strategy demonstrated a much stronger commitment to information operations than its immediate predecessor. In addition to announcing

efforts to create joint doctrine for information operations, it also required the incorporation of nonmilitary government organizations that had significant capabilities for both offensive and defensive information operations. As such, this document essentially provided the necessary requirements for the military and intelligence agencies to effectively merge their information operations, at least as pertained to military activities. Soon, the National Security Agency and various active-duty military units began long-lasting partnerships to develop cyber networks and the capabilities to attack and defend in the emerging domain. The 1997 version of the National Military Strategy is also important because it represented an effort by the top military commanders to halt the drawdown of forces that had occurred throughout the 1990s as a result of the end of the Cold War. By requiring that the military be capable of fighting two simultaneous theater wars, the strategy effectively set a floor on how low the necessary military forces could fall before the nation was incapable of carrying out its own strategy.

- ***Document 4:*** *Quadrennial Defense Review*
- ***When:*** May 1997
- ***Where:*** Washington, D.C.
- ***Significance:*** Many expected the United States to take advantage of the end of the Cold War to draw down the size of its military forces and take advantage of a "peace dividend" in the process. In theory, this would allow the United States to reduce the total size of its military budget, reduce the number of personnel on active duty, and slow down on weapons development and procurement programs. However, as the Quadrennial Defense Review (QDR) illustrated, although the Soviet Union's collapse reduced an existential threat, it also created opportunities for smaller actors, who might have been restrained by the bipolar power structure of the Cold War, to engage in a host of activities that might provoke American intervention.

DOCUMENT

Joint Vision 2010 and the Future of Warfare

In an effort to guide this transformation, the Chairman of the Joint Chiefs of Staff developed *Joint Vision 2010*, a conceptual template for how America's armed forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint military operations. *Joint Vision 2010* embraces information superiority and the technological advances that

will transform traditional warfighting via new operational concepts, organizational arrangements, and weapons systems. It guides the Department's preparations for the future through its focus on four new operational concepts—dominant maneuver, precision engagement, full-dimension protection, and focused logistics—that together aim at achieving full-spectrum dominance.

Information Superiority: Backbone of Military Innovation. The ongoing transformation of our military capabilities—the so-called Revolution in Military Affairs (RMA)—centers on developing the improved information and command and control capabilities needed to significantly enhance joint operations. With the support of an advanced command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) common backbone, the United States will be able to respond rapidly to any conflict; warfighters will be able to dominate any situation; and day-to-day operations will be optimized with accurate, timely, and secure information. Just as much of the non-defense world has become increasingly interconnected through the growth of internetted communications, the Department of Defense is working to provide a complementary, secure, open C4ISR network architecture.

The final five principal components of our evolving C4ISR architecture for 2010 and beyond are:

- A robust multi-sensor information grid providing dominant awareness of the battlespace to our commanders and forces;
- Advanced battle-management capabilities that allow employment of our globally deployed forces faster and more flexibly than those of potential adversaries;
- An information operations capability able to penetrate, manipulate, or deny an adversary's battlespace awareness or unimpeded use of his own forces;
- A joint communications grid with adequate capacity, resilience, and network-management capabilities to support the above capabilities as well as the range of communications requirements among commanders and forces;
- An information defense system to protect our globally distributed communications and processing network from interference or exploitation by an adversary.

In warfare, the information superiority that these capabilities provide will significantly increase the speed of command, enabling forward deployed and early-entry forces to take the initiative away from numerically superior enemy forces and set the conditions for early, favorable termination of the conflict.

. . .

QDR Modernizing Decisions: Supporting the Transformation of U.S. Forces

The Department's extensive modernization effort, which will reach the aggregate procurement spending objective of $60 billion per year shortly after the turn of the century, directly supports efforts to realize the modern, joint capabilities called for by *Joint Vision 2010* and to exploit the RMA in accordance with the "prepare now" tenet of our defense strategy. The QDR modernization review focused on a

number of programs for evaluation and decision, in order to ensure that future U.S. forces have modern, technologically superior equipment, that systems are effectively integrated across platforms and Services, and that programmatic and operational risks were weighed in the context of force requirements. Several of these decisions resulted in programmatic changes, highlighted below.

C4ISR. Because modernization of our forces depends on a strong C4ISR common backbone and because these systems require significant resources, the Department undertook a hard and sweeping look at our entire C4ISR effort. While a number of programmatic adjustments were evaluated, we did not change the general focus and amount of resources dedicated to C4ISR in the QDR. The net effect of the programmed investments will be to substantially improve our awareness of various types of enemy forces in the areas adjacent to our forces and at longer ranges as well. We will continue to evolve toward more interoperable battle management systems with the initial deployment of the Global Command and Control System (GCCS) below the joint command level and into operational Service units. The Department is committed to achieving information superiority and to the resolution of remaining challenges over the next several years. A significant C4ISR challenge is to overcome deficiencies in our ability to move information in a timely manner to the lowest tactical levels. We will fund efforts to meet such challenges by correcting certain imbalances in the overall C4ISR program and by more aggressively using advanced technologies to reduce ongoing program costs. Decisions on C4ISR will be made in the context of other decisions on force structure, force design, weapons platforms, munitions, and information-enabled operational concepts.

. . .

Information Operations. Efforts to exploit information technology to adapt and transform the U.S. military are well underway. To date, the Department has directed most of its efforts in this area toward protecting critical U.S. infrastructure against hostile information operations and developing U.S. information operation capabilities for use in peacetime engagement activities, smaller-scale contingencies, and major theater wars.

Although our current capabilities are adequate to defend against existing information operations threats, the increasing availability and decreasing costs of sophisticated technology to potential adversaries demand a robust commitment to improve our ability to operate in the face of information threats as we approach the 21st century. Critical to ensuring that ability will be the institutionalization of information operations—that is, the integration of informational operations concepts into military planning programming, budgeting, and operations. In the context of *Joint Vision 2010*, we will continue to develop additional guidance to strengthen information assurance—the protection, integrity, and availability of critical information systems and networks. Further, we will allocate adequate resources for these efforts within our information technology investment programs and improve the Defense-wide planning and implementation process, regularly assessing funding adequacies for all information assurance program components.

Defense against hostile information operations will require unprecedented cooperation between the Department of Defense, other federal agencies, the armed forces, commercial enterprises, our allies, and the public. The Department is working

closely with the Presidential Commission on Critical Infrastructure to develop this cooperative relationship. Technical measures to protect military information systems, both hardware and software, are being greatly expanded, and all Services now provide capabilities to test and assess their information networks and systems. Capabilities to protect information systems must also extend beyond traditional military structures into areas of civilian infrastructure that support national security requirements, such as the telecommunication and air traffic control systems.

Offensive actions to disrupt our adversary's access to information are also part of U.S. military capabilities. Such capabilities will be increased in the future to ensure that the United States maintains information superiority during a conflict.

SOURCE: U.S. Department of Defense, *Quadrennial Defense Review* (Washington, D.C.: Government Printing Office, 1997), 39–40, 44, 50–51.

ANALYSIS

This edition of the QDR, issued prior to the September 11 attacks, maintains most of its focus upon the possibility of peer and near-peer competitors. Despite the fact that the term "cyber" had been coined more than a decade earlier, it does not appear in the document in any form. However, many concepts that underpin cyber warfare are certainly present under the discussion related to information operations. Later editions of the QDR placed less emphasis upon the importance of information operations, and as a result, it created an environment allowing competitors to close the gap with the United States regarding cyber capabilities.

- ***Document 5:*** *A National Security Strategy for a New Century*
- ***When:*** December 1999
- ***Where:*** Washington, D.C.
- ***Significance:*** The William J. Clinton administration released its final National Security Strategy at the end of 1999 during a period of economic boom but political instability. With little more than a year left in his presidency, Clinton sought to define the nation's security priorities for the twenty-first century, with particular emphasis on the dangers of regional threats, failed states, and proliferation of dangerous weapons technology. The strategy did not have a clear primary adversary, as had been the case for Cold War iterations. Although it did recognize the emerging threat of cyberattacks, it seemed determined to place them into the category of criminal offenses rather than acts of war.

DOCUMENT

Drug Trafficking and Other International Crime

A broad range of criminal activities emanating from overseas threatens the safety and well-being of the American people.

. . .

Other International Crime. A free and efficient market economy requires transparency and effective law enforcement to combat unlawful activities such as extortion and corruption that impede rational business decisions and fair competition. The benefits of open markets are enhanced by fostering the safe and secure international movement of passengers and goods by all modes of transportation. Additionally, the integrity and reliability of the international financial system will be improved by standardizing laws and regulations governing financial institutions and improving international law enforcement cooperation in the financial sector. Corruption and extortion activities by organized crime groups can also undermine the integrity of government and imperil fragile democracies. And the failure of governments to effectively control international crime rings within their borders—or their willingness to harbor international criminals—endangers global stability. There must be no safe haven where criminals can roam free, beyond the reach of our extradition and legal assistance treaties.

We are negotiating and implementing new and updated extradition and mutual legal assistance treaties, and increasing our enforcement options through agreements on asset seizure, forfeiture, and money laundering. The new National Money Laundering Strategy being implemented by the Departments of Treasury and Justice is increasing the effectiveness of America's efforts both domestically and internationally to deprive organized crime groups the benefit of their illegal profits. Initiatives also are under way to accelerate the criminal identification process and facilitate global participation in the investigation and prosecution of criminal activities through the linking of worldwide law enforcement databases. This will be done in a manner that protects the privacy of U.S. citizens.

Because of the global nature of information networks, no area of criminal activity has greater international implications than high technology crime. Computer hackers and other cyber-criminals are not hampered by international boundaries, since information and transactions involving funds or property can be transmitted quickly and covertly via telephone and information systems. Many of the challenges that law enforcement faces in this area are extremely difficult to

DID YOU KNOW?

SQL Slammer Worm

In 2003, the SQL Slammer worm was released onto the internet by unknown parties for indeterminate reasons. The virus was a tiny piece of software, requiring only 374 bytes of information, which meant that it could carry out almost no functions other than propagating itself. However, in that respect, the SQL Slammer worm demonstrated the law of unintended consequences—it was so efficient at copying itself and spreading as fast as possible that it managed to shut down the entire internet for more than twelve hours. The crash of the World Wide Web came due to the enormous amount of traffic being sent to virtually every router on the planet, creating a cascading effect of failures. As routers were cleaned and reset, they notified connected routers, further increasing the strain on the network and triggering a series of follow-on shutdowns. Microsoft had actually patched the vulnerability exploited by SQL Slammer more than six months earlier, but the patch had not been installed on most computers and routers. Further, because billions of computers run pirated copies of Microsoft Office, they are not eligible for software patches released by the company. As a result, SQL Slammer remains one of the most commonly detected forms of malware on the internet today.

address without international consensus and cooperation. We seek to develop and implement new agreements and encourage cooperative research and development with other nations to address high technology crime, particularly cybercrime.

. . .

Critical Infrastructure Protection

Our national security and our economic prosperity rest on a foundation of critical infrastructures, including telecommunications, energy, banking and finance, transportation, water systems and emergency services. These infrastructures are vulnerable to computer-generated and physical attacks. More than any nation, America is dependent on cyberspace. We know that other governments and terrorist groups are creating sophisticated, well-organized capabilities to launch cyber-attacks against critical American information networks and the infrastructures that depend on them.

The President has directed that a plan for defending our critical infrastructures be in effect by May 2001, and fully operational by December 2003. Through this plan we will achieve and maintain the ability to protect our critical infrastructures from intentional acts that would significantly diminish the ability of the Federal Government to perform essential national security missions. This plan will also help ensure the general public health and safety; protect the ability of state and local governments to maintain order and to deliver minimum essential public services; and work with the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

The Federal government is committed to building this capability to defend our critical infrastructures, but it cannot do it alone. The private sector, as much as the Federal government, is a target for infrastructure attacks, whether by cyber or other means. A new partnership between the Federal government and the private sector is required. Acting jointly, we will work to identify and eliminate significant vulnerabilities in our critical infrastructures and the information systems that support them.

We are creating the systems necessary to detect and respond to attacks before they can cause serious damage. For the first time, law enforcement, intelligence agencies and the private sector will share, in a manner consistent with U.S. law, information about cyber-threats, vulnerabilities and attacks. The Government is developing and deploying new intrusion detection network technologies to protect Defense Department and other critical Federal systems, and we are encouraging the private sector to develop and deploy appropriate protective technology as well. A nationwide system for quickly reconstituting in the face of a serious cyber-attack is being developed. Every Federal Department is also developing a plan to protect its own critical infrastructures, which include both cyber and physical dimensions.

Finally, we will be building a strong foundation for continued protection of our critical infrastructures: increased Federal R&D in information security, increased investment in training and educating cybersecurity practitioners, and evaluating whether legislation is necessary to protect both our civil liberties and our critical infrastructures.

SOURCE: White House, *A National Security Strategy for a New Century* (Washington, D.C.: Government Printing Office, 1999), 15–18, http://nssarchive.us/NSSR/2000.pdf

ANALYSIS

The 1999 version of the National Security Strategy was the first such document to place special emphasis upon cyberattacks as a threat to national security. By the time the strategy was released, the internet had become a global sensation, and had already become a significant vector for criminal activity, as well as malicious attacks upon information networks and efforts to collect classified intelligence from rival states. The 1990s saw the rise of the first large internet-based companies, including retail titans like Amazon, although almost none of them managed to show much of a profit, and almost all of them collapsed in relatively short order. Business experts recognized the potential of e-commerce, and assumed that it would provoke entirely new forms of criminal activity. Military strategists were not as convinced of the utility of cyber systems, and hence, the emphasis upon crime seems to have been unchallenged by the Department of Defense (DOD).

- ***Document 6:*** *Quadrennial Defense Review Report*
- ***When:*** September 30, 2001
- ***Where:*** Washington, D.C.
- ***Significance:*** The QDR often serves as a bellwether for the defense posture of a presidential administration—and while it identifies the current priorities and capabilities of the Department of Defense, it also focuses upon the most likely threats in the near-term and distant future. As such, the QDR is, among other things, a predictive document that lays out the arguments for and against major defense programs, and typically clarifies for interested parties how the DOD intends to prepare for future conflicts.

DOCUMENT

America's Role in the World

America's goals are to promote peace, sustain freedom, and encourage prosperity. U.S. leadership is premised on sustaining an international system that is respectful of the rule of law. America's political, diplomatic, and economic leadership contributes directly to global peace, freedom, and prosperity. U.S. military strength is essential

DID YOU KNOW?

Nimda Worm

On September 18, 2001, computer researchers discovered a devastating new form of malware, the Nimda worm. This self-propagating computer virus spread itself through mass e-mailing the contact lists of an infected computer. In less than an hour, Nimda, which is "admin" spelled backward, went from unknown to the top reported attack on the internet. It proved particularly infectious as it could spread by a user opening an infected attachment to an email or by browsing on an infected server. Although the worm seemed designed to attack network servers, it also infected individual computers, and once it penetrated a network's defenses, it became extremely difficult to eradicate the worm. The program quickly scanned computer files, looking for additional attack vectors, to include moving through local area networks with ease. Although Nimda did not have a particularly destructive set of instructions, its single-minded focus upon spreading itself had substantial spillover effects upon the function of the entire internet, as it clogged bandwidth at exponential rates. Its launch immediately after the September 11 terror attacks made Nimda all the more devastating. Although the author of the worm remains unknown, certain clues within the code suggested it might have originated in the People's Republic of China.

to achieving these goals, as it assures friends and allies of an unwavering U.S. commitment to common interests.

America's security role in the world is unique. It provides the basis for a network of alliances and friendships. It provides a general sense of stability and confidence, which is crucial to the economic prosperity that benefits much of the world. And it warns those who would threaten the Nation's welfare or the welfare of U.S. allies and friends that their efforts at coercion or aggression will not succeed.

Even now as the Nation mourns the victims of terrorist attacks on the Pentagon and the World Trade Center, America's purposes remain clear and its commitment resolute.

. . .

Key Military-Technical Trends. Technology in the military sphere is developing as rapidly as the tremendous changes reshaping the civilian sector. The combination of scientific advancement and globalization of commerce and communications have contributed to several trends that significantly affect U.S. defense strategy.

Rapid advancement of military technologies. The ongoing revolution in military affairs could change the conduct of military operations. Technologies for sensors, information processing, precision guidance, and many other areas are rapidly advancing. This poses the danger that states hostile to the United States could significantly enhance their capabilities by integrating widely available off-the-shelf technologies into their weapon systems and armed forces. For the United States, the revolution in military affairs holds the potential to confer enormous advantages and to extend the current period of U.S. military superiority. Exploiting the revolution in military affairs requires not only technological innovation but also development of operational concepts, undertaking organizational adaptations, and training and experimentation to transform a country's military forces.

Increasing proliferation of CBRNE [Chemical, Biological, Radiological, Nuclear, and Explosive] weapons and ballistic missiles. The pervasiveness of proliferation in an era of globalization has increased the availability of technologies and expertise needed to create the military means to challenge directly the United States and its allies and friends. This includes the spread of CBRNE weapons and their means of delivery, as well as advanced conventional weapons. In particular, the pace and scale of recent ballistic missile proliferation has exceeded earlier intelligence estimates and suggests these challenges may grow at a faster pace than previously expected. Likewise, the biotechnology revolution holds the probability of increasing threats of biological warfare.

Emergence of new arenas of military competition. Technological advances create the potential that competitions will develop in space and cyber space. Space and

information operations have become the backbone of networked, highly distributed commercial civilian and military capabilities. This opens up the possibility that space control—the exploitation of space and the denial of the use of space to adversaries—will become a key objective in future military competition. Similarly, states will likely develop offensive information operations and be compelled to devote resources to protecting critical information infrastructure from disruption, either physically or through cyber space.

Increasing potential for miscalculation and surprise. Together, these military-technical trends create an increased potential for miscalculation and surprise. In recent years, the United States has been surprised by the speed with which other states have progressed in developing weapons of mass destruction and ballistic missiles. In the future, it is unlikely that the United States will be able accurately to predict how successfully other states will exploit the revolution in military affairs, how rapidly potential or actual adversaries will acquire CBRNE weapons and ballistic missiles, or how competitions in space and cyber space will develop.

SOURCE: U.S. Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C.: Government Printing Office, 2001), 1, 6–7.

ANALYSIS

Although this edition of the QDR directly addressed the concept of cyber warfare, it also made it clear that cyber conflict was to be considered a future problem, rather than a current, ongoing concern. Rather, the 2001 QDR focused much more upon conventional conflicts and the rise of new potential adversaries. In many ways, the 2001 QDR presaged the 2003 Iraq War, rather than the War on Terror that had commenced less than one month before its release. The 2001 QDR also made an explicit connection between cyber and space-based capabilities, which reflected an understanding of the amount of data being relayed through space assets, but which also served to delineate cyber operations as being outside the control of any of the individual services.

- ***Document 7:*** *The National Strategy to Secure Cyberspace*
- ***When:*** February 2003
- ***Where:*** Washington, D.C.
- ***Significance:*** In 2003, the United States released its first document regarding a unified strategy for operations in cyberspace, particularly those of a military character. This document, while somewhat raw and unrefined at times, represented the first effort by a major world power to codify its approach to the cyber domain, and to set appreciable limits upon acceptable behaviors in cyberspace.

DOCUMENT

A Nation in Cyberspace

Our Nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is the nervous system of these infrastructures—the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security. Unfortunately, recent events have highlighted the existence of cyberspace vulnerabilities and the fact that malicious actors seek to exploit them. (See, *Cyberspace Threats and Vulnerabilities*.)

This *National Strategy to Secure Cyberspace* is part of an overall effort to protect the Nation. It is an implementing component of the *National Strategy for Homeland Security* and is complemented by the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, or control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people.

A Unique Problem, a Unique Process

Most critical infrastructures, and the cyberspace on which they rely, are privately owned and operated. The technologies that create and support cyberspace evolve rapidly from privatesector and academic innovation. Government alone cannot sufficiently secure cyberspace. Thus, President Bush has called for voluntary partnerships among government, industry, academia, and nongovernmental groups to secure and defend cyberspace. (See, *National Policy and Guiding Principles*.)

In recognition of this need for partnership, the process to develop the *National Strategy to Secure Cyberspace* included soliciting views from both the public and private sectors. To do so, the White House sponsored town hall meetings on cyberspace security in ten metropolitan areas. Consequently, individual sectors (e.g., higher education, state and local government, banking and finance) formed workgroups to create initial sector-specific cyberspace security strategies. Additionally, the White House created a Presidential advisory panel, the National Infrastructure Advisory Council, consisting of leaders from the key sectors of the economy, government, and academia. The President's National Security Telecommunications Advisory Committee reviewed and commented on the *Strategy*.

In September 2002, the President's Critical Infrastructure Protection Board sought comments from individuals and institutions nationwide by placing a draft version of the *Strategy* online for review. Thousands participated in the town hall

meetings and provided comments online. Their comments contributed to shaping the *Strategy* by narrowing its focus and sharpening its priorities.

This process recognizes that we can only secure cyberspace successfully through an inclusive national effort that engages major institutions throughout the country. The federal government designed the *Strategy* development process to raise the Nation's level of awareness of the importance of cybersecurity. Its intent was to produce a *Strategy* that many Americans could feel they had a direct role in developing, and to which they would be committed.

Although the redrafting process reflects many of the comments provided, not everyone will agree with each component of the *National Strategy to Secure Cyberspace*. Many issues could not be addressed in detail, and others are not yet ripe for national policy. The *Strategy* is not immutable; actions will evolve as technologies advance, as threats and vulnerabilities change, and as our understanding of the cybersecurity issues improves and clarifies. A national dialogue on cyberspace security must therefore continue.

In the weeks following the release of the draft *Strategy*, Congress approved the creation of the Department of Homeland Security (DHS), assigned to it many agencies that are active in cybersecurity, and directed it to perform new cybersecurity missions. This *Strategy* reflects those changes. Congress passed and the President signed the *Cyber Security Research and Development Act* (Public Law 107-305), authorizing a multi-year effort to create more secure cyber technologies, to expand cybersecurity research and development, and to improve the cybersecurity workforce.

Five National Cyberspace Security Priorities

The *National Strategy to Secure Cyberspace* is a call for national awareness and action by individuals and institutions throughout the United States, to increase the level of cybersecurity nationwide and to implement continuous processes for identifying and remedying cyber vulnerabilities. Its framework is an agenda of five broad priorities that require widespread voluntary participation. Each individual program consists of several components, many of which were drawn from the draft *Strategy's* recommendations and related public comments.

Addressing these priorities requires the leadership of DHS as well as several other key federal departments and agencies. As part of the Office of Management and Budget (OMB)-led budget process, and with the support of Congress, these departments and agencies now have the task of translating the *Strategy's* recommendations into actions.

Corporations, universities, state and local governments, and other partners are also encouraged to take actions consistent with these five national cyberspace security priorities, both independently and in partnership with the federal government. Each private-sector organization must make its own decisions based on cost effectiveness analysis and risk-management and mitigation strategies. The *National Strategy to Secure Cyberspace* articulates five national priorities. The first priority focuses on improving our ability to respond to cyber incidents and reduce the potential damage from such events. The second, third, and fourth priorities aim to reduce the

numbers of cyber threats and our overall vulnerability to cyber attacks. The fifth priority focuses on preventing cyber attacks with the potential to impact national security assets and improving international management of and response to such attacks.

Priority I: A National Cyberspace Security Response System

Rapid identification, information exchange, and remediation can often mitigate the damage caused by malicious cyberspace activity. For those activities to take place effectively at a national level, the United States requires a partnership between government and industry to perform analyses, issue warnings, and coordinate response efforts. Privacy and civil liberties must be protected in the process. Because no cybersecurity plan can be impervious to concerted and intelligent attacks, information systems must be able to operate while under attack and also have the resilience to restore full operations in their wake. To prepare for the possibility of major cyber attacks, America needs a national cyber disaster recovery plan. The National Cyberspace Security Response System will involve public and private institutions and cyber centers to perform analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts.

Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program

By exploiting vulnerabilities in our cyber systems, an organized cyber attack may endanger the security of our Nation's critical infrastructures. Cyberspace vulnerabilities occur in the critical infrastructure enterprises and government departments themselves, in their external supporting structures (such as the mechanisms of the internet), and in unsecured sites across the interconnected network of networks. Vulnerabilities exist for several reasons including technological weaknesses, poor security-control implementation, and absences of effective oversight.

A National Cyberspace Security Threat and Vulnerability reduction program will include coordinated national efforts conducted by governments and the private sector to identify and remediate the most serious cyber vulnerabilities through collaborative activities, such as sharing best practices and evaluating and implementing new technologies. Additional program components will include raising cybersecurity awareness, increasing criminal justice activities, and developing national security programs to deter future cyber threats.

Priority III: A National Cyberspace Security Awareness and Training Program

Many information-system vulnerabilities exist because of a lack of cyberspace security awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers, chief executive officers, and corporate boards. These vulnerabilities can present serious risks to the infrastructures even if they are not actually part of the infrastructure itself. A lack of trained personnel and the absence of widely accepted, multi-level certifications for personnel further complicate the task of reducing vulnerabilities.

The National Cyberspace Security Awareness and Training Program will raise cybersecurity awareness in companies, government agencies, universities, and among the Nation's computer users. It will further address shortfalls in the numbers of trained and certified cybersecurity personnel.

Priority IV: Securing Governments' Cyberspace

Although governments administer only a minority of the Nation's critical infrastructure computer systems, governments at all levels perform essential services that rely on each of the critical infrastructure sectors, which are agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. With respect to investment in cyberspace security, government can lead by example by fostering a marketplace for more secure technologies through large procurements of advanced information assurance technologies. A program to implement such products will help to ensure that federal computer systems and networks are secure. The federal government will also assist state and local governments with cybersecurity awareness, training, and information exchange.

Priority V: National Security and International Cyberspace Security Cooperation

America's cyberspace links the United States to the rest of the world. A network of networks spans the planet, allowing malicious actors on one continent to act on systems thousands of miles away. Cyber attacks cross borders at light speed, and discerning the source of malicious activity is difficult. America must be capable of safeguarding and defending its critical systems and networks—regardless of where an attack originates. Facilitating our ability to do so requires a system of international cooperation to enable the information sharing, reduce vulnerabilities, and deter malicious actors.

SOURCE: White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: Government Printing Office, 2003), 1–4, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

ANALYSIS

Even in 2003, it was obvious that the cyber domain would grow as a key element in the U.S. economy, culture, and society as a whole. While this offered enormous potential as a source of strength, innovation, and information, it also created a significant vulnerability. If the United States wished to remain the world's foremost economic and military power, it needed to recognize the potential applications of cyberspace. Never before had information transfers been carried out with such ease—and as a result, technological developments became much more difficult to secure, as hackers might very well extract the key aspects of change and transmit them to competing powers, which in turn might be able to exploit those changes faster than the United States could. This principle applied to military technology, but it also applied to private corporations and their efforts to develop new products and processes. If a competitor could simply steal intellectual property, there was little incentive to develop new concepts. Thus, the United States, as a "nation in cyberspace," had a compelling reason to consider the security of the cyber domain, and how much effort and expenditure it might be willing to invest in such an endeavor.

- ***Document 8:*** *The National Military Strategy of the United States of America: A Strategy for Today; a Vision for Tomorrow*
- ***When:*** 2004
- ***Where:*** Washington, D.C.
- ***Significance:*** The 2004 iteration of the National Military Strategy was developed shortly after the commencement of Operation Iraqi Freedom, in which a U.S.-led coalition invaded Iraq with the goal of removing President Saddam Hussein from power. While it devoted relatively little space to issues related to cyberwarfare, the strategy placed substantial emphasis upon the need for the services to work together in a joint fashion for winning future conflicts, and nowhere is such a need for joint activity more closely felt than in cyber operations.

DOCUMENT

III. A Joint Force for Mission Success

The objectives of protect, prevent and prevail provide the foundation for defining military capabilities and creating a joint force that can contend effectively with uncertainty. They support a capabilities-based approach that focuses on how adversaries will fight in the future rather than on which specific adversaries we may fight. The Armed Forces must have the ability to defeat opponents that possess WMD/E, combine both low-tech and high-tech capabilities and merge traditional and asymmetric capabilities in an attempt to overcome US military advantages.

Defeating adaptive adversaries requires flexible, modular and deployable joint forces with the ability to combine the strengths of individual Services, combatant commands, other government agencies and multinational partners. Joint forces will require new levels of interoperability and systems that are "born joint," i.e., conceptualized and designed with joint architectures and acquisition strategies. This level of interoperability ensures that technical, doctrinal and cultural barriers do not limit the ability of joint commanders to achieve objectives. The goal is to design joint force capabilities that increase the range of options—from kinetic to non-kinetic—available to the President and Secretary of Defense.

. . .

B. Functions and Capabilities

Inherent in each military objective is a series of functions that the Joint Force must perform. Commanders derive their tasks and define required capabilities through an analysis of these functions and the concepts that describe how the Armed Forces will perform them. Capabilities that allow the Joint Force to perform these functions result from combinations of joint doctrine, organization, training programs, materiel solutions, leadership, personnel and facilities.

Applying Force

The application of military force to achieve the objectives of the NMS is the primary task of the Armed Forces. It requires the integrated use of maneuver and engagement to create precisely defined effects. Force application includes force movement to gain positional and temporal advantage to rapidly seize the initiative and complicate an adversary's defensive plans. Force application integrates air, land, sea, special operations, information and space capabilities. It also requires unprecedented levels of persistence that allow commanders, even in a high-threat environment, to assess results against mission objectives, adjust capabilities accordingly and reengage as required.

Applying force requires power projection assets to move capabilities rapidly, employ them precisely and sustain them even when adversaries employ anti-access and counter power projection strategies. Such power projection requires assured access to theaters of operation and enhanced expeditionary capabilities that support operational maneuver from strategic distances. Strong regional alliances and coalitions enhance expeditionary capabilities by providing physical access to host nation infrastructure and other support. They also provide access to regional intelligence that enables the precise application of military capabilities and allows the United States to focus combat power more effectively at the critical time and place.

Achieving shared situational awareness with allies and partners will require compatible information systems and security processes that protect sensitive information without degrading the ability of multinational partners to operate effectively with US elements. Such information and intelligence sharing helps build trust and confidence essential to strong international partnerships.

Force application focuses more on generating the right effects to achieve objectives than on generating overwhelming numbers of forces. The application of force against widely dispersed adversaries, including transnational terrorist organizations, will require improved intelligence collection and analysis systems. Effective global strike to damage, neutralize or destroy any objective results from a combination of precision and maneuver and the integration of new technologies, doctrine and organizations. Defeating the most dangerous threats will require persistence in force application that allows strikes against time-sensitive and time-critical targets. Ensuring capabilities are positioned and ready to conduct strikes against these targets requires the ability to sustain operations over time and across significant distances.

Deploying and Sustaining Military Capabilities

Force application in multiple overlapping operations will challenge sustainment capabilities. Sustaining such operations requires the ability to support forces operating in and from austere or unimproved forward locations. Additionally, the

DID YOU KNOW?

MyDoom Virus

In 2004, an email-propagated computer virus began to target networks running Microsoft Windows. The worm copied itself to infected computers through file attachments to ordinary messages, and once installed, sought to send copies of itself to everyone in the victim's address book. In addition to sending itself in this fashion, the MyDoom virus installed a Trojan horse program that allowed remote access and control of infected systems, typically resulting in the affected computer being used as part of a botnet. The worm spread extremely quickly, infecting five hundred thousand systems in short order. By the time Microsoft devised a patch to close the vulnerability exploited by MyDoom, the virus accompanied roughly one in twelve email messages being sent worldwide. Although Microsoft offered a $250,000 bounty for information leading to the arrest of MyDoom's creator, no one has ever been charged with its development.

increasing importance of mobility will necessitate more expeditionary logistics capabilities. Focused logistics provides the right personnel, equipment and supplies in the right quantities and at the right place and time. Such focused logistics capabilities will place a premium on networking to create a seamless end-to-end logistics system that synchronizes all aspects of the deployment and distribution processes.

Overlapping major combat operations place major demands on strategic mobility. Achieving objectives in such operations requires robust sealift, airlift, aerial refueling and pre-positioned assets. Strategic mobility that supports these operations also requires supporting equipment to store, move and distribute materiel and an information infrastructure to provide real-time visibility of the entire logistics chain.

Sustainment includes force generation and management activities that ensure the long-term viability of the force. Force generation includes recruiting, training, educating and retaining highly qualified people in the Active and Reserve Components as well as within the DOD civilian and contracted workforce. These personnel must have the right skill sets to apply joint doctrine within their organizations. Force generation requirements must include planning, programming, acquisition, maintenance, repair and recapitalization of equipment and infrastructure to maintain readiness.

Force management contributes to improving readiness levels even during high-intensity operations. It considers the effects of modernization and transformation on unit availability, readiness and integration. Force management policies, including force rotation policies that reduce stress on the joint force, evolve from continuous assessments of operational requirements. They also help to determine appropriate locations, capabilities and associated infrastructure required to support multiple, simultaneous operations. Force management policies help define the right mix of Active and Reserve Component forces and ensure a proper balance of capabilities.

Securing Battlespace

The Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace. Armed Forces must employ military capabilities to ensure access to these domains to protect the Nation, forces in the field and US global interests. The non-linear nature of the current security environment requires multi-layered active and passive measures to counter numerous diverse conventional and asymmetric threats. These include conventional weapons, ballistic and cruise missiles and WMD/E. They also include threats in cyberspace aimed at networks and data critical to US information-enabled systems. Such threats require a comprehensive concept of deterrence encompassing traditional adversaries, terrorist networks and rogue states able to employ any range of capabilities.

The Armed Forces require new capabilities to detect and interdict a wide range of threats close to their source and throughout the strategic approaches. The availability of intelligence and dual use technology to a wider variety of potential adversaries poses an increasing danger, providing them the ability to interrupt or exploit US information systems. Adversaries may find new and innovative ways to combine capabilities into effective weapons and enhance their ability to threaten the United States. Military forces must have both the means and established rules of engagement

to take action ranging from active counter proliferation to military action that supports non-proliferation policies. Securing battlespace will require cooperative activities with other government agencies and multinational partners to deny the use of these capabilities and to counter asymmetric attacks. This requires doctrine, tools and training to more effectively synchronize military capabilities with non-DOD assets.

Consequence management capabilities are essential in the aftermath of an attack, especially an attack with WMD/E. Such capabilities limit damage and casualties and include actions to counter the effects of WMD/E or the intentional or unintentional release of toxic chemicals following military operations. Consequence management helps restore affected areas through actions that contain, neutralize and decontaminate weapon agents. When directed, the Joint Force extends consequence management assistance to allies and other security partners.

Military operations require information assurance that guarantees access to information systems and their products and the ability to deny adversaries access to the same. Securing the battlespace includes actions to safeguard information and command and control systems that support the precise application of force and sustainment activities that ensure persistence across the full range of military operations. Securing battlespace ensures the ability of the Armed Forces to collect, process, analyze and disseminate all-source intelligence and other relevant information that contribute to decision superiority.

Achieving Decision Superiority

Decision superiority—the process of making decisions better and faster than an adversary—is essential to executing a strategy based on speed and flexibility. Decision superiority requires new ways of thinking about acquiring, integrating, using and sharing information. It necessitates new ideas for developing architectures for command, control, communications and computers (C4) as well as the intelligence, surveillance and reconnaissance assets that provide knowledge of adversaries. Decision superiority requires precise information of enemy and friendly dispositions, capabilities, and activities, as well as other data relevant to successful campaigns. Battlespace awareness, combined with responsive command and control systems, supports dynamic decision-making and turns information superiority into a competitive advantage adversaries cannot match.

Persistent surveillance, ISR [Intelligence, Surveillance, and Reconnaissance] management, collaborative analysis and on-demand dissemination facilitate battlespace awareness. Developing the intelligence products to support this level of awareness requires collection systems and assured access to air, land, sea and space-based sensors. Human collectors are a critical element in the collection system; they provide the ability to discern the intention of adversaries and produce actionable intelligence for plans and orders. Intelligence analysts operating well forward must have the ability to reach back to comprehensive, integrated databases and to horizontally integrate information and intelligence. The entire system must be supported by effective counterintelligence capabilities that deny an adversary access to critical information.

Battlespace awareness requires the ability to share relevant information with other government agencies and allies. Such information sharing requires multi-level security capabilities that allow multinational partners and other government agencies to access and use relevant information while reducing the probability of compromise. Seamless multi-level security access will empower distributed command and control and provide increased transparency in multinational operations. Decisions to apply force in multiple, widely dispersed locations require highly flexible and adaptive joint command and control processes. Commanders must communicate decisions to subordinates, rapidly develop alternative courses of action, generate required effects, assess results and conduct appropriate follow-on operations.

The Joint Force requires the ability to conduct information operations, including electronic warfare, computer network operations, military deception, psychological operations and operations security that enable information superiority. Information operations must be adaptive—tailorable to specific audiences and requirements and flexible enough to accommodate operational adjustments. Should deterrence fail, information operations can disrupt an enemy's network and communications-dependent weapons, infrastructure and command and control and battlespace management functions. Information operations, both offensive and defensive, are key to ensuring US freedom of action across the battlespace.

A decision superior joint force must employ decision-making processes that allow commanders to attack time-sensitive and time-critical targets. Dynamic decision-making brings together organizations, planning processes, technical systems and commensurate authorities that support informed decisions. Such decisions require networked command and control capabilities and a tailored common operating picture of the battlespace. Networking must also provide increased transparency in multinational operations and support the integration of other government agencies and multinational partners into joint operations. Force application, sustainment and actions to secure battlespace will rely on these capabilities.

SOURCE: U.S. Department of Defense, *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow* (Washington, D.C.: Government Printing Office, 2004), 16–20, https://history.defense.gov/Portals/70/Documents/nms/nms2004.pdf?ver=2014-06-25-123447-627

ANALYSIS

The particular emphasis on decision superiority, namely, the ability for military forces to make quicker and more accurate decisions in the face of enemy activity, is of particular interest for the cyber warrior. After all, correct decisions are almost entirely dependent upon having solid, accurate information available for the decision-maker. The nature of cyberwarfare makes such information much harder to secure and makes it much easier to face the possibility of degraded, destroyed, or incorrect information being presented to commanders. Thus, if the ultimate goal of the National Military Strategy is to find ways to conduct the application of force in

support of high-level strategic guidance, the protection of the underlying information is of utmost importance.

- ***Document 9:*** *The National Defense Strategy of the United States of America*
- ***When:*** March 2005
- ***Where:*** Washington, D.C.
- ***Significance:*** The National Defense Strategy is crafted using the National Security Strategy as guidance. Thus, it tends to be released a year or more after the National Security Strategy is produced, allowing the defense establishment time to consider how to implement the goals of the commander in chief. In 2005, the DOD faced constrained budgets and limited personnel while attempting to fight two wars in Afghanistan and Iraq, and counter the efforts of al Qaeda and other terror organizations.

DOCUMENT

I. America's Security in the 21st Century
A Changing Security Environment
Mature and Emerging Challenges

The U.S. military predominates in the world in *traditional* forms of warfare. Potential adversaries accordingly shift away from challenging the United States through *traditional* military action and adopt asymmetric capabilities and methods. An array of *traditional*, *irregular*, *catastrophic*, and *disruptive* capabilities and methods threaten U.S. interests:

- ***Traditional*** *challenges* are posed by states employing recognized military capabilities and forces in well-understood forms of military competition and conflict.
- ***Irregular*** challenges come from those employing "unconventional" methods to counter the *traditional* advantages of stronger opponents.
- ***Catastrophic*** challenges involve the acquisition, possession, and use of WMD or methods producing WMD-like effects.
- ***Disruptive*** challenges may come from adversaries who develop and use breakthrough technologies to negate current U.S. advantages in key operational domains.

These categories overlap. Actors proficient in one can be expected to try to reinforce their position with methods and capabilities drawn from others.

Indeed, recent experience indicates that the most dangerous circumstances arise when we face a complex of challenges. For example, our adversaries in Iraq and Afghanistan presented both *traditional* and *irregular* challenges. Terrorist groups like al Qaeda are *irregular* threats but also actively seek *catastrophic* capabilities. North Korea at once poses *traditional, irregular,* and *catastrophic* challenges. Finally, in the future, the most capable opponents may seek to combine truly *disruptive* capacity with *traditional, irregular,* or *catastrophic* forms of warfare.

. . .

Disruptive Challenges. In rare instances, revolutionary technology and associated military innovation can fundamentally alter long-established concepts of warfare. Some potential adversaries are seeking *disruptive* capabilities to exploit U.S. vulnerabilities and offset the current advantages of the United States and its partners.

Some *disruptive* breakthroughs, including advances in biotechnology, cyber operations, space, or directed-energy weapons, could seriously endanger our security.

As such breakthroughs can be unpredictable, we should recognize their potential consequences and hedge against them.

. . .

Desired Capabilities and Attributes
Key Operational Capabilities
Operating from the Global Commons

Our ability to operate in and from the global common—space, international waters and airspace, and cyberspace—is important. It enables us to project power anywhere in the world from secure bases of operation. Our capacity to operate in and from the strategic commons is critical to the direct defense of the United States and its partners and provides a stabilizing influence in key regions.

Such capacity provides our forces operational freedom of action. Ceding our historic maritime advantage would unacceptably limit our global reach. Our capacity to operate from international airspace and outer space will remain important for joint operations. In particular, as the nation's reliance on space-based systems continues to grow, we will guard against new vulnerabilities. Key goals, therefore, are to ensure our access to and use of space, and to deny hostile exploitation of space to adversaries.

Cyberspace is a new theater of operations. Consequently, information operations (IO) is becoming a core military competency. Successful military operations depend on the ability to protect information infrastructure and data. Increased dependence on information networks creates new vulnerabilities that adversaries may seek to exploit. At the same time, an adversary's use of information networks and technologies creates opportunities for us to conduct discriminate offensive IO as well. Developing IO as a core military competency requires fundamental shifts in processes, policies, and culture.

We will operate in and from the commons by overcoming challenges to our global maritime, air, space, and cyberspace operations.

. . .

Conducting Network-Centric Operations

The foundation of our operations proceeds from a simple proposition: the whole of an integrated and networked force is far more capable than the sum of its parts. Continuing advances in information and communications technologies hold promise for networking highly distributed joint and combined forces. Network-centric operational capability is achieved by linking compatible information systems with usable data. The functions of sensing, decision-making, and acting—which often in the past were built into a single platform—now can work closely even if they are geographically distributed across the battlespace.

Bringing decisive capabilities to bear increasingly will rely on our capacity to harness and protect advantages in the realm of information. Networking our forces will provide the foundation for doing so. Operations in the war on terrorism have demonstrated the advantages of timely and accurate information, while at the same time reinforcing the need for even greater joint, interoperable command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR).

Beyond battlefield applications, a network-centric force can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes by giving all users access to the latest, most relevant, most accurate information. It also enables "reach-back" by more effectively employing people and capabilities without deploying them forward.

Transforming to a network-centric force requires fundamental changes in processes, policy, and culture. Change in these areas will provide the necessary speed, accuracy, and quality of decision-making critical to future success.

We will conduct network-centric operations with compatible information and communications systems, usable data, and flexible operational constructs.

SOURCE: U.S. Department of Defense, *The National Defense Strategy of the United States* (Washington, D.C.: Government Printing Office, 2005), 2–3, 13, 14, https://history.defense.gov/Portals/70/Documents/nds/2005_NDS.pdf?ver=2014-06-25-124535-143

ANALYSIS

Under Secretary of Defense Donald Rumsfeld, the DOD undertook a massive transformation to recreate itself as a more lean, agile, and flexible force. Rumsfeld sought to shake off the Cold War assumptions about massive formations of overwhelming force, and instead, to seek ways to achieve the same effects through smaller commitments of more precise operational units. He also believed that conceptualizing potential adversaries as a network of interconnected nodes, rather than a monolithic entity, offered a better mechanism to devise means of both offensive and defensive activities. Striking at the connections within a network might have substantial effects throughout the entire network, well beyond the immediate target. In this regard, Rumsfeld's department seemed to be reinvigorating the industrial web theory of enemy systems from World War II, modernized to go well beyond attacks on sources of military production.

- ***Document 10:*** *Quadrennial Defense Review Report*
- ***When:*** February 6, 2006
- ***Where:*** Washington, D.C.
- ***Significance:*** This iteration of the QDR was completed while the United States was engaged in wars in Afghanistan and Iraq. Osama bin Laden remained at large, the Taliban had become a resurgent force, and the insurgency in Iraq had cost thousands of American lives with very little progress to show for it. Donald Rumsfeld resigned as the secretary of defense a few months after its publication to be replaced by Robert Gates. The term "network-centric warfare" became the key phrase for the DOD regarding the establishment of cyber forces.

DOCUMENT

Achieving Net-Centricity

Vision. Harnessing the power of information connectivity defines net-centricity. By enabling critical relationships between organizations and people, the Department is able to accelerate the speed of business processes, operational decision-making and subsequent actions. Recent operational experiences in Afghanistan and Iraq have demonstrated the value of net-centric operations. Ground forces were able to reach back to remote UAV [Unmanned Aerial Vehicles] pilots in Nevada to direct UAVs in support of their operations, achieving a level of air-ground integration that was difficult to imagine just a decade ago. Such connectivity is helping joint forces gain greater situational awareness to attack the enemy.

Achieving the full potential of net-centricity requires viewing information as an enterprise asset to be shared and as a weapon system to be protected. As an enterprise asset, the collection and dissemination of information should be managed by portfolios of capabilities that cut across legacy stove-piped systems. These capability portfolios would include network-based command and control, communications on the move and information fusion. Current and evolving threats highlight the need to design, operate and defend the network to ensure continuity of joint operations.

Progress to Date. The foundation for net-centric operations is the Global Information Grid (GIG), a globally interconnected, end-to-end set of trusted and protected information networks. The GIG optimizes the processes for collecting, processing, storing, disseminating, managing and sharing information within the Department and with other partners. The Department has made steady progress implementing net-centric systems and concepts of operation. It has deployed an enhanced land-based network and new satellite constellation as part of the Transformational Communication Architecture to provide high-bandwidth, survivable internet protocol communications. Together, they will support battle-space awareness, time-sensitive

targeting and communications on the move. Deployed terminals—from command and control (Joint Tactical Radio System) to very large bandwidth ISR systems—are extending the communications "backbone" down to the smallest tactical unit in the field. The Department has also implemented a data strategy enabling the fusion of information from any platform or terminal. Pulling all this together, the revised Unified Command Plan has assigned U.S. STRATCOM lead responsibility to operate and protect the Department's Global Information Grid.

QDR Decisions. To move closer toward this vision and build on progress to date, the Department will:

- Strengthen its data strategy—including the development of common data lexicons, standards, organization, and categorization—to improve information sharing and information assurance, and extend it across a multitude of domains, ranging from intelligence to personnel systems.
- Increase investment to implement the GIG, defend and protect information and networks and focus research and development on its protection.
- Develop an information-sharing strategy to guide operations with Federal, state, local and coalition partners.
- Shift from Military Service-focused efforts toward a more Department-wide enterprise net-centric approach, including expansion of the Distributed Common Ground System.
- Restructure the Transformational Satellite (TSAT) program to "spiral develop" its capabilities and re-phase launches accordingly, and add resources to increase space-based relay capacity.
- Develop an integrated approach to ensure alignment in the phasing and pacing of terminals and space vehicles.
- Develop a new bandwidth requirements model to determine optimal network size and capability to best support operational forces.

SOURCE: U.S. Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C.: Government Printing Office, 2006), 58–59, https://archive.defense.gov/pubs/pdfs/QDR20060203.pdf

ANALYSIS

It is clear from this segment of the 2006 QDR that the DOD had not yet begun to make cyber warfare a priority. In part, this was due to the ongoing conflicts in Afghanistan and Iraq—less than a year later, President Bush commenced the Iraq War troop surge, which is often credited for turning the tide of the insurgency. Other elements of the 2006 QDR are concerned with increasing the amount of special operations forces available, improving the departmental budgeting process, and renewing the department's focus on joint operations. Interestingly, this segment of the QDR also illustrates that in 2006, the leaders of the DOD had effectively lumped together cyber operations and the military usage of outer space, in large part due to the amount of communications capability being routed through satellites. By combining the two disparate elements, the DOD actually hindered the successful

development of either capability as the two military communities had little in common and no real means to reconcile their differences.

- ***Document 11:*** *National Defense Strategy*
- ***When:*** June 2008
- ***Where:*** Washington, D.C.
- ***Significance:*** This was the first National Defense Strategy released after the troop surge in Iraq in 2007. Thus, it was able to address the changed security situation caused by the infusion of tens of thousands of fresh troops. It was produced when al Qaeda had sustained enormous losses, but Osama bin Laden remained in hiding, making it a dangerous nonstate adversary. When this National Defense Strategy was released, NATO ally Estonia had suffered a devastating campaign of cyberattacks, ostensibly from Russian sources, demonstrating the utility of such mass attacks through the internet.

DOCUMENT

Future Challenges Risk

An underlying assumption in our understanding of the strategic environment is that the predominant near-term challenges to the United States will come from state and non-state actors using irregular and catastrophic capabilities. Although our advanced space and cyber-space assets give us unparalleled advantages on the traditional battlefield, they also entail vulnerabilities.

China is developing technologies to disrupt our traditional advantages. Examples include development of anti-satellite capabilities and cyber warfare. Other actors, particularly non-state actors, are developing asymmetric tactics, techniques, and procedures that seek to avoid situations where our advantages come into play.

The Department will invest in hedging against the loss or disruption of our traditional advantages, not only through developing mitigation strategies, but also by developing alternative or parallel means to the same end. This diversification parallelism is distinct from acquiring overmatch capabilities (whereby we have much more than an adversary of a similar capability). It will involve pursuing multiple routes to similar effects while ensuring that such capabilities are applicable across multiple mission areas.

SOURCE: U.S. Department of Defense, *National Defense Strategy* (Washington, D.C.: Government Printing Office, 2008), 22, https://history.defense.gov/Portals/70/Documents/nds/2008_NDS.pdf?ver=2014-06-25-124535-363

ANALYSIS

Interestingly, despite the obvious proof that cyberattacks can result in enormous disruptive effects, as demonstrated in the attacks on Estonia in 2007, the DOD essentially sidelined all discussions of cyber capabilities in its 2008 National Defense Strategy. In part, this might reflect a greater desire to maintain secrecy over the department's cyber capabilities—in succeeding years, cyber operations became increasingly likely to be subjected to classification, making them inaccessible to most of the public. However, this might also simply reflect that the department was so focused on completing the ongoing conflicts with Afghanistan and Iraq that it lost interest in predicting the nature of future conflicts.

- ***Document 12:*** *National Security Strategy*
- ***When:*** May 2010
- ***Where:*** Washington, D.C.
- ***Significance:*** The 2010 National Security Strategy was the first opportunity for President Barack Obama to offer his guidance to all the executive agencies tasked with national security, which then subsequently cooperated to develop the next iteration of the National Defense Strategy. In particular, the DOD utilized this guidance to create its National Military Strategy. Key threats to the nation included the ongoing struggles in Afghanistan and Iraq, the rise of new violent extremist organizations, and the possibility of a nuclear-armed Iran.

DOCUMENT

III. Advancing Our Interests
Security
Secure Cyberspace

Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority, but our unclassified government networks are constantly probed by intruders. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. The internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property.

DID YOU KNOW?

Classified Networks

The U.S. Department of Defense (DoD) operates several different network systems, with separate networks established for different levels of classified material. The Non-classified Internet Protocol Router Network (NIPRNet) is the primary computer network of the U.S. DoD, and handles the bulk of DoD communications on a daily basis. It is directly connected to the public internet, allowing DoD personnel to access some, but not all, of the websites available around the globe. There is a NIPRNet Federated Gateway system that serves to protect the network as a whole against malware and illicit websites. The Secret Internet Protocol Router Network (SIPRNet) is used to transmit information at the "Secret" level, meaning information that could be expected to cause substantial harm to national security if it is improperly disclosed. Access to the SIPRNet is strictly controlled—only members holding sufficient clearance may access the network, and they are required to utilize designated terminals that are hard-wired to the network. Although the SIPRNet has a stronger set of defensive protocols, it is not immune to malware and bad actors—the vast majority of Chelsea Manning's 2010 leak of classified materials to WikiLeaks came through the SIPRNet access Private Manning possessed. The Joint Worldwide Intelligence Communications System (JWICS) is used for the transfer of Top Secret information. Although it is administered by the Defense Information Services Agency, it is used by several other federal agencies, including the Department of Homeland Security, the Department of Justice, and the Department of State. Access to JWICS is strictly controlled, although it was also utilized by Private Manning to disclose classified material.

The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states. Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient. Our digital infrastructure, therefore, is a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority. We will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by:

Investing in People and Technology: To advance that goal, we are working across the government and with the private sector to design more secure technology that gives us the ability to better protect and to improve the resilience of critical government and industry systems and networks. We will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet these challenges. We have begun a comprehensive national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and to build a digital workforce for the 21st century.

Strengthening Partnerships: Neither government nor the private sector nor individual citizens can meet this challenge alone—we will expand the ways we work together. We will also strengthen our international partnerships on a range of issues, including the development of norms for acceptable conduct in cyberspace; laws concerning cybercrime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks. We will work with all the key players—including all levels of government and the private sector, nationally and internationally—to investigate cyber intrusion and to ensure an organized and unified response to future cyber incidents. Just as we do for natural disasters, we have to have plans and resources in place beforehand.

SOURCE: Barack Obama, *National Security Strategy* (Washington, D.C.: Government Printing Office, 2010), 27–28, http://nssarchive.us/NSSR/2010.pdf

ANALYSIS

This document demonstrates a fairly solid grasp of the wide varieties of cyber threats that might challenge the national security of the United States, as well as the need for public-private sector cooperation to meet those threats. However, it

does little to illustrate who actually holds responsibility for cyber defense within the United States, much less which agencies might be tasked with carrying out cyber-attacks on behalf of the nation. National Security Strategy documents of this type tend to be somewhat vague, but in this example, there is almost nothing to suggest that the federal government possessed a coherent plan for cybersecurity at the national level.

- ***Document 13:*** *Quadrennial Defense Review Report*
- ***When:*** February 2010
- ***Where:*** Washington, D.C.
- ***Significance:*** This was the first QDR conducted during the Obama administration. Secretary of Defense Robert M. Gates, who had been appointed to his role by President George W. Bush, remained in the position under President Obama, providing much-needed continuity to the department as it sought to end the conflicts in Afghanistan and Iraq. Fifteen months after the 2010 QDR, U.S. Navy SEALs raided a compound in Pakistan and killed Osama bin Laden, the secretive head of al Qaeda.

DOCUMENT

Rebalancing the Force

This QDR has explicitly linked force planning, which determines the overall size and capabilities of the Armed Forces, to the priority objectives of the defense strategy: prevail in today's wars; prevent and deter conflict; prepare to succeed in a wide range of contingencies, both near- and longer-term; and preserve and enhance the force. The QDR developed insights regarding the ways in which the capabilities of U.S. forces should evolve by evaluating alternative future forces in a diverse set of scenarios, which depicted a wide range of plausible challenges that might call for a response by U.S. military forces. The Department also assessed lessons learned from ongoing operations in Iraq, Afghanistan, and elsewhere. Collectively, these assessments helped inform decisions affecting capabilities in six key mission areas:

- Defend the United States and support civil authorities at home;
- Succeed in counterinsurgency, stability, and counterterrorism operations;
- Build the security capacity of partner states;
- Deter and defeat aggression in anti-access environments;
- Prevent proliferation and counter weapons of mass destruction; and
- Operate effectively in cyberspace.

. . .

Operate Effectively in Cyberspace

Our assessments of conflict scenarios involving state adversaries pointed to the need for improved capabilities to counter threats in cyberspace—a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the internet and telecommunication networks. Although it is a manmade domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space. There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace.

It is therefore not surprising that DoD's information networks have become targets for adversaries who seek to blunt U.S. military operations. Indeed, these networks are infiltrated daily by a myriad of sources, ranging from small groups of individuals to some of the largest countries in the world. For example, criminals may try to access DoD's healthcare systems in order to obtain personal information to perpetrate identity theft. Terrorists may seek to disrupt military networks and systems to cause chaos and economic damage. Foreign intelligence or military services may attempt to alter data in DoD databases to hinder our military's ability to operate effectively. DoD must actively defend its networks.

This is no small task. DoD currently operates more than 15,000 different computer networks across 4,000 military installations around the world. On any given day, there are as many as seven million DoD computers and telecommunications tools in use in 88 countries using thousands of warfighting and support applications. The number of potential vulnerabilities, therefore, is staggering. Moreover, the speed of cyber attacks and the anonymity of cyberspace greatly favor the offense. This advantage is growing as hacker tools become cheaper and easier to employ by adversaries whose skills are growing in sophistication.

We must therefore be constantly vigilant and prepared to react nearly instantaneously if we are to effectively limit the damage that the most sophisticated types of attacks can inflict. In this environment, the need to develop strategies, policies, authorities, and capabilities for DoD to manage and defend its information networks is manifest.

DoD is taking a number of steps to strengthen its capabilities in the cyberspace:

- *Develop a comprehensive approach to DoD operations in cyberspace*. A Department-wide comprehensive approach will help build an environment in which cyber security and the ability to operate effectively in cyberspace are viewed as priorities for DoD. Strategies and policies to improve cyber defense in depth, resiliency of networks, and surety of data and communication will allow DoD to continue to have confidence in its cyberspace operations. A central component of this approach is cultural and organizational: The Department will adapt and improve operational planning, its networks,

its organizational structures, and its relationships with interagency, industry, and international partners. New operational concepts, such as dynamic network defense operations, could enhance effectiveness by enabling more rapid actions and more comprehensive actions to protect DoD's networks.

- *Develop greater cyberspace expertise and awareness*. The Department will redouble its efforts to imbue its personnel with a greater appreciation for the threats and vulnerabilities in the cyber domain and to give them the skills to counter those threats and reduce those vulnerabilities at the user and system administrator levels. DoD can no longer afford to have users think of its information technologies and networks as simply the benign infrastructure that facilitates their work. Users and managers must be held accountable for ensuring network security and for implementing best practices. DoD is also growing its cadre of cyber experts to protect and defend its information networks and is investing in and developing the latest technologies to enable our forces to operate in cyberspace under a wide range of conditions, including in contested and degraded environments.
- *Centralize command of cyberspace operations*. In an effort to organize and standardize cyber practices and operations more effectively, the Department is standing up U.S. Cyber Command (USCYBERCOM), a subunified command under U.S. Strategic Command, to lead, integrate and better coordinate the day-to-day defense, protection, and operation of DoD networks. USCYBERCOM will direct the operation and defense of DoD's information networks, and will prepare to, and when directed, conduct full spectrum cyberspace military operations. An operational USCYBERCOM will also play a leading role in helping to integrate cyber operations into operational and contingency planning. In addition, DoD is training cyber experts, equipped with the latest technologies, to protect and defend its information networks. Essential to the success of this new approach will be the capabilities and growth of the Service components that are stood up to support USCYBERCOM.
- *Enhance partnerships with other agencies and governments*. Freedom of operation in cyberspace is important and DoD must have the capabilities to defend its own networks. However, the interdependence of cyberspace means DoD networks are heavily dependent on commercial infrastructure. Just as it does in conducting many of our missions, DoD needs to collaborate with other U.S. departments and agencies and international partners both to support their efforts and to ensure our ability to operate in cyberspace. This mutual assistance includes information sharing, support for law enforcement, defense support to civil authorities, and homeland defense. In particular, DoD will strengthen its cooperation with DHS, which leads the national effort to protect federal information systems.

SOURCE: U.S. Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C.: Government Printing Office, 2010), 17, 37–39, https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf

ANALYSIS

For the first time, the 2010 QDR demonstrated that the DOD was taking cyber warfare seriously—in large part due to a series of massive cyber espionage campaigns carried out against DOD networks that had been recently exposed. The massive vulnerabilities of military cyber networks to infiltration and exploitation by competitor nations came as a shock to the departmental leadership, which realized that while there might be little cyber threat from weaker states that the United States had faced in recent conflicts, any future engagement with Russia or China was likely to include substantially larger amounts of cyber operations. Further, the newly discovered espionage operations had largely focused on stealing the technical details for new weapons systems that had been expected to provide a major technological edge for the United States—an edge that could no longer be assumed when envisioning future conflicts. It was clear that the military needed to place greater emphasis upon cyber operations, what was unclear was precisely how the department might go about such activities.

- ***Document 14:*** *The National Military Strategy of the United States of America: Redefining America's Military Leadership*
- ***When:*** 2011
- ***Where:*** Washington, D.C.
- ***Significance:*** The 2011 edition of the National Military Strategy was the first iteration released under the Obama administration. President Obama entered office having pledged to end America's wars in Afghanistan and Iraq, both of which he considered ruinously expensive with very little utility for U.S. national security. This military strategy placed much greater emphasis on preserving U.S. access to the global commons and recognizing the importance of maintaining allied relationships.

DOCUMENT

II. Strategic Environment

Global Commons and Globally Connected Domains—Assured access to and freedom of maneuver within the global commons—shared areas of sea, air, and space—and globally connected domains such as cyberspace are being increasingly challenged by both state and non-state actors. Non-state actors such as criminal organizations, traffickers, and terrorist groups find a nexus of interests in exploiting the commons. States are developing anti-access and area-denial capabilities and strategies to

constrain U.S. and international freedom of action. These states are rapidly acquiring technologies, such as missiles and autonomous and remotely-piloted platforms that challenge our ability to project power from the global commons and increase our operational risk. Meanwhile, enabling and war-fighting domains of space and cyberspace are simultaneously more critical for our operations, yet more vulnerable to malicious actions. The space environment is becoming more congested, contested, and competitive. Some states are conducting or condoning cyber intrusions that foreshadow the growing threat in this globally connected domain. The cyber threat is expanded and exacerbated by lack of international norms, difficulties of attribution, low barriers to entry, and the relative ease of developing potent capabilities.

. . .

Enduring National Interests and National Military Objectives
Deter and Defeat Aggression

Preventing wars is as important as winning them, and far less costly. A prosperous and interconnected world requires a stable and secure environment, the absence of territorial aggression or conflict between states, and reliable access to resources and cyberspace for stable markets. Conventional or unconventional conflict between states interrupts commerce and triggers market volatility. Instantaneous information systems and the global economy's interconnectedness exacerbate and amplify these effects. In our role as security guarantor, and in concert with our allies and partners whenever possible, the Joint Force will be prepared to deter and defeat regional aggression that would threaten our national interests.

Deter Aggression: The United States seeks the peace and security of a world without nuclear weapons. However, as long as nuclear weapons exist, deterring nuclear attack on the United States, our allies, and partners will continue to be the fundamental role of U.S. nuclear weapons. In support of the President's vision, we will reduce the role and numbers of nuclear weapons, while maintaining a safe, secure, and effective strategic deterrent. The Joint Force will provide capabilities to deter aggression and assure our allies and partners through our nuclear arsenal and overseas missile defense capabilities. We will continue to lead in advancing Ballistic Missile Defense capabilities against limited attacks and we seek opportunities for cooperation with allies and partners in this area.

We will counter WMD proliferation as it presents a grave and common threat to our Nation and others. Working through institutions, alliances and coalitions, we will dismantle proliferation networks, interdict movement of materials, further improve nuclear forensics capabilities, and secure nuclear, chemical, and biological materials worldwide. We will help allies and

DID YOU KNOW?

Cyber Equivalence Doctrine

In 2011, the U.S. government announced for the first time that it considered cyberattacks to be on a spectrum of aggressive actions that might constitute an act of war. Further, the U.S. government reserved the right to respond to cyberattacks in kind or to utilize other forms of retaliation from elsewhere on the spectrum. Dubbed the Cyber Equivalence Doctrine, this announcement had the effect of moving cyber activities into the realm of acts of war. While such a pronouncement carried a provocative effect, it also probably provided a deterrent to some states considering cyberattacks against U.S. interests. Of course, such a deterrent effect depends in large part upon the credibility of the United States—which may or may not choose to escalate in response to a cyberattack by retaliating in the kinetic domain. Also, in order to respond effectively and justifiably to a cyberattack, the U.S. government would need to be absolutely sure about the correct attribution for the attack, lest it launch a retaliatory strike upon an innocent bystander nation.

partners to develop WMD detection and elimination capabilities to protect their own populations. Combatant Commanders shall conduct prudent planning and be prepared to eliminate sources of WMD, providing the President with an array of options for military action when and where necessary.

We must also maintain a robust conventional deterrent. Deterrence and assurance requires the ability to rapidly and globally project power in all domains. In turn, force posture—both rotational and forward based—shall be geographically distributed, operationally resilient, and politically sustainable through visible partnering efforts.

We will support whole-of-nation deterrence approaches that blend economic, diplomatic, and military tools to influence adversary behavior. Denying an aggressor the benefits of achieving its objectives can be just as effective as in altering its strategic calculus through the threat of retaliation. The most effective deterrence approaches make use of both techniques, while also providing potential adversaries acceptable alternative courses of action.

We must also adapt deterrence principles to 21st century security challenges. We will enhance deterrence in air, space, and cyberspace by possessing the capability to fight through a degraded environment and improving our ability to attribute and defeat attacks on our systems or supporting infrastructure.

Defeat Aggression: The core task of our Armed Forces remains to defend our Nation and win its wars. To do so, we must provide capabilities to defeat adversary aggression. Military force, at times, may be necessary to defend our Nation and allies or to preserve broader peace and security. Seeking to adhere to international standards, the United States will use military force in concert with allies and partners whenever possible, while reserving the right to act alone if necessary. Across a wide range of contingencies, military leaders will provide our Nation's leadership with options of how the military can help achieve the Nation's objectives.

Defeating adversary aggression will require the Joint Force to support National approaches to counter anti-access and area-denial strategies. Anti-access strategies seek to prevent our Nation's ability to project and sustain combat power into a region, while area denial strategies seek to constrain our Nation's freedom of action within the region. Defeating these strategies will require Joint Force doctrine to better integrate core military competencies across all domains and account for geographic considerations and constraints. These core military competencies include complementary, multi-domain power projection, joint forcible entry, the ability to maintain joint assured access to the global commons and cyberspace should they become contested, and the ability to fight and win against adversaries.

Joint assured access to the global commons and cyberspace constitutes a core aspect of U.S. national security and remains an enduring mission for the Joint Force. The global commons and globally connected domains constitute the connective tissue upon which all nations' security and prosperity depend. The maritime domain enables the bulk of the joint force's forward deployment and sustainment, as well as the commerce that underpins the global economic system. The interlinked domains of air, space, and cyberspace allow for the high-speed, high-volume exchange of people, ideas, goods, information and capital that are equally critical to the global economy. These collective domains are essential and interdependent mediums for

the Joint Force's projection and sustainment of power and ability to deter and defeat aggression.

In support of our Nation's interests, the Joint Force will take a strong role in international efforts to safeguard access, sustain security, provide oversight and accountability, and promote responsible norms in the global commons and cyberspace. The Joint Force will adhere to conventions, laws, and regulations our Nation supports to underpin collective security and govern conduct. We will also facilitate cooperation in the commons and cyberspace with transparent, routine, and predictable practices as part of our theater strategies.

Our ability to operate effectively in space and cyberspace, in particular, is increasingly essential to defeating aggression. The United States faces persistent, widespread, and growing threats from state and non-state actors in space and cyberspace. We must grow capabilities that enable operations when a common domain is unusable or inaccessible. Space and cyberspace enable effective global warfighting in the air, land, and maritime domains, and have emerged as war-fighting domains in their own right.

- *Space*—We will support whole-of-nation approaches to establishing and promoting norms, enhancing space situational awareness, and fostering greater transparency and information sharing. We will work with allies and partners to enhance space capabilities enabling coalitions and improving space architecture resiliency. We will also train for power projection operations in space-degraded environments that minimize the incentives to attack space capabilities, and will maintain a range of options to deter or punish such activities.
- *Cyberspace*—Cyberspace capabilities enable Combatant Commanders to operate effectively across all domains. Strategic Command and Cyber Command will collaborate with U.S. government agencies, nongovernment entities, industry, and international actors to develop new cyber norms, capabilities, organizations, and skills. Should a large-scale cyber intrusion or debilitating cyber attack occur, we must provide a broad range of options to ensure our access and use of the cyberspace domain and hold malicious actors accountable. We must seek executive and Congressional action to provide new authorities to enable effective action in cyberspace.

SOURCE: U.S. Department of Defense, *The National Military Strategy of the United States of America: Redefining America's Military Leadership* (Washington, D.C.: Government Printing Office, 2011), 3–4, 7–10, https://dod.defense.gov/Portals/1/Documents/pubs/2011-National-Military-Strategy.pdf

ANALYSIS

President Obama greatly emphasized on deterrence—a posture designed to discourage any form of aggression against the United States, its interests, and its allies. Of course, if deterrence failed, the U.S. military needed to be prepared to engage in conflict to punish aggression—a stance that implies that the United States would

not adopt the pose of the aggressor in global affairs. The war in Afghanistan was not a war of choice as it was triggered by the September 11 attacks. However, the war in Iraq, which was much more costly in terms of lives and resources, was certainly a conflict that could have been avoided or delayed if the Bush administration had chosen to do so. President Obama entered office wanting to reassure peer competitors that the United States would not utilize military force when other elements of national power might be more successful. Yet, he also wished to clarify that potential aggressors should not confuse restraint with weakness—lest they be undeterred out of a belief that the United States might not respond to aggressive moves.

- ***Document 15:*** *International Strategy for Cyberspace*
- ***When:*** May 2011
- ***Where:*** Washington, D.C.
- ***Significance:*** The 2011 U.S. strategy for cyberspace illustrated the federal government's understanding of the needs of the international cyberspace community and how nations interact through the cyber domain. This document, released to the public, called for free and open access to the internet for all people in the world—a guaranteed way to upset the totalitarian regimes of rival nations, and an interesting position to take a few months after the commencement of the Arab Spring protests of 2010.

DOCUMENT

The Future We Seek

The cyberspace environment that we seek rewards innovation and empowers individuals; it connects individuals and strengthens communities; it builds better governments and expands accountability; it safeguards fundamental freedoms and enhances personal privacy; it builds understanding, clarifies norms of behavior, and enhances national and international security. To sustain this environment, international collaboration is more than a best practice, it is a first principle.

Our Goal

The United States will work internationally to promote an **open, interoperable, secure, and reliable** information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which **norms of responsible behavior** guide states' actions, sustain partnerships, and support the rule of law in cyberspace.

Open and Interoperable: A Cyberspace That Empowers

At the core of digital innovation is the ability to add new functionality to networked machines. The openness of digital systems explains their explosive growth, rapid development, and enduring importance. Networked technology's basic tools are steadily increasing in availability and decreasing in price, as computer and internet access have spread to every nation. To continue to serve the needs of an ever-growing wired population, manufacturers of hardware and operating systems must continue to empower the widest possible range of developers across the globe. As companies continue to drive innovation in the development of proprietary software, we also applaud the vibrancy of the open-source software movement, giving developers and consumers the choice of community-driven solutions to meet their needs.

The United States supports an internet with end-to-end interoperability, which allows people worldwide to connect to knowledge, ideas, and one another through technology that meets their needs. The free flow of information depends on interoperability—a principle affirmed by 174 nations in the Tunis Commitment of the World Summit on the Information Society. The alternative to global openness and interoperability is a fragmented internet, where large swaths of the world's population would be denied access to sophisticated applications and rich content because of a few nations' political interests. The collaborative development of consensus-based international standards for information and communication technology is a key part of preserving openness and interoperability, growing our digital economies, and moving our societies forward.

Secure and Reliable: A Cyberspace That Endures

For cyberspace as we know it to endure, our networked systems must retain our trust. Users need to have confidence that their data will be secure in transit and storage, as well as reliable in delivery. An effective strategy will require action on many fronts, with shared responsibility at every level of society, from the end-user up through collaboration among nation-states.

Vulnerability reduction will require robust technical standards and solutions, effective incident management, trustworthy hardware and software, and secure supply chains. Risk reduction on a global scale will require effective law enforcement; internationally agreed norms of state behavior; measures that build confidence and enhance transparency; active, informed diplomacy; and appropriate deterrence. Finally, incident response will require increased collaboration and technical information sharing with the private sector and international community. This work cannot be fully addressed by any single nation or sector alone; it is a responsibility and duty that every nation, and its people, all share.

Network stability is a cornerstone of our global prosperity, and securing those networks is more than strictly a technical matter. Economically, we must advance sustainable growth and invest in infrastructure at home and abroad, while incentivizing network reliability and clarifying the obligations of firms and states. Politically, we must help to maintain an environment of respect for technical infrastructure, so disputes do not become excuses to disrupt and degrade networks. Socially, we must make end-users aware of their responsibilities to maintain and operate their devices in a safe and secure manner.

Stability Through Norms

The United States will work with like-minded states to establish an environment of expectations, or norms of behavior, that ground foreign and defense policies and guide international partnerships. The last two decades have seen the swift and unprecedented growth of the internet as a social medium; the growing reliance of societies on networked information systems to control critical infrastructures and communications systems essential to modern life; and increasing evidence that governments are seeking to exercise traditional national power through cyberspace. These events have not been matched by clearly agreed-upon norms for acceptable state behavior in cyberspace. To bridge that gap, we will work to build a consensus on what constitutes acceptable behavior, and a partnership among those who view the functioning of these systems as essential to the national and collective interest.

The Role of Norms. In other spheres of international relations, shared understandings about acceptable behavior have enhanced stability and provided a basis for international action when corrective measures are required. Adherence to such norms brings predictability to state conduct, helping prevent the misunderstandings that could lead to conflict.

The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these terms apply and what additional understandings might be necessary to supplement them. We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace.

The Basis for Norms. Rules that promote order and peace, advance basic human dignity, and promote freedom in economic competition are essential to any international environment. These principles provide a basic roadmap for how states can meet their traditional international obligations in cyberspace and, in many cases, reflect duties of states that apply regardless of context. The existing principles that should support cyberspace norms include:

- **Upholding Fundamental Freedoms:** States must respect fundamental freedoms of expression and association, online as well as off.
- **Respect for Property:** States should in their undertakings and through domestic laws respect intellectual property rights, including patents, trade secrets, trademarks, and copyrights.
- **Valuing Privacy:** Individuals should be protected from arbitrary or unlawful state interference with their privacy when they use the internet.
- **Protection from Crime:** States must identify and prosecute cybercriminals, to ensure laws and practices deny criminals safe havens, and cooperate with international criminal investigations in a timely manner.

– **Right of Self-Defense:** Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace.

Deriving from these traditional principles of interstate conduct are responsibilities more specific to cyberspace, focused in particular on preserving global network functionality and improving cybersecurity. Many of these responsibilities are rooted in the technical realities of the internet. Because the internet's core functionality relies on systems of trust (such as the Border Gateway Protocol), states need to recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader internet. Likewise, in designing the next generation of these systems, we must advance the common interest by supporting the soundest technical standards and governance structures, rather than those that will simply enhance national prestige or political control. Emerging norms, also essential to this space, include:

– **Global Interoperability:** States should act within their authorities to help ensure the end-to-end interoperability of an internet accessible to all.
– **Network Stability:** States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure.
– **Reliable Access:** States should not arbitrarily deprive or disrupt individuals' access to the internet or other networked technologies.
– **Multi-stakeholder Governance:** Internet governance efforts must not be limited to governments, but should include all appropriate stakeholders.
– **Cybersecurity Due Diligence:** States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse.

While cyberspace is a dynamic environment, international behavior in it must be grounded in the principles of responsible domestic governance, peaceful interstate conduct, and reliable network management. As these ideas develop, the United States will foster and participate fully in discussions, advancing a principled approach to internet policy-making and developing shared understandings appropriate to each issue.

. . .

Defense: Dissuading and Deterring

The United States will defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies. Just as importantly, we will seek to encourage good actors and dissuade and deter those who threaten peace and stability through actions in cyberspace. We will do so with overlapping policies that combine national and international network resilience with vigilance and a range of credible response options. In all our defense endeavors, we will protect civil liberties and privacy in accordance with our laws and principles.

Defense Objective

The United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate.

Dissuasion

Protecting networks of such great value requires robust defensive capabilities. The United States will continue to strengthen our network defenses and our ability to withstand and recover from disruptions and other attacks. For those more sophisticated attacks that do create damage, we will act on well-developed response plans to isolate and mitigate disruption to our machines, limiting effects on our networks, and potential cascade effects beyond them.

Strength at Home. Ensuring the resilience of our networks and information systems requires collective and concerted national action that spans the whole of government, in collaboration with the private sector and individual citizens. For a decade, the United States has been fostering a culture of cybersecurity and an effective apparatus for risk mitigation and incident response. We continue to emphasize that systematically adopting sound information technology practices—across the public and private sectors—will reduce our Nation's vulnerabilities and strengthen networks and systems. We are also making steady progress towards shared situational awareness of network vulnerabilities and risks among public and private sector networks. We have built new initiatives through our national computer security incident response team to share information among government, key industries, our critical infrastructure sectors, and other stakeholders. And we continually seek new ways to strengthen our partnership with the private sector to enhance the security of the systems on which we both rely.

Strength Abroad. This model of defense has been successfully shared internationally through education, training and ongoing operational and policy relationships. Today, through existing and developing collaborations in the technical and military defense arenas, nations share an unprecedented ability to recognize and respond to incidents—a crucial step in denying would-be attackers the ability to do lasting damage to our national and international networks. However, a globally distributed network requires globally distributed early warning capabilities. We must continue to produce new computer security incident response capabilities globally, and to facilitate their interconnection and enhanced computer network defense. The United States has a shared interest in assisting less developed nations to build capacity for defense, and in collaboration with our partners, will intensify our focus on this area. Building relationships with friends and allies will increase collective security across the international community.

Deterrence

The United States will ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits. We fully recognize that cyberspace activities can have effects extending beyond networks; such events may

require responses in self-defense. Likewise, interconnected networks link nations more closely, so an attack on one nation's networks may have impact far beyond its borders.

In the case of criminals and other non-state actors who would threaten our national and economic security, domestic deterrence requires all states have processes that permit them to investigate, apprehend, and prosecute those who intrude or disrupt networks at home and abroad. Internationally, law enforcement organizations must work in concert with one another whenever possible to freeze perishable data vital to ongoing investigations, to work with legislatures and justice ministries to harmonize their approaches, and to promote due process and the rule of law—all key tenets of the Budapest Convention on Cybercrime.

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.

. . .

Military: Preparing for 21st Century Security Challenges

Since our commitment to defend our citizens, allies, and interests extends to wherever they might be threatened, we will:

- **Recognize and adapt to the military's increasing need for reliable and secure networks.** We recognize that our armed forces increasingly depend on the networks that support them, and we will work to ensure that our military remains full equipped to operate even in an environment where others might seek to disrupt its systems, or other infrastructure vital to national defense. Like all nations, the United States has a compelling interest in defending its vital national assets, as well as our core principles and values, and we are committed to defending against those who would attempt to impede our ability to do so.
- **Build and enhance existing military alliances to confront potential threats in cyberspace.** Cybersecurity cannot be achieved by any one nation alone, and greater levels of international cooperating are needed to confront those actors who would seek to disrupt or exploit our networks. This effort begins by acknowledging that the interconnected nature of networked systems of our closest allies, such as those of NATO and its member states, creates opportunities and new risks. Moving forward, the United States will continue to work with the militaries and civilian counterparts of our allies

and partners to expand situational awareness and shared warning systems, enhance our ability to work together in times of peace and crisis, and develop the means and method of collective self-defense in cyberspace. Such military alliances and partnerships will bolster our collective deterrence capabilities and strengthen our ability to defend the United States against state and non-state actors.

– **Expand cyberspace cooperation with allies and partners to increase collective security.** The challenges of cyberspace also create opportunities to work in new ways with allied and partner militaries. By developing a shared understanding of standard operating procedures, our armed forces can enhance security through coordination and greater information exchange; these engagements will diminish misperceptions about military activities and the potential for escalatory behavior. Dialogues and best practice exchanges to enhance partner capabilities, such as digital forensics, work force development, and network penetration and resiliency testing will be important to this effort. The United States will work in close partnership with like-minded states to leverage capabilities, reduce collective risk, and foster multi-stakeholder initiatives to deter malicious activities in cyberspace.

. . .

Moving Forward

The benefits of networked technology should not be reserved to a privileged few nations, or a privileged few within them. But connectivity is no end unto itself; it must be supported by a cyberspace that is open to innovation, interoperable the world over, secure enough to earn people's trust, and reliable enough to support their work.

Thirty years ago, few understood that something called the internet would lead to a revolution in how we work and live. In that short time, millions now owe their livelihoods—and even their lives—to advances in networked technology. A billion more rely on it for everyday forms of social interaction. This technology propels society forward, accomplishing things previous generations scarcely thought possible. For our part, the United States will continue to spark the creativity and imagination of our people, and those around the world. We cannot know what the next great innovation will be, but are committed to realizing a world in which it can take shape and flourish.

This strategy is a roadmap allowing the United States Government's departments and agencies to better define and coordinate their role in our international cyberspace policy, to execute a specific way forward, and to plan for future implementation. It is a call to the private sector, civil society, and end-users to reinforce these efforts through partnership, awareness, and action. Most importantly, it is an invitation to other states and peoples to join us in realizing this vision of prosperity, security, and openness in our networked world. These ideals are central to preserving the cyberspace we know, and to creating, together, the future we seek.

SOURCE: Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, D.C.: Government Printing Office, 2011), 8–14, 20–21, 25, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

ANALYSIS

The 2011 cyber strategy was the first document of its kind in U.S. history. By effectively treating the cyber domain, and the military units tasked with operations within it, as a separate entity from the remainder of the military, President Obama served notice that cyber units would be essentially coequal with the formal branches of the DOD. Further, by clearly and explicitly stating the U.S. positions on the need for cyber norms regarding the behavior of nations, the United States sought to provoke such a conversation among the international community. Of course, if the positions staked out in this document were accepted and adhered to by the rest of the world, it would create an inherent advantage for the United States, as it would reframe the cyber domain as a conflict-free zone, where states did not interfere with each others' networks, data, or infrastructure. Given that the United States is by far the most targeted nation in cyberspace, any reduction of cyberattacks, particularly by nation-states, would make the U.S. cyber defense challenge substantially easier.

- ***Document 16:*** *Quadrennial Defense Review*
- ***When:*** March 2014
- ***Where:*** Washington, D.C.
- ***Significance:*** By 2014, President Obama had ordered almost a complete withdrawal from Iraq, and had refocused the U.S. military on completing the Afghanistan mission. Budgetary fights in the legislature led to a 2013 sequestration, by which the military was subjected to automatic budget cuts whenever a budget could not be passed. Such cuts created extreme strain on the DOD, and were warningly referenced throughout the QDR. After more than two decades of relative quiet from peer competitors after the end of the Cold War, the Obama administration confronted a resurgent Russian Federation, which launched a military campaign to annex the Crimean Peninsula from Ukraine just as the 2014 QDR was released. Like other recent Russian conflicts with neighboring states, the Ukraine campaign included a substantial amount of cyber activity from both sides.

DOCUMENT

Pillars of the U.S. Defense Strategy

Protect the Homeland

As the frequency and complexity of cyber threats grow, we will continue to place high priority on cyber defense and cyber capabilities. The Department of Defense will deter, and when approved by the President and directed by the Secretary of Defense, will disrupt and deny adversary cyberspace operations that threaten U.S. interests. To do so, we must be able to defend the integrity of our own networks, protect our key systems and networks, conduct effective cyber operations overseas when directed, and defend the Nation from an imminent, destructive cyberattack on vital U.S. interests. U.S. forces will abide by applicable laws, policies, and regulations that protect the privacy and civil liberties of U.S. persons. Further, the Department will operate consistent with the policy principles and legal frameworks associated with the law of war.

Deterring and defeating cyber threats requires a strong, multi-stakeholder coalition that enables the lawful application of the authorities, responsibilities, and capabilities resident across the U.S. Government, industry, and international allies and partners. We support the Federal government cybersecurity team and will continue working with the Department of Homeland Security (DHS) to improve critical infrastructure cybersecurity, and with DHS and the Federal Bureau of Investigation to support law enforcement activities. The Department of Defense remains committed to working with industry and international partners as well, sharing threat information and capabilities to protect and defend U.S. critical infrastructure, including in our role as the sector-specific agency for the defense industrial base. We will ensure that international alliances and partnerships remain relevant to challenges in the threat environment by helping these partners improve their own cyber defense capabilities and mitigate shared cyber threats through mutual action.

. . .

Protecting Key Priorities

Protect the Homeland

Cyber. The Department of Defense will continue to invest in new and expanded cyber capabilities, building on significant progress made in recent years in recruiting, training, and retaining cyber personnel. A centerpiece of our efforts is the development of the Department of Defense Cyber Mission Force. The Force includes Cyber Protection Forces that operate and defend the Department's networks and support military operations worldwide, Combat Mission Forces that support Combatant Commanders as they plan and execute military missions, and National Mission Forces that counter cyberattacks against the United States. The Cyber Mission Force will be manned by 2016. In addition to personnel, the Department is investing in state-of-the-art tools and infrastructure to conduct its missions. To defend its own networks, the Department is also migrating its information systems to a common, Defense-wide network infrastructure known as the Joint Information Environment (JIE). This JIE is critical to developing a more defensible network architecture and to improving network operations. The Department also will continue working with other U.S. departments and agencies, as well as with allies and partners abroad, to build their own cyber defense capabilities and mitigate shared cyber risks.

. . .

Main Elements of Planned U.S. Force Structure and End Strength, FY2019

Cyber Mission Forces

13 National Mission Teams (NMTs) with 8 National Support Teams (NSTs)
27 Combat Mission Teams (CMTs) with 17 Combat Support Teams (CSTs)
18 National Cyber Protection Teams (CPTs)
24 Service CPTs
26 Combatant Command and DOD Information Network CPTs

SOURCE: U.S. Department of Defense, *Quadrennial Defense Review* (Washington, D.C.: Government Printing Office, 2014), 14–15, 32–33, 41, https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/2014_Quadrennial_Defense_Review.pdf

ANALYSIS

The 2014 QDR was the first iteration to lay out specific manpower goals for the creation of a cyber force. This envisioned force was separated from each of the branches of service, signifying that it had taken on the cyber role in a joint fashion but also suggesting that it might become a separate branch of the military at some future point. Further, the QDR's emphasis on cyber defense as a key element of protecting the homeland demonstrated a rising understanding that only the military had the means and personnel capabilities necessary to defend against attacks launched by peer competitor nations, all of whom had already created dedicated cyber operators within their military forces. To be sure, the Department of Homeland Security and the intelligence agencies would still play a part in cyber defense—but the DOD seemed determined to take overall control of the effort.

- ***Document 17:*** *National Security Strategy*
- ***When:*** February 2015
- ***Where:*** Washington, D.C.
- ***Significance:*** The 2015 National Security Strategy was the last opportunity for President Barack Obama to reset the direction of national security priorities during his administration. Published almost five years after its predecessor, it reflected a number of changes in threats and priorities. In particular, the head of al Qaeda, Osama bin Laden, had been killed in a raid in Pakistan in 2011. Later, in 2015, the administration agreed to a nuclear arms limitation agreement with Iran, allowing it to refocus national security against the larger peer threats of Russia and China.

DOCUMENT

Still, there is no shortage of challenges that demand continued American leadership. The potential proliferation of weapons of mass destruction, particularly nuclear weapons, poses a grave risk. Even as we have decimated al-Qa'ida's core leadership, more diffuse networks of al-Qa'ida, ISIL, and affiliated groups threaten U.S. citizens, interests, allies, and partners. Violent extremists exploit upheaval across the Middle East and North Africa. Fragile and conflict-affected states incubate and spawn infectious disease, illicit weapons and drug smugglers, and destabilizing refugee flows. Too often, failures in governance and endemic corruption hold back the potential of rising regions. The danger of disruptive and even destructive cyber-attack is growing, and the risk of another global economic slowdown remains. The international community's ability to respond effectively to these and other risks is helped or hindered by the behaviors of major powers. Where progress has been most profound, it is due to the steadfastness of our allies and the cooperation of other emerging powers.

. . .

In the last 6 years alone, we arrested the worst financial crisis since the Great Depression and catalyzed a new era of economic growth. We increased our competitive edge and leadership in education, energy, science and technology, research and development, and healthcare. We achieved an energy transformation in North America. We are fortifying our critical infrastructure against all hazards, especially cyber espionage and attack. And we are working hard to safeguard our civil liberties while advancing our security.

. . .

Assure Access to Shared Spaces

The world is connected by shared spaces—cyber, space, air, and oceans—that enable the free flow of people, goods, services, and ideas. They are the arteries of the global economy and civil society, and access is at risk due to increased competition and provocative behaviors. Therefore, we will continue to promote rules for responsible behavior while making sure we have the capabilities to assure access to these shared spaces.

Cybersecurity

As the birthplace of the internet, the United States has a special responsibility to lead a networked world. Prosperity and security increasingly depend on an open, interoperable, secure, and reliable internet. Our economy, safety, and health are linked through a networked infrastructure that is targeted by malicious government, criminal, and individual actors who try to avoid attribution. Drawing on the voluntary cybersecurity framework, we are securing Federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of U.S. critical infrastructure. We will continue to work with the Congress to pursue a legislative framework that ensures high standards. We will defend ourselves, consistent with U.S. and international law, against cyber attacks and impose costs on malicious cyber actors, including through prosecution of illegal cyber activity. We will assist other countries to develop laws that enable strong action against

threats that originate from their infrastructure. Globally, cybersecurity requires that long-standing norms of international behavior—to include protection of intellectual property, online freedom, and respect for civilian infrastructure—be upheld, and the internet be managed as a shared responsibility between states and the private sector with civil society and internet users as key stakeholders.

. . .

The United States welcomes the rise of a stable, peaceful, and prosperous China. We seek to develop a constructive relationship with China that delivers benefits for our two peoples and promotes security and prosperity in Asia and around the world. We seek cooperation on shared regional and global challenges such as climate change, public health, economic growth, and the denuclearization of the Korean Peninsula. While there will be competition, we reject the inevitability of confrontation. At the same time, we will manage competition from a position of strength while insisting that China uphold international rules and norms on issues ranging from maritime security to trade and human rights. We will closely monitor China's military modernization and expanding presence in Asia, while seeking ways to reduce the risk of misunderstanding or miscalculation. On cybersecurity, we will take necessary actions to protect our businesses and defend our networks against cyber-theft of trade secrets for commercial gain whether by private actors or the Chinese government.

SOURCE: Barack Obama, *National Security Strategy* (Washington, D.C.: Government Printing Office, 2015), 1–2, 3, 12–13, 24, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

ANALYSIS

This document is particularly noteworthy because it recognizes the rising possibility of a catastrophic cyberattack, as opposed to the more traditional use of the cyber domain for espionage purposes. In particular, though, it also presents a direct challenge to the People's Republic of China (PRC) to cease the massive cyber operations being used to steal billions of dollars' worth of intellectual property on an annual basis. By publicly naming the PRC as a cyber adversary, President Obama served notice that the United States would no longer passively accept such intrusions and attempt to counter them through defensive measures. This also signaled the possibility of significant American retaliation for such activities, most likely through the cyber domain.

- ***Document 18:*** *The National Military Strategy of the United States of America: The United States Military's Contribution to National Security*
- ***When:*** June 2015
- ***Where:*** Washington, D.C.

- ***Significance:*** By the 2015 release of the National Military Strategy, the United States had withdrawn its troops from Iraq and greatly reduced the number of forces deployed in Afghanistan. Further, the death of Osama bin Laden significantly reduced the threat presented by al Qaeda, and while the Islamic State sought to conquer portions of Iraq and Syria, it had shown little interest or capability in launching spectacular attacks against targets in the West.

DOCUMENT

III. An Integrated Military Strategy
Deter, Deny, and Defeat State Adversaries

The U.S. military is the world's preeminent Joint Force. It supports the Nation by providing a full range of options to protect the homeland and our interests while assuring the security of our allies. The U.S. military deters aggression by maintaining a credible nuclear capability that is safe, secure, and effective; conducting forward engagement and operations; and maintaining Active, National Guard, and Reserve forces prepared to deploy and conduct operations of sufficient scale and duration to accomplish their missions. Forward deployed, rotational, and globally responsive forces regularly demonstrate the capability and will to act. Should deterrence fail to prevent aggression, the U.S. military stands ready to project power to deny an adversary's objectives and decisively defeat any actor that threatens the U.S. homeland, our national interests, or our allies and partners.

Deterring a direct attack on the United States and our allies is a priority mission, requiring homeland and regional defenses tied to secure conventional and nuclear strike capabilities. Thus U.S. strategic forces remain always ready. U.S. military defenses are enhanced by our North American Aerospace Defense Command Agreement with Canada and close cooperation with the U.S. Department of Homeland Security. These homeland defense partnerships are complemented by growing investments in the cyber realm designed to protect vital networks and infrastructure.

In case of aggression, denying adversaries their goals will be an immediate objective. This places special emphasis on maintaining highly-ready forces forward, as well as well trained and equipped surge forces at home, resilient logistics and transportation infrastructures, networked intelligence, strong communications links, and interoperability with allies and partners. Timely interagency planning and coordination also will be leveraged to develop holistic options that serve to integrate all elements of national power.

Should any actor directly attack the United States or our interests, the U.S. military will take action to defend our Nation. We are prepared to project power across all domains to stop aggression and win our Nation's wars by decisively defeating

adversaries. While we prefer to act in concert with others, we will act unilaterally if the situation demands. In the event of an attack, the U.S. military will respond by inflicting damage of such magnitude as to compel the adversary to cease hostilities or render it incapable of further aggression. War against a major adversary would require the full mobilization of all instruments of national power and, to do so, the United States sustains a full-spectrum military that includes strong Reserve and National Guard forces. They provide the force depth needed to achieve victory while simultaneously deterring other threats.

Joint Force Initiatives

Programs: Sustaining Our Quality Edge

Effective programs enable our Soldiers, Sailors, Airmen, Marines, and Coast Guardsmen to fight and win. Delivering next-generation programs on schedule and within cost is vital, as our current systems increasingly are being challenged by adversary capabilities. To win against the diverse range of state and non-state threats confronting us, we must think innovatively, challenge assumptions, and embrace change.

We are improving joint interoperability. We are in the process of defining the next set of interoperability standards for future capabilities. In view of the anti-access/area denial (A2/AD) challenges we increasingly face, our future force will have to operate in contested environments. Key to assuring such access will be deploying secure, interoperable systems between Services, allies, interagency, and commercial partners. Priority efforts in that regard are establishing a Joint Information Environment (JIE), advancing globally integrated logistics, and building an integrated Joint ISR Enterprise. The results of these initiatives—particularly the enhanced connectivity and cybersecurity provided by the JIE—will provide the foundation for future interoperability.

We are investing to enhance decisive advantages. Future capabilities must sustain our ability to defend the homeland and project military power globally. Important investments to counter A2/AD, space, cyber, and hybrid threats include: space and terrestrial-based indications and warning systems, integrated and resilient ISR platforms, strategic lift, long-range precision strike weapons, missile defense technologies, undersea systems, remotely operated vehicles and technologies, special operations forces, and the Cyber Mission Force, among others. We also are improving our global sustainment capabilities and upgrading our command and control infrastructure to better support widely dispersed operations. We are modernizing our nuclear enterprise and working to protect our Nation against asymmetric threats.

To improve institutional agility, we are expanding relations with American businesses, including many of the most innovative companies in the world, to learn their best practices. Further, we are aligning our programmatic efforts to take advantage of insights gleaned from the Defense Innovation Initiative, which is aimed at identifying potential strategic and operational advantages through wargaming, concept development, and a wide array of technology investments.

As we develop new capabilities to counter threats along the continuum of conflict, we also must procure sufficient capacity and readiness to sustain our global

responsibilities. This may include evolving traditional platforms. Or it may require developing entirely new systems that are affordable and flexible. In all cases, our programs must allow us to quickly adapt, to counter adversaries employing unexpected techniques or weapons.

SOURCE: U.S. Department of Defense, *The National Military Strategy of the United States of America: The United States Military's Contribution to National Security*, (Washington, D.C.: Government Printing Office, 2015), 7, 16–17, https://www.jcs.mil/Portals/36/Documents/Publications/National_Military_Strategy_2015.pdf

ANALYSIS

In some ways, the 2015 National Military Strategy sought to illustrate a technological renaissance in the U.S. military, something that typically only happens in peacetime, as wartime commitments require expenditures on existing systems rather than long-term development projects. This edition of the military strategy also demonstrated an increased focus on operating in a joint fashion, with each service providing unique capabilities to a whole-of-government approach to the exercise of military power. Likewise, it emphasized the need for military forces to cooperate with other instruments of national power in order to pursue the national defense objectives of the nation. The United States has, since World War II, largely relied upon technological superiority to offset the numerical disadvantages it faces on modern battlefields. The 2015 National Military Strategy included significant provisions to remind the reader of this legacy and of the need to maintain this vital advantage as a hedge against future conflicts.

- ***Document 19:*** *The Department of Defense Cyber Strategy*
- ***When:*** April 2015
- ***Where:*** Washington, D.C.
- ***Significance:*** Just as the DOD releases a National Military Strategy derived from the president's National Defense Strategy, the same form of hierarchical strategizing is found in more specific cyber strategies that are first propagated from the presidential level, and then from the cabinet level. In the 2015 DOD cyber strategy, the department sought to offer guidance to its subordinate units regarding the most important threats in the cyber domain, and how the military services would be empowered to counter them.

DOCUMENT

Strategic Context

Key Cyber Threats

From 2013-2015, the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001. Potential state and non-state adversaries conduct malicious cyber activities against U.S. interests globally and in a manner intended to test the limits of what the United States and the international community will tolerate. Actors may penetrate U.S. networks and systems for a variety of reasons, such as to steal intellectual property, disrupt an organization's operations for activist purposes, or to conduct disruptive and destructive attacks to achieve military objectives.

Potential adversaries have invested significantly in cyber as it provides them with a viable, plausibly deniable capability to target the U.S. homeland and damage U.S. interests. Russia and China have developed advanced cyber capabilities and strategies. Russian actors are stealthy in their cyber tradecraft and their intentions are sometimes difficult to discern. China steals intellectual property (IP) from global businesses to benefit Chinese companies and undercut U.S. competitiveness. While Iran and North Korea have less developed cyber capabilities, they have displayed an overt level of hostile intent towards the United States and U.S. interests in cyberspace.

In addition to state-based threats, non-state actors like the Islamic State in Iraq and the Levant (ISIL) use cyberspace to recruit fighters and disseminate propaganda and have declared their intent to acquire disruptive and destructive cyber capabilities. Criminal actors pose a considerable threat in cyberspace, particularly to financial institutions, and ideological groups often use hackers to further their political objectives. State and non-state threats often also blend together; patriotic entities often act as cyber surrogates for states, and non-state entities can provide cover for state-based operators. This behavior can make attribution more difficult and increases the chance of miscalculation.

Malware Proliferation

The global proliferation of malicious code or software ("malware") increases the risk to U.S. networks and data. To conduct a disruptive or destructive cyber operation against a military system or industrial control system requires expertise, but a potential adversary need not spend billions of dollars to develop an offensive capability. A nation-state, non-state group, or individual actor can purchase destructive malware and other capabilities on the black market. State and non-state actors also pay experts to search for vulnerabilities and develop exploits. This practice has created a dangerous and uncontrolled market that serves multiple actors within the international system, often for competing purposes. As cyber capabilities become more readily available over time, the Department of Defense assesses that state and non-state actors will continue to seek and develop cyber capabilities to use against U.S. interests.

Risk to DoD Networks and Infrastructure

The Defense Department's own networks and systems are vulnerable to intrusions and attacks. In addition to DoD's own networks, a cyberattack on the critical infrastructure and key resources on which DoD relies for its operations could impact the U.S. military's ability to operate in a contingency. DoD has made gains in identifying cyber vulnerabilities of its own critical assets through its Mission Assurance Program—for many key assets, DoD has identified its physical network infrastructure on which key physical assets depend—but more must be done to secure DoD's cyber infrastructure.

In addition to destructive and disruptive attacks, cyber actors steal operational information and intellectual property from a range of U.S. government and commercial entities that impact the Defense Department. Victims include weapons developers as well as commercial firms that support force movements through U.S. Transportation Command (USTRANSCOM). State actors have stolen DoD's intellectual property to undercut the United States' strategic and technological advantage and to benefit their own military and economic development.

Finally, the Defense Department faces a risk from the U.S. government's continued budgetary uncertainty. Although DoD has prioritized the allocation of resources in its budget to develop cyber capabilities, continued fiscal uncertainty requires that DoD plan to build its cyber capabilities under a declining overall defense budget. DoD must continue to prioritize its cyber investments and develop the capabilities required to defend U.S. interests at home and overseas.

Deterrence in the Future Security Environment

In the face of an escalating threat, the Department of Defense must contribute to the development and implementation of a comprehensive cyber deterrence strategy to deter key state and non-state actors from conducting cyberattacks against U.S. interests. Because of the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors' behavior.

As DoD builds its Cyber Mission Force and overall capabilities, DoD assumes that the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems. The deterrence of state and non-state groups in cyberspace will thus require the focused attention of multiple U.S. government departments and agencies. The Department of Defense has a number of specific roles to play in this equation.

Deterrence is partially a function of perception. It works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed. The United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the

overall resilience of U.S. systems to withstand a potential attack if it penetrates the United States' defenses. In addition, the United States requires strong intelligence, forensics, and indications and warning capabilities to reduce anonymity in cyberspace and increase confidence in attribution.

- Response: The United States has been clear that it will respond to a cyberattack on U.S. interests through its defense capabilities. The United States has articulated this declaratory policy in the 2011 United States International Strategy for Cyberspace, in the Department of Defense Cyberspace Policy Report to Congress of 2011, and through public statements by the President and the Secretary of Defense. The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law.
- Denial: While DoD has made progress in building the Cyber Mission Force, DoD must increase its defensive capabilities to defend DoD networks and defend the nation from sophisticated cyberattacks, and must work with other departments, agencies, international allies and partners, and the private sector to strengthen deterrence by denial through improved cybersecurity.
- Resilience: Because the Defense Department's capabilities cannot necessarily guarantee that every cyberattack will be denied successfully, the Defense Department must invest in resilient and redundant systems so that it may continue its operations in the face of disruptive or destructive cyberattacks on DoD networks. The Defense Department cannot, however, foster resilience in organizations that fall outside of its authority. In order for resilience to succeed as a factor in effective deterrence, other agencies of the government must work with critical infrastructure owners and operators and the private sector more broadly to develop resilient and redundant systems that can withstand a potential attack. Effective resilience measures can help convince potential adversaries of the futility of commencing cyberattacks on U.S. networks and systems.

Attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups. On matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace. Intelligence and attribution capabilities help to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics, techniques, and procedures. Attribution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack.

Public and private attribution can play a significant role in dissuading cyber actors from conducting attacks in the first place. The Defense Department will continue to collaborate closely with the private sector and other agencies of the U.S. government to strengthen attribution. This work will be especially important for deterrence as activist groups, criminal organizations, and other actors acquire advanced cyber capabilities over time.

Finally, cyber capabilities present state and non-state actors with the ability to strike at U.S. interests in a manner that may or may not necessarily warrant a purely military response by the United States, but which may nonetheless present a significant threat to U.S. national security and may warrant a non-military response of some kind. In response to certain attacks and intrusions, the United States may undertake diplomatic actions, take law enforcement actions, and consider economic sanctions.

For example, the United States used verifiable and attributable data to engage China about the risks posed by its economic espionage. The attribution of this data allowed the United States to express concerns regarding the impact of Chinese intellectual property theft on U.S. economic competitiveness, and the potential risks posed to strategic stability by Chinese activity. Because they broke the law and to deter China from conducting future cyber espionage, the Justice Department indicted five members of the People's Liberation Army for stealing U.S. intellectual property to directly benefit Chinese companies. The Defense Department will support the Justice Department and other agencies in exploring new tools and capabilities to help deter such activity in cyberspace.

SOURCE: U.S. Department of Defense, *The Department of Defense Cyber Strategy* (Washington, D.C.: Government Printing Office, 2015), 9–12, https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf

ANALYSIS

It is unsurprising that the cyber strategy for the DOD emphasized the role of nonstate actors in the cyber domain, at the same time that the National Defense Strategy focused upon the behavior of the Islamic State and other nonstate entities. Perhaps more interestingly, this cyber strategy directly confronted the problems associated with attribution of cyberattacks and responsibility. Kinetic strikes are often relatively straightforward to trace back to their source, but the same cannot be said of cyberattacks. Thus, to heavily focus on attribution, and provide limited examples of how successful attribution has been turned toward deterring future attacks, is an interesting departure from previous cyber strategy documents. Of course, it is impossible to say whether the indictment of People's Liberation Army hackers will have any form of deterrent effect going forward. It is highly unlikely that the Chinese government will agree to extradite any of its uniformed personnel to the United States to face a trial for cyberattacks, and barring such an extradition, the individuals in question are unlikely to ever face any legal repercussions for their activities. Likewise, the Chinese government is unlikely to consent to individuals with such highly classified knowledge traveling outside of China's borders, making their capture all but impossible. Yet, the DOD considered it a victory important enough to include their indictments in the cyber strategy, which suggests that military leaders believe the indictments offered some degree of deterrent value.

- ***Document 20:*** *National Security Strategy of the United States of America*
- ***When:*** December 2017
- ***Where:*** Washington, D.C.
- ***Significance:*** After less than one year in office, President Donald Trump released a new national security agenda for the nation's executive departments. Typically, the National Security Strategy had been revised every four to five years, and thus a new strategy after less than three years signaled a marked departure from the priorities of his predecessor in office. Trump's national security strategy emphasized the dangers of conflict with Russia and China, and somewhat minimized the threats presented by terror organizations and other nonstate actors.

DOCUMENT

Keep America Safe in the Cyber Era

America's response to the challenges and opportunities of the cyber era will determine our future prosperity and security. For most of our history, the United States has been able to protect the homeland by controlling its land, air, space, and maritime domains. Today, cyberspace offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders. Cyberattacks offer adversaries low-cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business.

Critical infrastructure keeps our food fresh, our houses warm, our trade flowing, and our citizens productive and safe. The vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication.

Federal networks also face threats. These networks allow government agencies to carry out vital functions and provide services to the American people. The government must do a better job of protecting data to safeguard information and the privacy of the American people. Our Federal networks must be modernized and updated.

In addition, the daily lives of most Americans rely on computer-driven and interconnected technologies. As our reliance on computers and connectivity increases,

we become increasingly vulnerable to cyberattacks. Businesses and individuals must be able to operate securely in cyberspace.

Security was not a major consideration when the internet was designed and launched. As it evolves, the government and private sector must design systems that incorporate prevention, protection, and resiliency from the start, not as an afterthought. We must do so in a way that respects free markets, private competition, and the limited but important role of government in enforcing the rule of law. As we build the next generation of digital infrastructure, we have an opportunity to put our experience into practice.

The internet is an American invention, and it should reflect our values as it continues to transform the future for all nations and all generations. A strong, defensible cyber infrastructure fosters economic growth, protects our liberties, and advances our national security.

Priority Actions

Identify and Prioritize Risk: To improve the security and resilience of our critical infrastructure, we will assess risk across six key areas: national security, energy and power, banking and finance, health and safety, communications, and transportation. We will assess where cyberattacks could have catastrophic or cascading consequences and prioritize our protective efforts, capabilities, and defenses accordingly.

Build Defensible Government Networks: We will use the latest commercial capabilities, shared services, and best practices to modernize our Federal information technology. We will improve our ability to provide uninterrupted and secure communications and services under all conditions.

Deter and Disrupt Malicious Cyber Actors: The Federal Government will ensure that those charged with securing critical infrastructure have the necessary authorities, information, and capabilities to prevent attacks before they affect or hold at risk U.S. critical infrastructure. The United States will impose swift and costly consequences on foreign governments, criminals, and other actors who undertake significant malicious cyber activities. We will work with allies and friends to expand our awareness of malicious activities. A stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.

Improve Information Sharing and Sensing: The U.S. Government will work with our critical infrastructure partners to assess their informational needs and to reduce the barriers to information sharing, such as speed and classification levels. We will also invest in capabilities that improve the ability of the United States to attribute cyberattacks. In accordance with the protection of civil liberties and privacy, the U.S. Government will expand collaboration with the private sector so that we can better detect and attribute attacks.

Deploy Layered Defenses: Since threats transit globally, passing through communications backbones without challenge, the U.S. Government will work with the private sector to remediate known bad activities at the network level to improve the security of all customers. Malicious activity must be defeated within a network and not be passed on to its destination whenever possible.

. . .

Renew Capabilities

Cyberspace

Malicious state and non-state actors use cyberattacks for extortion, information warfare, disinformation, and more. Such attacks have the capability to harm large numbers of people and institutions with comparatively minimal investment and a troubling degree of deniability. These attacks can undermine faith and confidence in democratic institutions and the global economic system.

Many countries now view cyber capabilities as tools for projecting influence, and some use cyber tools to protect and extend their autocratic regimes. Cyberattacks have become a key feature of modern conflict. The United States will deter, defend, and when necessary defeat malicious actors who use cyberspace capabilities against the United States. When faced with the opportunity to take action against malicious actors in cyberspace, the United States will be risk informed, but not risk averse, in considering our options.

Priority Actions

Improve Attribution, Accountability, and Response: We will invest in capabilities to support and improve our ability to attribute cyberattacks, to allow for rapid response.

Enhance Cyber Tools and Expertise: We will improve our cyber tools across the spectrum of conflict to protect U.S. Government assets and U.S. critical infrastructure, and to protect the integrity of data and information. U.S. departments and agencies will recruit, train, and retain a workforce capable of operating across this spectrum of activity.

Improve Integration and Agility: We will improve the integration of authorities and procedures across the U.S. Government so that cyber operations against adversaries can be conducted as required. We will work with the Congress to address the challenges that continue to hinder timely intelligence and information sharing, planning and operations, and the development of necessary cyber tools.

SOURCE: Donald J. Trump, *National Security Strategy of the United States of America* (Washington, D.C.: Government Printing Office, 2017), 12–13, 31–32, http://nssarchive.us/wp-content/uploads/2017/12/2017.pdf

ANALYSIS

Unlike previous versions of the National Security Strategy, the 2017 version is very deliberate in laying out the key priorities of the administration for each area of focus. In this regard, the document proved extremely useful in devising the roles of subordinate organizations. It also demonstrated an excellent understanding of the steps required to improve national cybersecurity. By clarifying exactly what needed to be done first, this document made the formulation of a national cyber strategy substantially easier for those units tasked with devising and carrying out such a function.

- ***Document 21:*** *Summary of the 2018 National Defense Strategy of the United States of America*
- ***When:*** 2018
- ***Where:*** Washington, D.C.
- ***Significance:*** This was the first National Defense Strategy created during the administration of President Donald Trump. Its preparation was overseen by Secretary of Defense James Mattis, and it sought to restructure the DOD to meet the changing needs of the nation. In particular, Trump and Mattis wished to re-emphasize the ability to engage in great power conflict, should it be necessary to openly confront Russia or China. Because the National Defense Strategy of 2018 is the current guiding document for the DOD, only the unclassified summary of the report is currently available to the public.

DOCUMENT

Strategic Environment

The *National Defense Strategy* acknowledges an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations. These changes require a clear-eyed appraisal of the threats we face, acknowledgement of the changing character of warfare, and a transformation of how the Department conducts business.

The central challenge to U.S. prosperity and security is the *reemergence of long-term, strategic competition* by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions.

China is leveraging military modernization, influence operations, and predatory economics to coerce neighboring countries to reorder the Indo-Pacific region to their advantage. As China continues its economic and military ascendance, asserting power through an all-of-nation long-term strategy, it will continue to pursue a military modernization program that seeks Indo-Pacific regional hegemony in the near-term and displacement of the United States to achieve global preeminence in the future. The most far-reaching objective of this defense strategy is to set the military relationship between our two countries on a path of transparency and non-aggression.

Concurrently, Russia seeks veto authority over nations on its periphery in terms of their governmental, economic, and diplomatic decisions, to shatter the North

Atlantic Treaty Organization and change European and Middle East security and economic structures to its favor. The use of emerging technologies to discredit and subvert democratic processes in Georgia, Crimea, and eastern Ukraine is concern enough, but when coupled with its expanding and modernizing nuclear arsenal the challenge is clear.

Another change to the strategic environment is a *resilient, but weakening, post-WWII international order*. In the decades after fascism's defeat in World War II, the United States and its allies and partners constructed a free and open international order to better safeguard their liberty and people from aggression and coercion. Although this system has evolved since the end of the Cold War, our network of alliances and partnerships remain the backbone of global security. China and Russia are now undermining the international order from within the system by exploiting its benefits while simultaneously undercutting its principles and "rules of the road."

Rogue regimes such as North Korea and Iran are destabilizing regions through their pursuit of nuclear weapons or sponsorship of terrorism. North Korea seeks to guarantee regime survival and increased leverage by seeking a mixture of nuclear, biological, chemical, conventional, and unconventional weapons and a growing ballistic missile capability to gain coercive influence over South Korea, Japan, and the United States. In the Middle East, Iran is competing with its neighbors, asserting an arc of influence and instability while vying for regional hegemony, using state-sponsored terrorist activities, a growing network of proxies, and its missile program to achieve its objectives.

Both revisionist powers and rogue regimes are competing across all dimensions of power. They have increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals.

Challenges to the U.S. military advantage represent another shift in the global security environment. For decades the United States has enjoyed uncontested or dominant superiority in every operating domain. We could generally deploy our forces when we wanted, assemble them where we wanted, and operate how we wanted. Today, every domain is contested—air, land, sea, space, and cyberspace.

We face an ever more lethal and disruptive battlefield, combined across domains, and conducted at increasing speed and reach—from close combat, throughout overseas theaters, and reaching to our homeland. Some competitors and adversaries seek to optimize their targeting of our battle networks and operational concepts, while also using other areas of competition short of open warfare to achieve their ends (e.g., information warfare, ambiguous or denied proxy operations, and subversion). These trends, if unaddressed, will challenge our ability to deter aggression.

DID YOU KNOW?

Georbot

Georbot is the name of one of the most successful cyberattack networks ever created. During the 2008 confrontation between Russia and Georgia, thousands of Russian partisans knowingly downloaded the software necessary to infect their own computers, making them part of a botnet designed to attack Georgian government and banking computer networks. Elements of the Russian Secret Service and the criminal Russian Business Network were linked to the control systems of Georbot. Georgia's computer emergency response team (CERT) managed to identify the botmaster of Georbot and planted a trap by hiding malware, itself a version of the original Georbot, in a document file. When the botmaster downloaded the "poisoned" file, the Georgian CERT was able to activate the hacker's webcam and take a picture of him, as well as seize control of his computer's control panel. This not only ended the threat presented by Georbot it also provided substantial insight into the techniques preferred by Russian hackers targeting enemy state cyber systems.

The security environment is also affected by *rapid technological advancements and the changing character of war*. The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed. New technologies include advanced computing, "big data" analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future.

New commercial technology will change society and, ultimately, the character of war. The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed. Maintaining the Department's technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base.

States are the principal actors on the global stage, but *non-state actors* also threaten the security environment with increasingly sophisticated capabilities. Terrorists, trans-national criminal organizations, cyber hackers and other malicious non-state actors have transformed global affairs with increased capabilities of mass disruption. There is a positive side to this as well, as our partners in sustaining security are also more than just nation-states: multilateral organizations, non-governmental organizations, corporations, and strategic influencers provide opportunities for collaboration and partnership. Terrorism remains a persistent condition driven by ideology and unstable political and economic structures, despite the defeat of ISIS's physical caliphate.

It is now undeniable that the *homeland is no longer a sanctuary*. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. New threats to commercial and military uses of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated.

Rogue regimes, such as North Korea, continue to seek out or develop WMD—nuclear, chemical, and biological—as well as long range missile capabilities and, in some cases, proliferate these capabilities to malign actors as demonstrated by Iranian ballistic missile exports. Terrorists likewise continue to pursue WMD, while the spread of nuclear weapon technology and advanced manufacturing technology remains a persistent problem. Recent advances in bioengineering raise another concern, increasing the potential, variety, and ease of access to biological weapons.

Department of Defense Objectives

In support of the National Security Strategy, the Department of Defense will be prepared to defend the homeland, remain the preeminent military power in the world, ensure the balances of power remain in our favor, and advance an international order that is most conducive to our security and prosperity.

Long-term strategic competitions with China and Russia are the principal priorities for the Department, and require both increased and sustained investment, because of the magnitude of the threats they pose to U.S. security and prosperity today, and the potential for those threats to increase in the future. Concurrently, the Department will sustain its efforts to deter and counter rogue regimes such as North Korea and Iran, defeat terrorist threats to the United States, and consolidate our gains in Iraq and Afghanistan while moving to a more resource-sustainable approach.

SOURCE: U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, D.C.: Government Printing Office, 2018), 2–4, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

ANALYSIS

It is clear that under Secretary Mattis, the U.S. DOD radically shifted its focus back to traditional forms of conflict, with an emphasis upon peer competitors such as Russia and China, as well as rising threats from Iran and North Korea. This summary is illustrative in that it has very little focus on terror organizations, beyond a note that the geographic area under the control of the Islamic State had been recaptured. It also makes little mention of the role of cyber operations in modern conflict, despite their importance to any effort requiring command and control of military forces.

- ***Document 22:*** *National Cyber Strategy of the United States*
- ***When:*** September 2018
- ***Where:*** Washington, D.C.
- ***Significance:*** With each iteration, the National Cyber Strategy of the United States tends to become both more proscriptive and paradoxically more vague. In part, this is due to the recognition that many aspects of a nation's cyber efforts need to remain classified if they are to have any value to national defense. But, in part, this is probably due to the recognition that threats in the cyber domain often come from completely unexpected quarters, and thus, any effort to announce how the United States might behave in cyberspace is likely to be obsolete shortly after its propagation.

DOCUMENT

How Did We Get Here?

The rise of the internet and the growing centrality of cyberspace to all facets of the modern world corresponded with the rise of the United States as the world's lone superpower. For the past quarter century, the ingenuity of the American people drove the evolution of cyberspace, and in turn, cyberspace has become fundamental to American wealth creation and innovation. Cyberspace is an inseparable component of America's financial, social, government, and political life. Meanwhile, Americans sometimes took for granted that the supremacy of the United States in the cyber domain would remain unchallenged, and that America's vision for an open, interoperable, reliable, and secure internet would inevitably become a reality. Americans believed the growth of the internet would carry the universal aspirations for free expression and individual liberty around the world. Americans assumed the opportunities to expand communication, commerce, and free exchange of ideas would be self-evident. Large parts of the world have embraced America's vision of a shared and open cyberspace for the mutual benefit of all.

Our competitors and adversaries, however, have taken an opposite approach. They benefit from the open internet, while constricting and controlling their own people's access to it, and actively undermine the principles of an open internet in international forums. They hide behind notions of sovereignty while recklessly violating the laws of other states by engaging in pernicious economic espionage and malicious cyber activities, causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world. They view cyberspace as an arena where the United States' overwhelming military, economic, and political power could be neutralized and where the United States and its allies and partners are vulnerable.

Russia, Iran, and North Korea conducted reckless cyber attacks that harmed American and international businesses and our allies and partners without paying costs likely to deter future cyber aggression. China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft. Non-state actors—including terrorists and criminals—exploited cyberspace to profit, recruit, propagandize, and attack the United States and its allies and partners, with their actions often shielded by hostile states. Public and private entities have struggled to secure their systems as adversaries increase the frequency and sophistication of their malicious cyber activities. Entities across the United States have faced cybersecurity challenges in effectively identifying, protecting, and ensuring resilience of their networks, systems, functions, and data as well as detecting, responding to, and recovering from incidents.

The Way Forward

New threats and a new era of strategic competition demand a new cyber strategy that responds to new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the American people to thrive. Securing cyberspace is fundamental to our strategy and requires technical advancements and administrative efficiency across the Federal Government and the private sector. The Administration

also recognizes that a purely technocratic approach to cyberspace is insufficient to address the nature of the new problems we confront. The United States must also have policy choices to impose costs if it hopes to deter malicious cyber actors and prevent further escalation.

The Administration is already taking action to aggressively address these threats and adjust to new realities. The United States has sanctioned malign cyber actors and indicted those that have committed cybercrimes. We have publicly attributed malicious activity to the responsible adversaries and released details of the tools and infrastructure they employed. We have required departments and agencies to remove software vulnerable to various security risks. We have taken action to hold department and agency heads accountable for managing the cybersecurity risks to systems they control, while empowering them to provide adequate security.

The Administration's approach to cyberspace is anchored by enduring American values, such as the belief in the power of individual liberty, free expression, free markets, and privacy. We retain our commitment to the promise of an open, interoperable, reliable, and secure internet to strengthen and extend our values and protect and ensure economic security for American workers and companies. The future we desire will not come without a renewed American commitment to advance our interests across cyberspace.

The Administration recognizes that the United States is engaged in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks. Russia, China, Iran, and North Korea all use cyberspace as a means to challenge the United States, its allies, and partners, often with a recklessness they would never consider in other domains. These adversaries use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes. We are vulnerable to peacetime cyber attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber attacks against the United States during a crisis short of war. These adversaries are continually developing new and more effective cyber weapons. This National Cyber Strategy outlines how we will (1) defend the homeland by protecting networks, systems, functions, and data; (2) promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) preserve peace and security by strengthening the United States' ability—in concert with allies and partners—to deter and if necessary punish those who use cyber tools for malicious purposes; and (4) expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure internet. The Strategy's success will be realized when cybersecurity vulnerabilities are effectively managed through identification and protection of networks, systems, functions, and data as well as detection of, resilience against, response to, and recovery from incidents; destructive, disruptive, or otherwise destabilizing malicious cyber activities directed against United States interests are reduced or prevented; activity that is contrary to responsible behavior in cyberspace is deterred through the imposition of costs through cyber and non-cyber means; and the United States is positioned to use cyber capabilities to achieve national security objectives. The articulation of the National Cyber Strategy is organized according to the pillars of the National Security Strategy. The National Security Council staff will coordinate with departments, agencies, and the

Office of Management and Budget (OMB) on an appropriate resource plan to implement this Strategy. Departments and agencies will execute their missions informed by the following strategic guidance.

Protect the American People, the Homeland, and the American Way of Life

Protecting the American people, the American way of life, and American interests is at the forefront of the National Security Strategy. Protecting American information networks, whether government or private, is vital to fulfilling this objective. It will require a series of coordinated actions focused on protecting government networks, protecting critical infrastructure, and combating cybercrime. The United States Government, private industry, and the public must each take immediate and decisive actions to strengthen cybersecurity, with each working on securing the networks under their control and supporting each other as appropriate.

Objective: Manage cybersecurity risks to increase the security and resilience of the Nation's information and information systems.

Secure Federal Networks and Information

The responsibility to secure Federal networks—including Federal information systems and national security systems—falls squarely on the Federal Government. The Administration will clarify the relevant authorities, responsibilities, and accountability within and across departments and agencies for securing Federal information systems, while setting the standard for effective cybersecurity risk management. As part of this effort, the Administration will centralize some authorities within the Federal Government, enable greater cross-agency visibility, improve management of our Federal supply chain, and strengthen the security of United States Government contractor systems.

. . .

Secure Critical Infrastructure

The responsibility to secure the Nation's critical infrastructure and manage its cybersecurity risk is shared by the private sector and the Federal Government. In partnership with the private sector, we will collectively use a risk-management approach to mitigating vulnerabilities to raise the base level of cybersecurity across critical infrastructure. We will simultaneously use a consequence-driven approach to prioritize actions that reduce the potential that the most advanced adversaries could cause large-scale or long-duration disruptions to critical infrastructure. We will also deter malicious cyber actors by imposing costs on them and their sponsors by leveraging a range of tools, including but not limited to prosecutions and economic sanctions, as part of a broader deterrence strategy.

. . .

Combat Cybercrime and Improve Incident Reporting

Federal departments and agencies, in cooperation with state, local, tribal, and territorial government entities, play a critical role in detecting, preventing, disrupting, and investigating cyber threats to our Nation. The United States is regularly the victim of malicious cyber activity perpetrated by criminal actors, including

state and non-state actors and their proxies and terrorists using network infrastructure in the United States and abroad. Federal law enforcement works to apprehend and prosecute offenders, disable criminal infrastructure, limit the spread and use of nefarious cyber capabilities, prevent cyber criminals and their state sponsors from profiting from their illicit activity, and seize their assets. The Administration will push to ensure that our Federal departments and agencies have the necessary legal authorities and resources to combat transnational cybercriminal activity, including identifying and dismantling botnets, dark markets, and other infrastructure used to enable cybercrime, and combatting economic espionage. To effectively deter, disrupt, and prevent cyber threats, law enforcement will work with private industry to confront challenges presented by technological barriers, such as anonymization and encryption technologies, to obtain time-sensitive evidence pursuant to appropriate legal process. Law enforcement actions to combat criminal cyber activity serve as an instrument of national power by, among other things, deterring those activities.

. . .

Preserve Peace through Strength

Challenges to United States security and economic interests, from nation states and other groups, which have long existed in the offline world are now increasingly occurring in cyberspace. This now-persistent engagement in cyberspace is already altering the strategic balance of power. This Administration will issue transformative policies that reflect today's new reality and guide the United States Government towards strategic outcomes that protect the American people and our way of life. Cyberspace will no longer be treated as a separate category of policy or activity disjointed from other elements of national power. The United States will integrate the employment of cyber options across every element of national power.

Objective: Identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace.

Enhance Cyber Stability through Norms of Responsible State Behavior

The United States will promote a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary non-binding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence building measures to reduce the risk of conflict stemming from malicious cyber activity. These principles should form a basis for cooperative responses to counter irresponsible state actions inconsistent with this framework.

. . .

Attribute and Deter Unacceptable Behavior in Cyberspace

As the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners. All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic,

information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities. The United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyber activities with integrated strategies that impose swift, costly, and transparent consequences when malicious actors harm the United States or our partners.

SOURCE: White House, *National Cyber Strategy of the United States* (Washington, D.C.: Government Printing Office, 2018), 1–3, 6, 8, 10, 20–21, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

ANALYSIS

One of the persistent themes of this document is that the nation's adversaries in cyberspace, particularly Russia, China, and North Korea, have engaged in reckless behavior in the cyber domain that they would not dare to emulate in the physical domain. While it is true that none of those states has recently launched any form of kinetic attack against American forces, all three have fought against the United States in relatively recent conflicts. Further, given that the norms of cyberspace differ from those of the physical world, it is unsurprising that the behavior of participants in cyberspace also differ. Of course, the unstated concept in this document is that the United States might be engaging in equally reckless behavior in cyberspace through a variety of actions against adversaries such as the aforementioned nations. Each of them has accused the United States of launching cyberattacks, conducting cyber espionage, and engaging in cybercrime in a multitude of fashions. Whether such attacks have occurred, or this represents posturing by rivals in the cyber domain, is of less consequence than the perception that perhaps the United States is making unreasonable demands regarding the behavior of other states, in that it does not hold itself to the same standards of behavior.

- ***Document 23:*** *Summary, Department of Defense Cyber Strategy*
- ***When:*** 2018
- ***Where:*** Washington, D.C.
- ***Significance:*** In 2018, the DOD released a revised cyber strategy, superseding the 2015 document. While many portions of the strategy were not released to the public due to their classified information, a broad summary of the strategy was prepared as a separate document and placed into the public domain. It offers broad guidance of how the DOD expects to build a long-term foundation to tackle the ongoing challenges of military operations and security in the cyber domain.

DOCUMENT

Introduction

American prosperity, liberty, and security depend upon open and reliable access to information. The internet empowers us and enriches our lives by providing ever-greater access to new knowledge, businesses, and services. Computers and network technologies underpin U.S. military warfighting superiority by enabling the Joint Force to gain the information advantage, strike at long distance, and exercise global command and control.

The arrival of the digital age has also created challenges for the Department of Defense (DoD) and the Nation. The open, transnational, and decentralized nature of the internet that we seek to protect creates significant vulnerabilities. Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure.

We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners. China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation.

The Department must take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia. We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. We will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. We will collaborate with our interagency, industry, and international partners to advance our mutual interests. During wartime, U.S. cyber forces will be prepared to operate alongside our air, land, sea, and space forces to target adversary weaknesses, offset adversary strengths, and amplify the effectiveness of other elements of the Joint Force. Adversary militaries are increasingly reliant on the same type of computer and network technologies that have become central to Joint Force warfighting. The Department will exploit this reliance to gain military advantage. The Joint Force will employ offensive cyber capabilities and innovative concepts that allow for the use of cyberspace operations across the full spectrum of conflict.

The *2018 Department of Defense Cyber Strategy* represents the Department's vision for addressing this threat and implementing the priorities of the *National Security Strategy* and *National Defense Strategy* for cyberspace. It supersedes the *2015 DoD Cyber Strategy*.

The United States cannot afford inaction: our values, economic competitiveness, and military edge are exposed to threats that grow more dangerous every day. We must assertively defend our interests in cyberspace below the level of armed conflict and ensure the readiness of our cyberspace operators to support the Joint Force in crisis and conflict. Our Soldiers, Sailors, Airmen, Marines, and civilian employees stand ready, and we will succeed.

The Department's cyberspace objectives are:

1. Ensuring the Joint Force can achieve its missions in a contested cyberspace environment;
2. Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
3. Defending U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;
4. Securing DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
5. Expanding DoD cyber cooperation with interagency, industry, and international partners.

Strategic Approach

Our strategic approach is based on mutually reinforcing lines of effort to build a more lethal force; compete and deter in cyberspace; expand alliances and partnerships; reform the Department; and cultivate talent.

Build a More Lethal Joint Force

Accelerate cyber capability development: The Department will accelerate the development of cyber capabilities for both warfighting and countering malicious cyber actors. Our focus will be on fielding capabilities that are scalable, adaptable, and diverse to provide maximum flexibility to Joint Force commanders. The Joint Force will be capable of employing cyberspace operations throughout the spectrum of conflict, from day-to-day operations to wartime, in order to advance U.S. interests.

Innovate to foster agility: The Department must innovate to keep pace with rapidly evolving threats and technologies in cyberspace. We will accept and manage operational and programmatic risk in a deliberate manner that moves from a "zero defect" culture to one that fosters agility and innovation because success in this domain requires the Department to innovate faster than our strategic competitors.

Leverage automation and data analysis to improve effectiveness: The Department will use cyber enterprise solutions to operate at machine speed and large-scale data analytics to identify malicious cyber activity across different networks and systems. The Department will leverage these advances to improve our own defensive posture and to ensure that our cyber capabilities will continue to be effective against competitors armed with cutting edge technology.

Employ commercial-off-the-shelf (COTS) cyber capabilities: The Department excels at creating cyber capabilities tailored for specific operational problems. In addition to these capabilities, we will make greater use of COTS capabilities that can be optimized for DoD use.

Compete and Deter in Cyberspace

Deter malicious cyber activities: The United States seeks to use all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten U.S. national interests, our allies, or our partners. The Department will prioritize securing sensitive DoD information and deterring malicious cyber activities that constitute a use of force against the United States, our allies, or our partners. Should deterrence fail, the Joint Force stands ready to employ the full range of military capabilities in response.

Persistently contest malicious cyber activity in day-to-day competition: The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions. This includes working with the private sector and our foreign allies and partners to contest cyber activity that could threaten Joint Force missions and to counter the exfiltration of sensitive DoD information.

Increase the resilience of U.S. critical infrastructure: The Department will work with its interagency and private sector partners to reduce the risk that malicious cyber activity targeting U.S. critical infrastructure could have catastrophic or cascading consequences. We will streamline our public-private information-sharing mechanisms and strengthen the resilience and cybersecurity of critical infrastructure networks and systems.

Strengthen Alliances and Attract New Partnerships

Build trusted private sector partnerships: The private sector owns and operates the majority of U.S. infrastructure and is on the frontlines of nation-state competition in cyberspace. In coordination with other Federal departments and agencies, the Department will build trusted relationships with private sector entities that are critical enablers of military operations and carry out deliberate planning and collaborative training that enables mutually supporting cybersecurity activities.

Operationalize international partnerships: Many of the United States' allies and partners possess advanced cyber capabilities that complement our own. The Department will work to strengthen the capacity of these allies and partners and increase DoD's ability to leverage its partners' unique skills, resources, capabilities, and perspectives. Information-sharing relationships with allies and partners will increase the effectiveness of combined cyberspace operations and enhance our collective cybersecurity posture.

Reinforce norms of responsible State behavior in cyberspace: The Department will reinforce voluntary, non-binding norms of responsible State behavior in cyberspace during peacetime. The United States has endorsed the work done by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) to develop a

framework of responsible State behavior in cyberspace. The principles developed by the UNGGE include prohibitions against damaging civilian critical infrastructure during peacetime and against allowing national territory to be used for intentionally wrongful cyber activity. The Department will work alongside its interagency and international partners to promote international commitments regarding behavior in cyberspace as well as to develop and implement cyber confidence building measures (CBM). When cyber activities threaten U.S. interests, we will contest them and we will be prepared to act, in conjunction with partners, to defend U.S. interests.

Reform the Department

Incorporate cyber awareness into DoD institutional culture: The Department will adapt its institutional culture so individuals at every level are knowledgeable about the cyberspace domain and can incorporate that knowledge into their day-to-day activities. Leaders and their staffs need to be "cyber fluent" so they can fully understand the cybersecurity implications of their decisions and are positioned to identify opportunities to leverage the cyberspace domain to gain strategic, operational, and tactical advantages.

Increase cybersecurity accountability: Reducing the Department's "attack surface" requires an increase in cybersecurity awareness and accountability across the Department. We will hold DoD personnel and our private sector partners accountable for their cybersecurity practices and choices.

Seek material solutions that are affordable, flexible, and robust: The Department will reduce the time it takes to procure software and hardware in order to keep pace with the rapid advance of technology. We will identify opportunities to procure scalable services, such as cloud storage and scalable computing power, to ensure that our systems keep pace with commercial information technology and can scale when necessary to match changing requirements. We will also leverage COTS capabilities where feasible to reduce our reliance on expensive, custom-built software that is difficult to maintain or upgrade.

Expand crowd-sourced vulnerability identification: The Department will continue to identify crowdsourcing opportunities, such as hack-a-thons and bug-bounties, in order to identify and mitigate vulnerabilities more effectively and to foster innovation.

Cultivate Talent

Sustain a ready cyber workforce: The Department's workforce is a critical cyber asset. We will invest in building future talent, identifying and recruiting sought-after talent, and retaining our current cyber workforce. We will provide ample opportunities—both inside and outside the Department—for the professional development and career progression of cyber personnel. We will create processes for maintaining visibility of the entire military and civilian cyber workforce and optimizing personnel rotations across military departments and commands, including maximizing the use of the Reserve Components. The Department will also ensure that its cyber requirements are filled by the optimal mix of military service members, civilian employees, and contracted support to serve mission requirements.

Enhance the Nation's cyber talent: The Department plays an essential role in enhancing the Nation's pool of cyber talent in order to further the goal of increasing national resilience across the private and public sectors. To that end, we will increase our efforts alongside other Federal departments and agencies to promote science, technology, engineering, mathematics, and foreign language (STEM-L) disciplines at the primary and secondary education levels throughout the United States. The Department will also partner with industry and academia to establish standards in training, education, and awareness that will facilitate the growth of cyber talent in the United States.

Embed software and hardware expertise as a core DoD competency: To make it attractive to skilled candidates, the Department will establish a career track for computer science related specialties (including hardware engineers, software developers, and data analysts) that offers meaningful challenges, rotational billets at other Federal departments and agencies, specialized training opportunities tied to retention commitments, and the expansion of compensation incentives for the Cyber Excepted Service (CES).

Establish a cyber top talent management program: The Department will establish a cyber talent management program that provides its most skilled cyber personnel with focused resources and opportunities to develop key skills over the course of their careers. The Department will use competitive processes, including individual and team competitions, to identify the most capable DoD military and civilian cyber specialists and then empower those personnel to solve the Department's toughest challenges.

Conclusion

The arrival of the cyber era has created new opportunities and challenges for the Department and the Nation. Open and reliable access to information is a vital U.S. interest, and our allies and competitors alike should understand that we will assertively defend it. The *2018 DoD Cyber Strategy* directs the Department to defend forward, shape the day-to-day competition, and prepare for war by building a more lethal force, expanding alliances and partnerships, reforming the Department, and cultivating talent, while actively competing against and deterring our competitors. Taken together, these mutually reinforcing activities will enable the Department to compete, deter, and win in the cyberspace domain.

SOURCE: U.S. Department of Defense, *Summary, Department of Defense Cyber Strategy 2018* (Washington, D.C.: Government Printing Office, 2018), 1–7, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

ANALYSIS

Though the 2018 cyber strategy establishes a number of long-term goals, many of them are not necessarily within the purview of the military. For example, a substantial portion of the document revolves around the training of existing personnel in

better cyber practices and the development of personnel suited for cyber missions. While training programs exist to help current personnel better understand their role in the cyber domain, and how any individual on the department's computer networks can represent a potential threat vector if they practice poor internet hygiene, the vast majority of the department's personnel, military, and civilian are not inherently a part of the cyber mission. Previous attempts to train personnel to be more security-conscious regarding cyber issues have been met with strong resistance, in part because of the clumsy nature of the training modules created for a one-size-fits-all training approach. The initiative to recruit cyber expertise might bear fruit if the department can offer significant enough incentives to compete with private employers—but current federal hiring practices make that a dubious proposition, at best. However the DOD chooses to pursue the personnel necessary to carry out its strategy, it will require the active assistance of many nonmilitary organizations, requiring the creation of mutually beneficial partnerships before it can succeed.

2

U.S. ASSESSMENTS OF CYBER ADVERSARIES

- ***Document 24:*** *Military Power of the People's Republic of China*
- ***When:*** 2009
- ***Where:*** Washington, D.C.
- ***Significance:*** The U.S. Department of Defense (DOD) periodically creates analyses of the military capabilities, intentions, and technological developments of peer contenders and potential adversaries. In recent iterations, the cyber capabilities of those nations have become an increasingly important portion of the reports.

DOCUMENT

Integrated Network Electronic Warfare. PRC military writings highlight the seizure of electromagnetic dominance in the early phases of a campaign as among the foremost tasks to ensure battlefield success. PLA theorists have coined the term "integrated network electronic warfare" to describe the use of electronic warfare, computer network operations, and kinetic strikes to disrupt battlefield network information systems that support an adversary's warfighting and power projection capabilities. PLA writings on future models of joint operations identify "integrated network electronic warfare" as one of the basic forms of "integrated joint operations," suggesting the centrality of seizing and dominating the electromagnetic spectrum in PLA campaign theory.

. . .

Information Warfare. There has been much writing on information warfare among China's military thinkers, who indicate a strong conceptual understanding of its methods and uses. For example, a November 2006 *Liberation Army Daily* commentary outlines:

> *"[The] mechanism to get the upper hand of the enemy in a war under conditions of informatization finds prominent expression in whether or not we are capable of using various means to obtain information and of ensuring the effective circulation of information; whether or not we are capable of making full use of the permeability, sharable property, and connection of information to realize the organic merging of materials, energy, and information to form a combined fighting strength; [and,] whether or not we are capable of applying effective means to weaken the enemy side's information superiority and lower the operational efficiency of enemy information equipment."*

The PLA is investing in electronic countermeasures, defenses against electronic attack (e.g., electronic and infrared decoys, angle reflectors, and false target

generators), and Computer Network Operations (CNO). China's CNO concepts include computer network attack (CNA), computer network exploitation (CNE), and computer network defense (CND). The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks. In 2005, the PLA began to incorporate offensive CNO into its exercises, primarily in first strikes against enemy networks.

. . .

Cyberwarfare Capabilities. In 2008, numerous computer systems around the world, including those owned by the U.S. Government, continued to be the target of intrusions that appear to have originated within the PRC. Although these intrusions focused on exfiltrating information, the accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks. It remains unclear if these intrusions were conducted by, or with the endorsement of, the PLA or other elements of the PRC Government. However, developing capabilities for cyberwarfare is consistent with authoritative PLA military writings on the subject. Publicized 2008 attacks by suspected PRC actors include:

- In April 2008, Indian Government officials confirmed that its Ministry of External Affairs' computer network and servers were the victims of intrusions that appeared to originate in China.
- In May 2008, the Belgian Government reported that it had been targeted by PRC hackers multiple times.
- In May 2008, U.S. authorities investigated whether PRC officials secretly copied contents of a U.S. Government laptop during a visit to China by the U.S. Commerce Secretary and used the information to try to penetrate into Commerce computers. The investigation is ongoing.

SOURCE: U.S. Department of Defense, *Military Power of the People's Republic of China 2009* (Washington, D.C.: Government Printing Office, 2009), 13, 27–28, 52–53, https://dod.defense.gov/Portals/1/Documents/pubs/China_Military_Power_Report_2009.pdf

ANALYSIS

The 2009 iteration of the U.S. DOD's periodic reports on Chinese military developments noted that Chinese hackers had become more aggressive in targeting Western nations for espionage operations. However, the largest and longest Chinese cyber espionage campaigns had not been detected yet, meaning the authors were unaware that at the time of the report, Chinese hackers had infiltrated defense contractors and a host of major industrial corporations, stealing large amounts of technical data, construction specifications, and competitive bids for international development rights. Unfortunately, the DOD had woefully underestimated Chinese capabilities and intentions in its 2009 report, and had instead focused on the noncyber aspects of Chinese military power.

- ***Document 25:*** *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*
- ***When:*** October 9, 2009
- ***Where:*** McLean, VA
- ***Significance:*** Northrop Grumman is a major defense contractor within the United States. In addition to producing hardware, including major weapons systems, the company also provides analytical services on a contract basis. In 2009, Northrop Grumman analysts provided an assessment of the Chinese capabilities and intentions in cyberspace, which correctly predicted a growing threat from Chinese cyberattacks targeting American infrastructure and defense contractors.

DOCUMENT

The government of the People's Republic of China (PRC) is a decade into a sweeping military modernization program that has fundamentally transformed its ability to fight high tech wars. The Chinese military, using increasingly networked forces capable of communicating across service arms and among all echelons of command, is pushing beyond its traditional missions focused on Taiwan and toward a more regional defense posture. This modernization effort, known as informationization, is guided by the doctrine of fighting "Local War Under Informationized Conditions," which refers to the PLA's ongoing effort to develop a fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the electromagnetic spectrum.

This doctrinal focus is providing the impetus for the development of an advanced IW [Information Warfare] capability, the stated goal of which is to establish control of an adversary's information flow and maintain dominance in the battlespace. Increasingly, Chinese military strategists have come to view information dominance as the precursor for overall success in a conflict. The growing importance of IW to China's People's Liberation Army (PLA) is also driving it to develop more comprehensive computer network exploitation (CNE) techniques to support strategic intelligence collection objectives and to lay the foundation for success in potential future conflicts.

One of the chief strategies driving the process of informatization in the PLA is the coordinated use of CNO, electronic warfare (EW), and kinetic strikes designed to strike an enemy's networked information systems, creating "blind spots" that various PLA forces could exploit at predetermined times or as the tactical situation warranted. Attacks on vital targets such as an adversary's intelligence, surveillance, and

reconnaissance (ISR) systems will be largely the responsibility of EW and counterspace forces with an array of increasingly sophisticated jamming systems and antisatellite (ASAT) weapons. Attacks on an adversary's data and networks will likely be the responsibility of dedicated computer network attack and exploitation units.

The Chinese have adopted a formal IW strategy called "Integrated Network Electronic Warfare" (INEW) that consolidates the offensive mission for both computer network attack (CNA) and EW under PLA General Staff Department's (GSD) 4th Department (Electronic Countermeasures) while the computer network defense (CND) and intelligence gathering responsibilities likely belong to the GSD 3rd Department (Signals Intelligence), and possibly a variety of the PLA's specialized IW militia units.

This strategy, which relies on a simultaneous application of electronic warfare and computer network operations against an adversary's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) networks and other essential information systems, appears to be the foundation for Chinese offensive IW. Analysis of this strategy suggests that CNO tools will be widely employed in the earliest phases of a conflict, and possibly preemptively against an enemy's information systems and C4ISR systems.

The PLA is training and equipping its force to use a variety of IW tools for intelligence gathering and to establish information dominance over its adversaries during a conflict. PLA campaign doctrine identifies the early establishment of information dominance over an enemy as one of the highest operational priorities in a conflict; INEW appears designed to support this objective.

The PLA is reaching out across a wide swath of Chinese civilian sector to meet the intensive personnel requirements necessary to support its burgeoning IW capabilities, incorporating people with specialized skills from commercial industry, academia, and possibly select elements of China's hacker community. Little evidence exists in open sources to establish firm ties between the PLA and China's hacker community, however, research did uncover limited cases of apparent collaboration between more elite individual hackers and the PRC's civilian security services. The caveat to this is that amplifying details are extremely limited and these relationships are difficult to corroborate.

China is likely using its maturing computer network exploitation capability to support intelligence collection against the US Government and industry by conducting a long term, sophisticated, computer network exploitation campaign. The problem is characterized by disciplined, standardized operations, sophisticated techniques, access to high-end software development resources, a deep knowledge of the targeted networks, and an ability to sustain activities inside targeted networks, sometimes over a period of months.

Analysis of these intrusions is yielding increasing evidence that the intruders are turning to Chinese "black hat" programmers (i.e. individuals who support illegal hacking activities) for customized tools that exploit vulnerabilities in software that vendors have not yet discovered. This type of attack is known as a "zero day exploit" (or "0-day") as the defenders haven't yet started counting the days since the release of vulnerability information. Although these relationships do not prove any government affiliation, it suggests that the individuals participating in ongoing penetrations

of US networks have Chinese language skills and have well established ties with the Chinese underground hacker community. Alternately, it may imply that the individuals targeting US networks have access to a well resourced infrastructure that is able to broker these relationships with the Chinese blackhat hacker community and provide tool development support often while an operation is underway.

The depth of resources necessary to sustain the scope of computer network exploitation targeting the US and many countries around the world coupled with the extremely focused targeting of defense engineering data, US military operational information, and China-related policy information is beyond the capabilities or profile of virtually all organized cybercriminal enterprises and is difficult at best without some type of state-sponsorship.

The type of information often targeted for exfiltration has no inherent monetary value to cybercriminals like credit card numbers or bank account information. If the stolen information is being brokered to interested countries by a third party, the activity can still technically be considered "state-sponsored," regardless of the affiliation of the actual operators at the keyboard.

The US information targeted to date could potentially benefit a nation-state defense industry, space program, selected civilian high technology industries, foreign policymakers interested in US leadership thinking on key China issues, and foreign military planners building an intelligence picture of US defense networks, logistics, and related military capabilities that could be exploited during a crisis. The breadth of targets and range of potential "customers" of this data suggests the existence of a collection management infrastructure or other oversight to effectively control the range of activities underway, sometimes nearly simultaneously.

In a conflict with the US, China will likely use its CNO capabilities to attack select nodes on the military's Non-classified Internet Protocol Router Network (NIPRNET) and unclassified DoD and civilian contractor logistics networks in the continental US (CONUS) and allied countries in the Asia-Pacific region. The stated goal in targeting these systems is to delay US deployments and impact combat effectiveness of troops already in theater.

No authoritative PLA open source document identifies the specific criteria for employing computer network attack against an adversary or what types of CNO actions PRC leaders believe constitutes an act of war.

Ultimately, the only distinction between computer network exploitation and attack is the intent of the operator at the keyboard: The skill sets needed to penetrate a network for intelligence gathering purposes in peacetime are the same skills necessary to penetrate that network for offensive action during wartime. The difference is what the operator at that keyboard does with (or to) the information once inside the targeted network. If Chinese operators are, indeed, responsible for even some of the current exploitation efforts targeting US Government and commercial networks, then they may have already demonstrated that they possess a mature and operationally proficient CNO capability.

SOURCE: Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA: Northrop Grumman Corporation for the USCC, 2009), 6–9, https://web.archive.org

/web/20110203052113/http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

ANALYSIS

The Chinese government tends to view cyber warfare as part of a larger "informatization" approach to conflict. Under this concept, one of the fundamental goals of any combatant commander is to control the flow of information by engaging in substantial deception operations, devoting a major share of resources to intelligence collection and analysis, and attempting to disrupt the enemy's ability to accurately sense and assess the battlefield environment. While the United States will often utilize the term "information operations" to signify more than simply the exploitation of computer networks through cyberattack, Chinese doctrine calls for essentially treating information as a weapon, and wielding it in the most advantageous fashion to coerce or deter adversaries without undertaking the risks of physical confrontations. Cyber operations are an important subset of both informatization and information operations and allow the movement of enormous volumes of data, as well as an opportunity to transform the information available to an opponent. By changing the opponent's perceptions through data alteration, a commander might very well alter that opponent's decision of how to conduct physical operations, and even paralyze their ability to engage in combat due to a lack of sensory awareness.

- ***Document 26:*** *Mandiant APT1 Report: Exposing One of China's Cyber Espionage Units*
- ***When:*** February 18, 2013
- ***Where:*** Alexandria, VA
- ***Significance:*** Kevin Mandia, the founder of Mandiant Corporation (now known as FireEye Mandiant), served in the United States Air Force before forming his cybersecurity company. His company provided cyber defense to hundreds of U.S.-based companies, and noticed a coordinated attack upon dozens of companies that appeared to originate in the People's Republic of China. After several years of studying the threat, Mandiant Corporation released its report, as well as the underpinning evidence for its conclusions, accusing the Chinese military of conducting a sophisticated campaign of cyber espionage.

DOCUMENT

Executive Summary

Since 2004, Mandiant has investigated computer security breaches at hundreds of organizations around the world. The majority of these security breaches are attributed to advanced threat actors referred to as the "Advanced Persistent Threat" (APT). We first published details about the APT in our January 2010 M-Trends report. As we stated in the report, our position was that "The Chinese government may authorize this activity, but there's no way to determine the extent of its involvement." Now, three years later, we have the evidence required to change our assessment. The details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them.[1]

Mandiant continues to track dozens of APT groups around the world; however, this report is focused on the most prolific of these groups. We refer to this group as "APT1" and it is one of more than 20 APT groups with origins in China. APT1 is a single organization of operators that has conducted a cyber espionage campaign against a broad range of victims since at least 2006. From our observations, it is one of the most prolific cyber espionage groups in terms of the sheer quantity of information stolen. The scale and impact of APT1's operations compelled us to write this report.

The activity we have directly observed likely represents only a small fraction of the cyber espionage that APT1 has conducted. Though our visibility of APT1's activities is incomplete, we have analyzed the group's intrusions against nearly 150 victims over seven years. From our unique vantage point responding to victims, we tracked APT1 back to four large networks in Shanghai, two of which are allocated directly to the Pudong New Area. We uncovered a substantial amount of APT1's attack infrastructure, command and control, and modus operandi (tools, tactics, and procedures). In an effort to underscore there are actual individuals behind the keyboard, Mandiant is revealing three personas we have attributed to APT1. These operators, like soldiers, may merely be following orders given to them by others.

Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support. In seeking to identify the organization behind this activity, our research found that People's Liberation Army (PLA's) Unit 61398 is similar to APT1 in its mission, capabilities, and resources. PLA Unit 61398 is also located in precisely the same area from which APT1 activity appears to originate.

Key Findings

APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (总参三部二局), which is

[1] Our conclusions are based exclusively on unclassified, open source information derived from Mandiant observations. None of the information in this report involves access to or confirmation by classified intelligence.

most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (61398部队).

- The nature of "Unit 61398's" work is considered by China to be a state secret; however, we believe it engages in harmful "Computer Network Operations."
- Unit 61398 is partially situated on Datong Road (大同路) in Gaoqiaozhen (高桥镇), which is located in the Pudong New Area (浦东新区) of Shanghai (上海). The central building in this compound is a 130,663 square foot facility that is 12 stories high and was built in early 2007.
- We estimate that Unit 61398 is staffed by hundreds, and perhaps thousands of people based on the size of Unit 61398's physical infrastructure.
- China Telecom provided special fiber optic communications infrastructure for the unit in the name of national defense.
- Unit 61398 requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language.
- Mandiant has traced APT1's activity to four large networks in Shanghai, two of which serve the Pudong New Area where Unit 61398 is based.

APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.[2]

- Since 2006, Mandiant has observed APT1 compromise 141 companies spanning 20 major industries.
- APT1 has a well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property.
- Once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership.

DID YOU KNOW?

People's Liberation Army Unit 61398

The People's Liberation Army (PLA) has a long history of engaging in cyber espionage acts that might be considered cyber warfare. Unit 61398, also known as the Third Office of the PLA General Staff Department Third Department Second Bureau, is headquartered in a twelve-story office building in Shanghai. Its existence was disclosed by a 2013 report released by the Mandiant Corporation, which designated the PLA organization as an advanced persistent threat (APT). The company had first begun investigations of Unit 61398 as part of an attempt to counter and attribute attacks against the *New York Times*, which had published a series of articles critical of an outgoing Chinese prime minister.

The Mandiant *APT1 Report* offered alternative explanations for the phenomena it described, before ultimately concluding that the Shanghai-based Unit 61398 was almost certainly responsible for a series of long-running cyber campaigns against Western targets. Members of the unit appear to be well-trained in social engineering techniques as well as the use of spearphishing attacks and hacker toolkits. Although it is difficult to narrow down responsibility for specific actions in such a secretive unit, the United States indicted five military officers from Unit 61398 in 2014. The indictments indicated that the officers were heading cyber espionage campaigns against private U.S. corporations, and were the first time a state actor has been legally charged with carrying out a criminal cyberattack.

[2] We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has conducted. Therefore, Mandiant is establishing the lower bounds of APT1 activities in this report.

- APT1 uses some tools and techniques that we have not yet observed being used by other groups including two utilities designed to steal email—GETMAIL and MAPIGET.
- APT1 maintained access to victim networks for an average of 356 days.[3] The longest time period APT1 maintained access to a victim's network was 1,764 days, or four years and ten months.
- Among other large-scale thefts of intellectual property, we have observed APT1 stealing 6.5 terabytes of compressed data from a single organization over a ten-month time period.
- In the first month of 2011, APT1 successfully compromised at least 17 new victims operating in 10 different industries.

APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries.

- Of the 141 APT1 victims, 87% of them are headquartered in countries where English is the native language.
- The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.

APT1 maintains an extensive infrastructure of computer systems around the world.

- APT1 controls thousands of systems in support of their computer intrusion activities.
- In the last two years we have observed APT1 establish a minimum of 937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries. The majority of these 849 unique IP addresses were registered to organizations in China (709), followed by the U.S. (109).
- In the last three years we have observed APT1 use fully qualified domain names (FQDNs) resolving to 988 unique IP addresses.
- Over a two-year period (January 2011 to January 2013) we confirmed 1,905 instances of APT1 actors logging into their attack infrastructure from 832 different IP addresses with Remote Desktop, a tool that provides a remote user with an interactive graphical interface to a system.
- In the last several years we have confirmed 2,551 FQDNs attributed to APT1.

In over 97% of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language.

- In 1,849 of the 1,905 (97%) of the Remote Desktop sessions APT1 conducted under our observation, the APT1 operator's keyboard layout setting was "Chinese (Simplified)—US Keyboard." Microsoft's Remote Desktop client configures this setting automatically based on the selected

[3] This is based on 91 of 141 victim organizations. In the remaining cases, APT1 activity is either ongoing or else we do not have visibility into the last known date of APT1 activity in the network.

language on the client system. Therefore, the APT1 attackers likely have their Microsoft® operating system configured to display Simplified Chinese fonts.

- 817 of the 832 (98%) IP addresses logging into APT1 controlled systems using Remote Desktop resolved back to China.
- We observed 767 separate instances in which APT1 intruders used the "HUC Packet Transmit Tool" or HTRAN to communicate between 614 distinct routable IP addresses and their victims' systems using their attack infrastructure. Of the 614 distinct IP addresses used for HTRAN communications:
  - 614 of 614 (100%) were registered in China.
  - 613 (99.8%) were registered to one of four Shanghai net blocks.

The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators.

- We conservatively estimate that APT1's current attack infrastructure includes over 1,000 servers.
- Given the volume, duration and type of attack activity we have observed, APT1 operators would need to be directly supported by linguists, open source researchers, malware authors, industry experts who translate task requests from requestors to the operators, and people who then transmit stolen information to the requestors.
- APT1 would also need a sizable IT staff dedicated to acquiring and maintaining computer equipment, people who handle finances, facility management, and logistics (e.g., shipping).

In an effort to underscore that there are actual individuals behind the keyboard, Mandiant is revealing three personas that are associated with APT1 activity.

- The first persona, "UglyGorilla," has been active in computer network operations since October 2004. His activities include registering domains attributed to APT1 and authoring malware used in APT1 campaigns. "UglyGorilla" publicly expressed his interest in China's "cyber troops" in January 2004.
- The second persona, an actor we call "DOTA," has registered dozens of email accounts used to conduct social engineering and spear phishing attacks in support of APT1 campaigns. "DOTA" used a Shanghai phone number while registering these accounts.
- We have observed both the "UglyGorilla" persona and the "DOTA" persona using the same shared infrastructure, including FQDNs and IP ranges that we have attributed to APT1.
- The third persona, who uses the nickname "SuperHard," is the creator or a significant contributor to the AURIGA and BANGAT malware families which we have observed APT1 and other APT groups use. "SuperHard" discloses his location to be the Pudong New Area of Shanghai.

Mandiant is releasing more than 3,000 indicators to bolster defenses against APT1 operations.

- Specifically, Mandiant is providing the following:
  - Digital delivery of over 3,000 APT1 indicators, such as domain names, IP addresses, and MD5 hashes of malware.
  - Sample Indicators of Compromise (IOCs) and detailed descriptions of over 40 families of malware in APT1's arsenal of digital weapons.
  - Thirteen (13) X.509 encryption certificates used by APT1.
  - A compilation of videos showing actual attacker sessions and their intrusion activities.
- While existing customers of Mandiant's enterprise-level products, Mandiant Managed Defense and Mandiant Intelligent Response, have had prior access to these APT1 Indicators, we are also making them available for use with Redline, our free host-based investigative tool. Redline can be downloaded at http://www.mandiant.com/ resources/download/redline.

Conclusion

The sheer scale and duration of sustained attacks against such a wide set of industries from a singularly identified group based in China leaves little doubt about the organization behind APT1. We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398. However, we admit there is one other unlikely possibility:

> A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission.

Why We Are Exposing APT1

The decision to publish a significant part of our intelligence about Unit 61398 was a painstaking one. What started as a "what if" discussion about our traditional non-disclosure policy quickly turned into the realization that the positive impact resulting from our decision to expose APT1 outweighed the risk to our ability to collect intelligence on this particular APT group. It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively. The issue of attribution has always been a missing link in publicly understanding the landscape of APT cyber espionage. Without establishing a solid connection to China, there will always be room for observers to dismiss APT actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns. We hope that this report will lead to increased understanding and coordinated action in countering APT network breaches.

At the same time, there are downsides to publishing all of this information publicly. Many of the techniques and technologies described in this report are vastly

more effective when attackers are not aware of them. Additionally, publishing certain kinds of indicators dramatically shortens their lifespan. When Unit 61398 changes their techniques after reading this report, they will undoubtedly force us to work harder to continue tracking them with such accuracy. It is our sincere hope, however, that this report can temporarily increase the costs of Unit 61398's operations and impede their progress in a meaningful way.

We are acutely aware of the risk this report poses for us. We expect reprisals from China as well as an onslaught of criticism.

SOURCE: FireEye Corporation, *Mandiant APT1 Report: Exposing One of China's Cyber Espionage Units, 2013, Executive Summary*. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf. Used by permission of FireEye Mandiant. Please note that this is a historical document; for current content on China APTs, follow their website at www.fireeye.com

ANALYSIS

By not only lodging an accusation against the People's Liberation Army but also providing the specific evidence to support the accusation, Mandiant essentially forced the U.S. government to react to the cyberattacks against a wide variety of private and public interests. Although Mandiant held some contracts with the federal government, it was in no way controlled by governmental interests—which leads to the conclusion that this report was written either to serve the public interest or to trigger the intervention of state assets to defend nonstate interests. Less than a year after the report was issued, Mandia sold his company to FireEye in a $1 billion transaction.

The APT1 Report was unprecedented in size, scope, and willingness to expose specific malicious actors in cyberspace. In addition to warning potential victims about the activities of the PLA cyber unit, it served to demonstrate the weaknesses of that unit's ability to prevent the detection and tracking of its intrusive activities. In particular, because the report included direct accusations regarding which unit of the Chinese military was conducting the attacks, and from where, it illustrated that the cyber experts from Mandiant had more than enough capability to discover and backtrack the Chinese intrusions, even if it did not have the legal authority to conduct any offensive operations.

- ***Document 27:*** *Military and Security Developments Involving the Democratic People's Republic of Korea*
- ***When:*** 2013
- ***Where:*** Washington, D.C.
- ***Significance:*** The U.S. DOD periodically creates analyses of the military capabilities, intentions, and technological developments

of peer contenders and potential adversaries. In recent iterations, the cyber capabilities of those nations have become an increasingly important portion of the reports.

DOCUMENT

Cyberwarfare Capabilities. North Korea probably has a military offensive cyber operations (OCO) capability. Implicated in malicious cyber activity and cyber effects operations since 2009, North Korea may view OCO as an appealing platform from which to collect intelligence and cause disruption in South Korea.

- From 2009 to 2011, North Korea was allegedly responsible for a series of distributed denial of service attacks against South Korean commercial, government, and military websites, rendering them briefly inaccessible.
- North Korea was allegedly behind two separate cyberattacks in 2013, which targeted South Korean banking, media, and governmental networks, resulting in the erasure of critical data.

Given North Korea's bleak economic outlook, OCO may be seen as a cost-effective way to develop asymmetric, deniable military options. Because of North Korea's historical isolation from outside communications and influence, it is also likely to use internet infrastructure from third-party nations. This increases the risk of destabilizing actions and escalation on and beyond the Korean Peninsula.

. . .

Intelligence Services. North Korea leverages information collected by four intelligence organizations to plan and formulate internal policy and to undermine the political stability of South Korea. North Korean intelligence and security services collect political, military, economic, and technical information through open-source, human intelligence, and signals intelligence capabilities. North Korea's primary intelligence collection targets are South Korea, the United States, and Japan.

The Ministry of State Security (MSS) is North Korea's primary counterintelligence service and is an autonomous agency of the North Korean government reporting directly to Kim Jong Un. The MSS is responsible for operating North Korean prison camps, investigating cases of domestic espionage, repatriating defectors, and conducting overseas counterespionage activities.

The United Front Department (UFD) overtly attempts to establish pro-North Korean groups in South Korea such as the Korean Asia-Pacific Committee and the Ethnic Reconciliation Council. The UFD is also the primary department involved in managing inter-Korean dialogue and North Korea's policy toward the South.

North Korea's Reconnaissance General Bureau (RGB) is responsible for clandestine operations. The RGB includes six bureaus charged with operations, reconnaissance, technology and cyber, overseas intelligence, inter-Korean talks, and service support.

The 225th Bureau is responsible for training agents, infiltrating South Korea, and establishing underground political parties focused on fomenting unrest and revolution.

Command and Control. The DPRK National Defense Commission (NDC) is the symbolic nominal authority over the North's military and security services. The Ministry of Peoples Armed Forces (MPAF) is the administrative superior of the KPA, while operational command and control is exercised by its subordinate General Staff Department. The 1992 constitution gives control of the North's military to the NDC, and Kim Jong Un exercises control of the military as "first chairman" of the NDC and supreme commander of the KPA. Kim Jong Un further exercises control as first secretary of the Korean Worker's Party (KWP) and chairman of the KWP's Central Military Commission.

Telecommunications. North Korea has a nationwide fiber-optic network, and has invested in a modern nationwide cellular network. However, telecommunication services and access are strictly controlled, and all networks are available for military use, if necessary.

Cell phone subscribership increased beyond 2 million with the growth of Koryolink, North Korea's 3G cellular network. Mobile phone users consist primarily of high-ranking officials in Pyongyang and their families, though ownership is beginning to spread into smaller cities and towns. Most cell phones cannot access the internet and can only make calls within North Korea.

North Koreans are restricted from using the internet, but are able to access the national intranet, which is insulated from the World Wide Web. The intranet hosts government-approved websites, including Korean Central News Agency and North Korean propaganda website Uriminzokkiri.

SOURCE: U.S. Department of Defense, *Military and Security Developments Involving the Democratic People's Republic of Korea 2013* (Washington, D.C.: Government Printing Office, 2013), 11, 13–14, https://dod.defense.gov/Portals/1/Documents/pubs/North_Korea_Military_Power_Report_2013-2014.pdf

DID YOU KNOW?

Office of Personnel Management Data Breach

In April 2015, the U.S. Office of Personnel Management (OPM) detected a massive data breach of background investigation records. More than twenty million current and former federal government employees were directly affected by the breach, as were tens of millions of family members and professional contacts whose information was also exposed. The resulting investigation demonstrated that OPM's efforts to streamline and standardize hiring practices created a significant vulnerability to outside actors. Throughout 2014, a series of smaller breaches exposed thousands of employees' records, but none of the OPM leadership recognized that the smaller events probably signified a larger campaign to gain full access to OPM records. During the earlier breaches, hackers stole login and password data for OPM personnel, allowing further access to the massive database. The hackers involved in the breach exfiltrated Electronic Questionnaires for Investigations Processing (e-QIP) forms, which included information about personal finances, previous addresses, criminal records, Social Security numbers, and digitized copies of fingerprints. In short, the system was almost tailor-made to empower identify theft on a massive scale. The hack was so large that most investigators believe it was the work of a nation-state, most likely the People's Republic of China, although the Obama administration did not choose to publicly accuse China of carrying out the attack.

ANALYSIS

Although this report notes an increasing sophistication in North Korean cyber capabilities and suggests that the reclusive nation might be interested in launching cyberattacks against Western targets, the report did not draw the conclusion that

North Korea was on the verge of launching a wave of cyber sabotage and extortion attacks. In 2014, North Korean cyber operations targeted Sony Pictures Corporation, stealing enormous volumes of data, defacing websites, and destroying hardware systems. Three years later, North Korean cyberattacks managed to implant ransomware in dozens of Western locations, demanding cryptocurrency payments in exchange for releasing encrypted data on infected machines. Reportedly, even victims who chose to pay the demanded ransom did not recover their encrypted data, suggesting that the North Korean attackers wished to inflict as much damage as possible while extracting whatever payments they could coerce.

- ***Document 28:*** *China and International Law in Cyberspace*
- ***When:*** May 6, 2014
- ***Where:*** Washington, D.C.
- ***Significance:*** For more than a decade prior to 2014, the Chinese government actively encouraged its citizens, including members of its military, to engage in cyberattacks that undoubtedly violated international laws governing espionage, sabotage, and intellectual property. However, in the early 2010s, the Chinese attitude toward such attacks seemed to gradually shift, which might signal an impending change in Chinese behavior in cyberspace.

DOCUMENT

Domestic Cyber Policy in China and Implications for Development of International Norms

China has until recently developed and executed cyber policies without a coordinated approach to cyberspace. Since the early 2010s, however, China has begun to increase interagency coordination on cyber policy. This may be a response to the increasing number and sophistication of internet users in China, the perceived role of the internet in fueling social and political movements in China and in the "color revolutions" of the late 2000s, and the growing need to align foreign and domestic policy priorities in cyberspace.

In late February 2014, China announced a new Central Internet Security and Informatization Leading Group. President Xi Jinping chairs the leading group, reflecting the importance Beijing ascribes to the issue. Leading groups are deliberative committees at the top levels of the CCP [Chinese Communist Party] that influence policy through their coordinating function and recommendations to the Politburo Standing Committee, the top-level decision-making body in China. The new cyber leading group is tasked with drafting a national cybersecurity strategy

and the coordination of cybersecurity across multiple government entities, including the Ministry of Public Security, State Encryption Bureau, Ministry of State Security, Ministry of Industry and Information Technology, and the PLA. The establishment of this body indicates China likely is developing a national-level cyber policy, and by extension an authoritative viewpoint on the applicability of legal principles to cyberspace.

As China and other countries have not yet crystallized their positions on various aspects of international law in cyberspace, the 2014 GGE meeting is an opportunity for the United States to continue to socialize cyberspace norms internationally. According to Christopher Painter, Coordinator for Cyber Issues at the U.S. Department of State, the upcoming meeting will "look more closely at how international law applies to state-on-state conduct in cyberspace." In addition, the GGE will discuss "additional norms of responsible state behavior, grounded in existing international law, that apply to the spectrum of cyber activity that falls below the use-of-force threshold." In the intervening year since the last meeting, revelations about the United States' cyber espionage activities, particularly those against China, have further fraught the cyberspace policy discussion between the United States and China with tension. The United States distinguishes between China's "cyber-enabled economic espionage" against U.S. companies and government-to-government espionage for state purposes, whereas China does not recognize this distinction. Having laid significant groundwork in 2013, the GGE now faces the challenge of consensus on the more divisive and difficult policy issues in cyberspace.

SOURCE: Kimberly Hsu and Craig Murray, *China and International Law in Cyberspace* (Washington, D.C.: U.S.-China Economic and Security Review Commission, 2014), 5–6, https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf

DID YOU KNOW?

Operation Orchard

In 2007, Israel Defence Force aircraft launched a massive airstrike against a Syrian nuclear enrichment facility located near Deir es-Zor. The attacking aircraft did not possess stealth characteristics, and hence should have been vulnerable to Syria's Russian-built state-of-the-art integrated air defense system. Yet, it seems that the Syrian military's first indication of the attack was the impact of precision munitions upon the target. Later investigations suggested that the Israelis had carried out a cyberattack against Syrian radar sites, rendering them incapable of detecting the Israeli warplanes. Syria barely lodged a protest against the attack, other than to note that Israel had attacked a nonmilitary building. Interestingly, the loudest protests came from the People's Democratic Republic of Korea, which had almost certainly supplied technical personnel and hardware for the construction of the site. Soon after the attack, the Syrian government bulldozed the site, eliminating any evidence of its original purpose.

ANALYSIS

There are a number of potential explanations for changing Chinese behavior in the cyber domain. One is that the Chinese government finds it advantageous to reduce its cyberattacks to obtain favorable treatment or conditions in other fashions. Another is that the number of Chinese citizens using the internet has grown, and hence China might be more vulnerable to attacks from outside its territory—meaning that it has more to lose from cyberattacks than in earlier years. A third explanation might simply be that the Chinese government believes the establishment of reasonable norms governing cyberspace behavior is to the mutual benefit of

all nations. Regardless of the causes, though, if the Chinese government is becoming more interested in developing and adhering to international laws in cyberspace, it is likely to reduce the total number of cyberattacks faced by the United States as a side effect, making it in the best interests of the United States to encourage such developments.

- ***Document 29:*** *Military and Security Developments Involving the People's Republic of China*
- ***When:*** 2014
- ***Where:*** Washington, D.C.
- ***Significance:*** The U.S. DOD periodically analyzes the military capabilities, intentions, and technological developments of peer contenders and potential adversaries. In recent iterations, the cyber capabilities of those nations have become an increasingly important portion of the reports.

DOCUMENT

Chinese Engagement on International Cyber Issues. China has increased diplomatic engagement and advocacy in multilateral and international fora where cyber issues are discussed and debated. China's agenda is frequently in line with Russia's efforts to promote more intergovernmental control over cyberspace. China and Russia continue to promote an Information Security Code of Conduct that advances a state-centric concept of cyberspace and seeks to impose state control of content in cyberspace. Given the growing consensus on the need for cyber transparency and confidence-building measures in international fora such as the ASEAN Regional Forum and the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), China may be willing to play a more constructive role in these efforts. Notably, in June 2013, China joined a landmark consensus of the UN GGE that addressed three fundamental issues: (1) confirmed that existing international law, including the UN Charter, applies to cyberspace and that the law of state responsibility should guide state behavior with regard to the use of cyberspace; (2) expressed the need to promote international stability, transparency, and confidence in cyberspace; and (3) explored how the international community can help build the cybersecurity capacity of less-developed states.

. . .**Building an Informationized Military.** Chinese military writings describe informationized warfare as an asymmetric form of warfare used to defeat a

technologically superior, information-dependent adversary through dominance of the battlefield's information space. Information operations encompass defensive and offensive military actions and focus on defending PLA information systems, while disrupting or destroying an adversary's information systems. Chinese writings view informationized warfare as a way to weaken an adversary's ability to acquire, transmit, process, and use information during war and discuss it as a way to force an adversary to capitulate before the onset of conflict. The PLA conducts military exercises simulating operations in complex electromagnetic environments and likely views conventional and cyber operations as a means of achieving information dominance. The PLA GSD Fourth Department (Electronic Countermeasures and Radar) would likely use jamming and electronic warfare, cyberspace operations, and deception to augment counterspace and other kinetic operations during a wartime scenario to deny an adversary's use of information systems. "Simultaneous and parallel" operations would involve strikes against U.S. warships, aircraft, and associated supply craft, as well as the use of information attacks to hamper tactical and operational communications and computer networks. These operations could have a significant effect upon an adversary's navigational and targeting radars.

. . .

Cyber Activities Directed against the U.S. Department of Defense. In 2013, numerous computer systems around the world, including those owned by the U.S. Government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military. These intrusions were focused on exfiltrating information. China is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs. The information targeted could potentially be used to benefit China's defense industry, high-technology industries, policymakers' interest in U.S. leadership thinking on key China issues, and military planners' understanding of U.S. defense networks, logistics, and related military capabilities that could be exploited during a crisis. The accesses and skills required for these intrusions are similar to those necessary to conduct computer network attacks.

Cyber Warfare in China's Military. China's 2010 Defense White Paper noted China's own concern over foreign cyber warfare efforts and highlighted the importance of cybersecurity in China's national defense. Cyber warfare could support Chinese military operations in three key areas. First, it will enable data collection for intelligence and computer network attack. Second, it constrains an adversary's actions or slows their response. Third, it is as a force multiplier when coupled with kinetic attacks.

DID YOU KNOW?

JPMorgan Chase Hack

In 2014, hackers launched a cyberattack against JPMorgan Chase that compromised over 80 million accounts with the massive investment firm. The vast majority of accounts were held by individual households, although almost 10 percent of affected accounts belonged to small businesses. Although JPMorgan Chase's cybersecurity teams realized that they had been hacked in July, the company did not disclose the attacks until September, and did not manage to halt the attacks for more than a month after they were discovered. Eventually, the corporation reported their findings to the Federal Bureau of Investigations (FBI), which indicted four men in November 2015 for their role in the attacks. Two of the men, Gery Shalon and Zic Orenstein, were Israeli citizens who were extradited to face prosecution in 2016. Although the attackers did not manage to gain access to Social Security numbers or account passwords, they still managed to capture significant amounts of sensitive and valuable data.

Developing cyber capabilities for warfare is consistent with authoritative PLA military writings. Two military doctrinal writings, *Science of Strategy*, and *Science of Campaigns*, identify information warfare (IW) as integral to achieving information superiority and an effective means for countering a stronger foe. Although neither document identifies the specific criteria for employing computer network attack against an adversary, both advocate developing capabilities to compete in this medium. The *Science of Strategy* and *Science of Campaigns* detail the effectiveness of IW and CNO in conflicts and advocate targeting adversary C2 and logistics networks to affect their ability to operate during the early stages of conflict. As *Science of Strategy* explains, "In the information war, the command and control system is the heart of information collection, control, and application on the battlefield. It is also the nerve center of the entire battlefield."

SOURCE: U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2014* (Washington, D.C.: Government Printing Office, 2014), 11–12, 32–35, https://dod.defense.gov/Portals/1/Documents/pubs/2014_DoD_China_Report.pdf

ANALYSIS

The United States clearly regards the People's Republic of China as one of its foremost competitors in cyberspace and possibly the greatest current cyber threat to American interests. As such, it is unsurprising that the U.S. DOD continuously monitors Chinese activities and intentions in cyberspace. By 2014, it was evident that the Chinese government felt empowered to launch large-scale attacks against U.S. government agencies, private corporations, and individual citizens, in part because the United States seemed unwilling to retaliate in any overt fashion. Warnings regarding Chinese capabilities and intentions in cyberspace did little to alter U.S. behaviors, both in terms of cybersecurity and offensive actions against Chinese targets. It is possible that American retaliation was carried out in such a fashion as to remain undetected by the Chinese government—but it is also possible that the United States chose to exercise restraint and not engage in cyberattacks that might be perceived as an escalation of burgeoning conflict between the two major powers.

- ***Document 30:*** *Cybersecurity Law of the People's Republic of China*
- ***When:*** November 6, 2016
- ***Where:*** Beijing, People's Republic of China
- ***Significance:*** As part of changing Chinese behavior in cyberspace, the Chinese government issued a series of regulations and guidelines for public and private organizations within the People's Republic of China. The regulations included a substantial commitment to

cybersecurity, suggesting that China may have been the target of increased cyberattacks in recent years in contrast to earlier periods of relative immunity from cyber intrusions.

DOCUMENT

Chapter III: Network Operations Security
Section 1: Ordinary Provisions

Article 21: The State implements a cybersecurity multi-level protection system [MLPS]. Network operators shall perform the following security protection duties according to the requirements of the cybersecurity multi-level protection system to ensure the network is free from interference, damage, or unauthorized access, and to prevent network data leaks, theft, or falsification:

(1) Formulate internal security management systems and operating rules, determine persons who are responsible for cybersecurity, and implement cybersecurity protection responsibility;
(2) Adopt technical measures to prevent computer viruses, cyber attacks, network intrusions, and other actions endangering cybersecurity;
(3) Adopt technical measures for monitoring and recording network operational statuses and cybersecurity incidents, and follow provisions to store network logs for at least six months;
(4) Adopt measures such as data classification, backup of important data, and encryption;
(5) Other obligations provided by law or administrative regulations.

Article 22: Network products and services shall comply with the relevant national and mandatory requirements. Providers of network products and services must not install malicious programs; when discovering that their products and services have security flaws or vulnerabilities, they shall immediately adopt remedial measures, and follow provisions to promptly inform users and report to the competent departments.

Providers of network products and services shall provide security maintenance for their products and services, and they must not terminate the provision of security maintenance during the time limits or period agreed on with clients.

If a network product or service has the function of collecting user information, its provider shall clearly indicate this and obtain consent from the user; and if this involves a user's personal information, the provider shall also comply with the provisions of this law and relevant laws and administrative regulations on the protection of personal information.

Article 23: Critical network equipment and specialized cybersecurity products shall follow national standards and mandatory requirements, and be security certified by a qualified establishment or meet the requirements of a security inspection, before being sold or provided. The state cybersecurity and

DID YOU KNOW?

Operation Night Dragon

Operation Night Dragon was a cyber-espionage campaign from 2007 through 2009, almost certainly conducted by elements of the People's Liberation Army of the People's Republic of China. It targeted oil and gas companies, and particularly sought to steal classified proprietary information regarding project financing and exploratory operations. The attackers gained access to corporate networks through spearphishing campaigns that tricked corporate executives and engineers into compromising their networks. Once the sensitive corporate information had been lifted, it was almost certainly shared with state-run Chinese companies, which could then launch competing bids for project development with the knowledge of how Western companies would compare. McAfee Corporation released a report demonstrating that the attacks were coordinated by an individual in the Shandong Province of China, and that the majority of the campaign was conducted during normal business hours in Beijing using tools of Chinese origin.

informatization departments, together with the relevant departments of the State Council, will formulate and release a catalog of critical network equipment and specialized cybersecurity products, and promote reciprocal recognition of security certifications and security inspection results to avoid duplicative certifications and inspections.

Article 24: Network operators handling network access and domain name registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with users or confirming the provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services.

The State implements a network identity credibility strategy and supports research and development of secure and convenient electronic identity authentication technologies, promoting reciprocal acceptance among different electronic identity authentication methods.

Article 25: Network operators shall formulate emergency response plans for cybersecurity incidents and promptly address system vulnerabilities, computer viruses, cyber attacks, network intrusions, and other such cybersecurity risks. When cybersecurity incidents occur, network operators should immediately initiate an emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions.

Article 26: Those carrying out cybersecurity certification, testing, risk assessment, or other such activities—or publicly publishing cybersecurity information such as system vulnerabilities, computer viruses, network attacks, or network incursions—shall comply with relevant national provisions.

Article 27: Individuals and organizations must not engage in illegal intrusion into the networks of other parties, disrupt the normal functioning of the networks of other parties, or steal network data or engage in other activities endangering cybersecurity; they must not provide programs, or tools specially used in network intrusions, that disrupt normal network functions and protection measures, steal network data, or engage in other acts endangering cybersecurity; and where they clearly are aware that others will engage in actions that endanger cybersecurity, they must not provide help such as technical support, advertisement and promotion, or payment of expenses.

Article 28: Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.

Article 29: The State supports cooperation between network operators in areas such as the gathering, analysis, reporting, and emergency handling of cybersecurity information, increasing the security safeguarding capacity of network operators.

Relevant industrial organizations are to establish and complete mechanisms for standardization and coordination of cybersecurity for their industry, strengthen their analysis and assessment of cybersecurity, and periodically conduct risk warnings, support, and coordination for members in responding to cybersecurity risks.

Article 30: Information obtained by cybersecurity and informatization departments and relevant departments performing cybersecurity protection duties can only be used as necessary for the protection of cybersecurity, and must not be used in other ways.

Section 2: Operations Security for Critical Information Infrastructure

Article 31: The State implements key protection on the basis of the cybersecurity multi-level protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest. The State Council will formulate the specific scope and security protection measures for critical information infrastructure.

The State encourages operators of networks outside the [designated] critical information infrastructure systems to voluntarily participate in the critical information infrastructure protection system.

Article 32: In accordance with the duties and division of labor provided by the State Council, departments responsible for security protection work for critical information infrastructure are to separately compile and organize security implementation plans for their industry's or sector's critical information infrastructure, and to guide and supervise security protection efforts for critical information infrastructure operations.

Article 33: Those constructing critical information infrastructure shall ensure that it has the capability to support business stability and sustained operations, and ensure the synchronous planning, synchronous establishment, and synchronous application of security technical measures.

Article 34: In addition to the provisions of Article 21 of this Law, critical information infrastructure operators shall also perform the following security protection duties:

(1) Set up specialized security management bodies and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions;
(2) Periodically conduct cybersecurity education, technical training, and skills evaluations for employees;
(3) Conduct disaster recovery backups of important systems and databases;

(4) Formulate emergency response plans for cybersecurity incidents, and periodically organize drills;
(5) Other duties provided by law or administrative regulations.

Article 35: Critical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council.

Article 36: Critical information infrastructure operators purchasing network products and services shall follow relevant provisions and sign a security and confidentiality agreement with the provider, clarifying duties and responsibilities for security and confidentiality.

Article 37: Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.

Article 38: At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks' security and risks that might exist, either on their own or through retaining a cybersecurity services organization; CII operators should submit a cybersecurity report on the circumstances of the inspection and assessment as well as improvement measures, to be sent to the relevant department responsible for critical information infrastructure security protection efforts.

Article 39: State cybersecurity and informatization departments shall coordinate relevant departments in employing the following measures for critical information infrastructure security protection:

(1) Conduct spot testing of critical information infrastructure security risks, put forward improvement measures, and when necessary they can retain a cybersecurity services organization to conduct testing and assessment of cybersecurity risks;
(2) Periodically organize critical information infrastructure operators to conduct emergency cybersecurity response drills, increasing the level, coordination, and capacity of responses to cybersecurity incidents.
(3) Promote cybersecurity information sharing among relevant departments, critical information infrastructure operators, and also relevant research institutions and cybersecurity services organizations.
(4) Provide technical support and assistance for cybersecurity emergency management and recovery, etc.

SOURCE: People's Republic of China, *Cybersecurity Law of the People's Republic of China*, trans. Rogier Creemers, Paul Triolo, and Graham Webster (Washington, D.C.: New America, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

ANALYSIS

A new interest in cybersecurity probably indicates that the People's Republic of China has been the target of a substantial increase in cyberattacks. Government attempts to control computer networks, software installations, and data transfer are an interesting aspect of these new regulations. In part, the government might be attempting to prevent individual Chinese hackers from launching attacks because such attacks provoke retaliation against targets that are under government control. If that is the primary driver behind the regulations, the Chinese government might be signaling its intent to follow behavioral norms in cyberspace, or it might be attempting to retain control of the types and targets of cyberattacks by reining in the cyber militia forces that are less likely to carry out successful campaigns of cyber espionage, and far more likely to be caught engaging in cyberattacks. It is also possible that these regulations are a face-saving international gesture, but that the Chinese government has no intention of enforcing its own regulations—essentially allowing it to deny any knowledge of cyberattacks originating from mainland China, while turning a blind eye to the behavior of its citizens.

- ***Document 31:*** *Grizzly Steppe—Russian Malicious Cyber Activity*
- ***When:*** December 29, 2016
- ***Where:*** Washington, D.C.
- ***Significance:*** Joint Analysis Reports allow multiple government agencies to contribute to a collective study of a key issue of national security. In the aftermath of the 2016 presidential election, the Department of Homeland Security and the Federal Bureau of Investigation commenced an analysis of Russian attempts to disrupt and influence the election cycle. They dubbed the effort by Russian intelligence services (RIS) "Grizzly Steppe."

DOCUMENT

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to RIS is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities. This determination expands upon the Joint Statement released October 7, 2016, from the Department of Homeland Security and the Director of National Intelligence on Election Security.

This activity by RIS is part of an ongoing campaign of cyber-enabled operations directed at the U.S. government and its citizens. These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information. In foreign countries, RIS actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack. This JAR provides technical indicators related to many of these operations, recommended mitigations, suggested actions to take in response to the indicators provided, and information on how to report such incidents to the U.S. Government.

Description

The U.S. Government confirms that two different RIS actors participated in the intrusion into a U.S. political party. The first actor group, known as Advanced Persistent Threat (APT) 29, entered into the party's systems in summer 2015, while the second, known as APT28, entered in spring 2016.

Both groups have historically targeted government organizations, think tanks, universities, and corporations around the world. APT29 has been observed crafting targeted spearphishing campaigns leveraging web links to a malicious dropper; once executed, the code delivers Remote Access Tools (RATs) and evades detection using a range of techniques. APT28 is known for leveraging domains that closely mimic those of targeted organizations and tricking potential victims into entering legitimate credentials. APT28 actors relied heavily on shortened URLs in their spearphishing email campaigns. Once APT28 and APT29 have access to victims, both groups exfiltrate and analyze information to gain intelligence value. These groups use this information to craft highly targeted spearphishing campaigns. These actors set up operational infrastructure to obfuscate their source infrastructure, host domains and malware for targeting organizations, establish command and control nodes, and harvest credentials and other valuable information from their targets.

In summer 2015, an APT29 spearphishing campaign directed emails containing a malicious link to over 1,000 recipients, including multiple U.S. Government victims. APT29 used legitimate domains, to include domains associated with U.S. organizations and educational institutions, to host malware and send spearphishing emails. In the course of that campaign, APT29 successfully compromised a U.S. political party. At least one targeted individual activated links to malware hosted on operational infrastructure of opened attachments containing malware. APT29 delivered malware to the political party's systems, established persistence, escalated privileges, enumerated active directory accounts, and exfiltrated email

from several accounts through encrypted connections back through operational infrastructure.

In spring 2016, APT28 compromised the same political party, again via targeted spearphishing. This time, the spearphishing email tricked recipients into changing their passwords through a fake webmail domain hosted on APT28 operational infrastructure. Using the harvested credentials, APT28 was able to gain access and steal content, likely leading to the exfiltration of information from multiple senior party members. The U.S. Government assesses that information was leaked to the press and publicly disclosed.

Actors likely associated with RIS are continuing to engage in spearphishing campaigns, including one launched as recently as November 2016, just days after the U.S. election.

SOURCE: National Cybersecurity & Communications Integration Center, "Grizzly Steppe—Russian Malicious Cyber Activity," Joint Analysis Report 16-20296A, December 29, 2016, 1–3, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

ANALYSIS

Russian intelligence agencies are among the most skilled cyberattackers in the world. When they turned their efforts to disrupting the presidential election cycle, and in particular to damaging the Hillary Clinton campaign, it was all but guaranteed that they would have a significant effect. In particular, Russian hackers are extremely adept at social engineering and spearphishing efforts, which include specific targeting of individuals for attempts to compromise credentials and gain access to computer networks. Several members of Clinton's campaign team were targeted for such attempts, and at least one, John Podesta, fell victim to a spearphishing attack. As a result, his personal emails, including a substantial trove of communications about the presidential campaign, were stolen and subsequently published by WikiLeaks. The release of his email communications in the weeks before the election had a deleterious effect upon the campaign, as many of his private communications were considered embarrassing or controversial.

- ***Document 32:*** *Assessing Russian Activities and Intentions in Recent U.S. Elections*
- ***When:*** January 6, 2017
- ***Where:*** Washington, D.C.
- ***Significance:*** In the 2016 presidential campaign, a shocking amount of false information and external propaganda permeated the election landscape. When Donald Trump unexpectedly won the

election over Hillary Clinton, there were many public accusations that the Trump campaign had received substantial assistance from foreign governments through the cyber domain, particularly Russia. On the campaign trail, Trump seemed to openly call for Russian hackers to target his opponent, and on a number of occasions, cyberattacks against the Democratic Party and its leadership led to the release of damaging information stolen from poorly secured computer networks. In the two months between the election and Trump's inauguration, the FBI conducted an investigation of Russian activities, seeking to determine if Russian hackers had somehow altered the outcome of the election.

DOCUMENT

Russia's Influence Campaign Targeting the 2016 US Presidential Election
Putin Ordered Campaign to Influence US Election

We assess with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election, the consistent goals of which were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign then focused on undermining her expected presidency.

- We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.
- In trying to influence the US election, we assess the Kremlin sought to advance its longstanding desire to undermine the US-led liberal democratic order, the promotion of which Putin and other senior Russian leaders view as a threat to Russia and Putin's regime.
- Putin publicly pointed to the Panama Papers disclosure and the Olympic doping scandal as US-directed efforts to defame Russia, suggesting he sought to use disclosures to discredit the image of the United States and cast it as hypocritical.
- Putin most likely wanted to discredit Secretary Clinton because he has publicly blamed her since 2011 for inciting mass protests against his regime in late 2011 and early 2012, and because he holds a grudge for comments he almost certainly saw as disparaging him. We assess Putin, his advisers, and

the Russian Government developed a clear preference for President-elect Trump over Secretary Clinton.

- Beginning in June, Putin's public comments about the US presidential race avoided directly praising President-elect Trump, probably because Kremlin officials thought that any praise from Putin personally would backfire in the United States. Nonetheless, Putin publicly indicated a preference for President-elect Trump's stated policy to work with Russia, and pro-Kremlin figures spoke highly about what they saw as his Russia-friendly positions on Syria and Ukraine. Putin publicly contrasted the President-elect's approach to Russia with Secretary Clinton's "aggressive rhetoric."
- Moscow also saw the election of President-elect Trump as a way to achieve an international counterterrorism coalition against the Islamic State in Iraq and the Levant (ISIL).
- Putin has had many positive experiences working with Western political leaders whose business interests made them more disposed to deal with Russia, such as former Italian Prime Minister Silvio Berlusconi and former German Chancellor Gerhard Schroeder.
- Putin, Russian officials, and other pro-Kremlin pundits stopped publicly criticizing the US election process as unfair almost immediately after the election because Moscow probably assessed it would be counterproductive to building positive relations.

DID YOU KNOW?

Russian Cyberwar against Estonia

In 2007, Russian cyber activists became incensed at an Estonian plan to remove a World War II monument to Soviet soldiers located in the capital, Tallinn. When the plan was announced, riots erupted, and were accompanied by a massive wave of cyberattacks against Estonian government and banking sites that effectively shut down Estonian internet activity for three weeks. In addition to blaming Russia for the attacks, Estonia attempted to invoke Article V of the North Atlantic Treaty, essentially arguing that the cyber activity amounted to an act of war requiring the involvement of NATO. Although NATO allies refused to formally join the conflict, they did subsequently establish a NATO Cyber Center in Tallinn. Russia vehemently denied responsibility for the attacks, and when they were definitively proven to originate from Russian territory, blamed the attacks upon fervent, if misguided, patriots. In any event, Estonia, one of the most internet-dependent nations on earth, proved extremely vulnerable to the attacks, which caused enormous economic harm despite having relatively unsophisticated methods.

We assess the influence campaign aspired to help President-elect Trump's chances of victory when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to the President-elect. When it appeared to Moscow that Secretary Clinton was likely to win the presidency the Russian influence campaign focused more on undercutting Secretary Clinton's legitimacy and crippling her presidency from its start, including by impugning the fairness of the election.

- Before the election, Russian diplomats had publicly denounced the US electoral process and were prepared to publicly call into question the validity of the results. Pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory, judging from their social media activity.

Russian Campaign Was Multifaceted

Moscow's use of disclosures during the US election was unprecedented, but its influence campaign otherwise followed a longstanding Russian messaging strategy

that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls."

- We assess that influence campaigns are approved at the highest levels of the Russian Government—particularly those that would be politically sensitive.
- Moscow's campaign aimed at the US election reflected years of investment in its capabilities, which Moscow has honed in the former Soviet states.
- By their nature, Russian influence campaigns are multifaceted and designed to be deniable because they use a mix of agents of influence, cutouts, front organizations, and false-flag operations. Moscow demonstrated this during the Ukraine crisis in 2014, when Russia deployed forces and advisers to eastern Ukraine and denied it publicly.

The Kremlin's campaign aimed at the US election featured disclosures of data obtained through Russian cyber operations; intrusions into US state and local electoral boards; and overt propaganda. Russian intelligence collection both informed and enabled the influence campaign.

Cyber Espionage Against US Political Organizations. Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties.

We assess Russian intelligence services collected against the US primary campaigns, think tanks, and lobbying groups they viewed as likely to shape future US policies. In July 2015, Russian intelligence gained access to Democratic National Committee (DNC) networks and maintained that access until at least June 2016.

- The General Staff Main Intelligence Directorate (GRU) probably began cyber operations aimed at the US election by March 2016. We assess that the GRU operations resulted in the compromise of the personal e-mail accounts of Democratic Party officials and political figures. By May, the GRU had exfiltrated large volumes of data from the DNC.

Public Disclosures of Russian-Collected Data. We assess with high confidence that the GRU used the Guccifer 2.0 persona, DCLeaks.com, and WikiLeaks to release US victim data obtained in cyber operations publicly and in exclusives to media outlets.

- Guccifer 2.0, who claimed to be an independent Romanian hacker, made multiple contradictory statements and false claims about his likely Russian identity throughout the election. Press reporting suggests more than one person claiming to be Guccifer 2.0 interacted with journalists.
- Content that we assess was taken from e-mail accounts targeted by the GRU in March 2016 appeared on DCLeaks.com starting in June.

We assess with high confidence that the GRU relayed material it acquired from the DNC and senior Democratic officials to WikiLeaks. Moscow most likely chose

WikiLeaks because of its self-proclaimed reputation for authenticity. Disclosures through WikiLeaks did not contain any evident forgeries.

- In early September, Putin said publicly it was important the DNC data was exposed to WikiLeaks, calling the search for the source of the leaks a distraction and denying Russian "state-level" involvement.
- The Kremlin's principal international propaganda outlet RT (formerly Russia Today) has actively collaborated with WikiLeaks. RT's editor-in-chief visited WikiLeaks founder Julian Assange at the Ecuadorian Embassy in London in August 2013, where they discussed renewing his broadcast contract with RT, according to Russian and Western media. Russian media subsequently announced that RT had become "the only Russian media company" to partner with WikiLeaks and had received access to "new leaks of secret information." RT routinely gives Assange sympathetic coverage and provides him a platform to denounce the United States. These election-related disclosures reflect a pattern of Russian intelligence using hacked information in targeted influence efforts against targets such as Olympic athletes and other foreign governments. Such efforts have included releasing or altering personal data, defacing websites, or releasing emails.
- A prominent target since the 2016 Summer Olympics has been the World Anti-Doping Agency (WADA), with leaks that we assess to have originated with the GRU and that have involved data on US athletes.

Russia collected on some Republican-affiliated targets but did not conduct a comparable disclosure campaign.

Russian Cyber Intrusions Into State and Local Electoral Boards. Russian intelligence accessed elements of multiple state or local electoral boards. Since early 2014, Russian intelligence has researched US electoral processes and related technology and equipment.

- DHS assesses that the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying.

Russian Propaganda Efforts. Russia's state-run propaganda machine—comprised of its domestic media apparatus, outlets targeting global audiences such as RT and Sputnik, and a network of quasi-government trolls—contributed to the influence campaign by serving as a platform for Kremlin messaging to Russian and international audiences. State-owned Russian media made increasingly favorable comments about President-elect Trump as the 2016 US general and primary election campaigns progressed while consistently offering negative coverage of Secretary Clinton.

- Starting in March 2016, Russian Government-linked actors began openly supporting President-elect Trump's candidacy in media aimed at English-speaking audiences. RT and Sputnik—another government-funded outlet producing pro-Kremlin radio and online content in a variety of languages

for international audiences—consistently cast President-elect Trump as the target of unfair coverage from traditional US media outlets that they claimed were subservient to a corrupt political establishment.
- Russian media hailed President-elect Trump's victory as a vindication of Putin's advocacy of global populist movements—the theme of Putin's annual conference for Western academics in October 2016—and the latest example of Western liberalism's collapse.
- Putin's chief propagandist Dmitriy Kiselev used his flagship weekly newsmagazine program this fall to cast President-elect Trump as an outsider victimized by a corrupt political establishment and faulty democratic election process that aimed to prevent his election because of his desire to work with Moscow.
- Pro-Kremlin proxy Vladimir Zhirinovskiy, leader of the nationalist Liberal Democratic Party of Russia, proclaimed just before the election that if President-elect Trump won, Russia would "drink champagne" in anticipation of being able to advance its positions on Syria and Ukraine.

RT's coverage of Secretary Clinton throughout the US presidential campaign was consistently negative and focused on her leaked e-mails and accused her of corruption, poor physical and mental health, and ties to Islamic extremism. Some Russian officials echoed Russian lines for the influence campaign that Secretary Clinton's election could lead to a war between the United States and Russia.

- In August, Kremlin-linked political analysts suggested avenging negative Western reports on Putin by airing segments devoted to Secretary Clinton's alleged health problems.
- On 6 August, RT published an English-language video called "Julian Assange Special: Do WikiLeaks Have the E-mail That'll Put Clinton in Prison?" and an exclusive interview with Assange entitled "Clinton and ISIS Funded by the Same Money." RT's most popular video on Secretary Clinton, "How 100% of the Clintons' 'Charity' Went to . . . Themselves," had more than 9 million views on social media platforms. RT's most popular English language video about the President-elect, called "Trump Will Not Be Permitted To Win," featured Assange and had 2.2 million views.
- For more on Russia's past media efforts—including portraying the 2012 US electoral process as undemocratic—please see Annex A: Russia—Kremlin's TV Seeks To Influence Politics, Fuel Discontent in US.

Russia used trolls as well as RT as part of its influence efforts to denigrate Secretary Clinton. This effort amplified stories on scandals about Secretary Clinton and the role of WikiLeaks in the election campaign.

- The likely financier of the so-called Internet Research Agency of professional trolls located in Saint Petersburg is a close Putin ally with ties to Russian intelligence.
- A journalist who is a leading expert on the Internet Research Agency claimed that some social media accounts that appear to be tied to Russia's professional trolls—because they previously were devoted to supporting Russian

actions in Ukraine—started to advocate for President-elect Trump as early as December 2015.

Influence Effort Was Boldest Yet in the US

Russia's effort to influence the 2016 US presidential election represented a significant escalation in directness, level of activity, and scope of effort compared to previous operations aimed at US elections. We assess the 2016 influence campaign reflected the Kremlin's recognition of the worldwide effects that mass disclosures of US Government and other private data—such as those conducted by WikiLeaks and others—have achieved in recent years, and their understanding of the value of orchestrating such disclosures to maximize the impact of compromising information.

- During the Cold War, the Soviet Union used intelligence officers, influence agents, forgeries, and press placements to disparage candidates perceived as hostile to the Kremlin, according to a former KGB archivist.

Since the Cold War, Russian intelligence efforts related to US elections have primarily focused on foreign intelligence collection. For decades, Russian and Soviet intelligence services have sought to collect insider information from US political parties that could help Russian leaders understand a new US administration's plans and priorities.

- The Russian Foreign Intelligence Service (SVR) Directorate S (Illegals) officers arrested in the United States in 2010 reported to Moscow about the 2008 election.
- In the 1970s, the KGB recruited a Democratic Party activist who reported information about then-presidential hopeful Jimmy Carter's campaign and foreign policy plans, according to a former KGB archivist.

Election Operation Signals "New Normal" in Russian Influence Efforts

We assess Moscow will apply lessons learned from its campaign aimed at the US presidential election to future influence efforts in the United States and worldwide, including against US allies and their election processes. We assess the Russian intelligence services would have seen their election influence campaign as at least a qualified success because of their perceived ability to impact public discussion.

- Putin's public views of the disclosures suggest the Kremlin and the intelligence services will continue to consider using cyber-enabled disclosure operations because of their belief that these can accomplish Russian goals relatively easily without significant damage to Russian interests.
- Russia has sought to influence elections across Europe.

We assess Russian intelligence services will continue to develop capabilities to provide Putin with options to use against the United States, judging from past practice and current efforts. Immediately after Election Day, we assess Russian intelligence began a spearphishing campaign targeting US Government employees and individuals associated with US think tanks and NGOs in national security, defense, and foreign policy fields. This campaign could provide material for future influence efforts as well as foreign intelligence collection on the incoming administration's goals and plans.

SOURCE: Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* (Washington, D.C.: Office of the Director of National Intelligence, 2017), 1–5, https://www.dni.gov/files/documents/ICA_2017_01.pdf

ANALYSIS

For the Director of National Intelligence to release a report to the public that points out the influence of a foreign state in a presidential election two weeks before the inauguration of a new president, the evidence of meddling had to be overwhelming. While the report makes no claims that the Trump campaign engaged in any form of collusion with the Russian government, it does provide ample proof that the Russian government, in general, and President Vladimir Putin, in particular, placed enormous effort into disrupting the U.S. election cycle. Such behavior is not outside the norm for Russia (or for other states, including the United States), but the level of involvement was unprecedented. Also, it is perhaps most important to note that the authors of the report consider future interference to be all but certain, particularly given the level of success in 2016. Further investigations demonstrated that Russian hackers attempted to influence state and local elections in 2018, and planned to increase their efforts heading into the 2020 election cycle. It is impossible to determine whether they will seek to support President Trump's reelection campaign or will place a greater emphasis upon creating as much chaos as possible, but it is a virtual certainty that they will renew their efforts to influence the U.S. electorate.

- ***Document 33:*** *Russia Military Power*
- ***When:*** 2017
- ***Where:*** Bethesda, MD
- ***Significance:*** The U.S. DOD periodically analyzes the military capabilities, intentions, and technological developments of peer contenders and potential adversaries. In recent iterations, the cyber capabilities of those nations have become an increasingly important portion of the reports.

DOCUMENT

Cyber

Russia views the information sphere as a key domain for modern military conflict. Moscow perceives the information domain as strategically decisive and critically important to control its domestic populace and influence adversary states.

Information warfare is a key means of achieving its ambitions of becoming a dominant player on the world stage.

Since at least 2010, the Russian military has prioritized the development of forces and means for what it terms "information confrontation," which is a holistic concept for ensuring information superiority, during peacetime and wartime. This concept includes control of the information content as well as the technical means for disseminating that content. Cyber operations are part of Russia's attempts to control the information environment.

The weaponization of information is a key aspect of Russia's strategy and is employed in time of peace, crisis, and war. In practice, information battles draw upon psychological warfare tactics and techniques from the Soviet Era for influencing Western societies. Moscow views information and psychological warfare as a measure to neutralize adversary actions in peace to prevent escalation to crisis or war.

Chief of the General Staff Gerasimov announced that "information operations troops" were involved for the first time in the Kavkaz-2016 strategic command staff exercise in September 2016, demonstrating Russian military commitment to controlling the information domain.

DID YOU KNOW?

Russian Cyberattacks against Georgia (2008)

In 2008, Russia and Georgia became engaged in a territorial dispute over South Ossetia, a province of Georgia with a majority of ethnic Russian citizens. After a short physical clash, the Russian edge in numbers and military technology drove the Georgian military from the area, effectively ceding control of the region to Russia. The Russian incursion and occupation was accompanied by a wave of debilitating cyberattacks reminiscent of the Estonian cyber war of 2007. The cyber activities consisted primarily of distributed denial of service (DDoS) attacks against Georgian government and economic websites, as well as an effort to disrupt Georgian military communications. Although Georgian cyber forces attempted to counter the attacks, they were overwhelmed by the sheer scope and relentless nature of the cyber assault. The attacks effectively halted all digital monetary transactions, cellular telephone functionality, and government communications, including the ability of the Georgian government to request international support. Although cyberattacks did not prove to be the decisive factor in the conflict, they certainly provided a useful means of disrupting Georgian military responses, and as such, will likely be repeated in future Russian conflicts.

Propaganda Helps Shape the Information Environment

Russian propaganda strives to influence, confuse, and demoralize its intended audience, often containing a mixture of true and false information to seem plausible and fit into the preexisting worldview of the intended audience. Russian propaganda targets a wide variety of audiences, including its own population, selected populations of other countries, domestic and foreign political elites, and the West writ large. The variety of techniques for disseminating Russian propaganda include pro-Kremlin "news" websites and TV and radio channels such as Russia Today and Sputnik News, bots and trolls on social media, search engine optimization, and paid journalists in Western and other foreign media.

Cyber-Enabled Psychological Operations

One of the newest tools in Russia's information toolkit is the use of cyber-enabled psychological operations that support its strategic and tactical information warfare objectives. These new techniques involve compromising networks for intelligence information that could be used to embarrass, discredit, or falsify information. Compromised material can then be leaked to the media at inopportune times.

- **Hacktivists**. Russian intelligence services have been known to co-opt or masquerade as other hacktivist groups. These groups appeal to Russia due to the difficulty of attribution and the level of anonymity provided. It is widely

accepted that Russia, via patriotic hackers, conducted a cyber attack on Estonia in 2007. Under the guise of hacktivism, a group called "CyberCaliphate," seemingly ISIS associated, conducted a hack against French station TV5 Monde in January 2015. The CyberCaliphate group was later linked to Russian military hackers. The same group hijacked the Twitter feed of the U.S. Central Command.

- **CyberBerkut.** A False Persona. Russian hackers also use false personas. CyberBerkut is a front organization for Russian state-sponsored cyber activity, supporting Russia's military operations and strategic objectives in Ukraine. CyberBerkut employs a range of both technical and propaganda attacks, consistent with the Russian concept of "information confrontation." Since emerging in March 2014, CyberBerkut has been implicated in multiple incidents of cyber espionage and attack, including distributed denial of service attacks against NATO, Ukraine, and German government websites. More recently, it has focused on the online publication of hacked documents, ostensibly obtained from the Ukrainian government and political figures' computers. CyberBerkut uses information gained through these hacks to discredit the Ukrainian government. The intent is to demoralize, embarrass, and create distrust of elected officials.
- **Trolls.** Russia employs a troll army of paid online commentators who manipulate or try to change the narrative of a given story in Russia's favor. Russia's Troll Army, also known as the Internet Research Agency, is a state-funded organization that blogs and tweets on behalf of the Kremlin. Trolls typically post pro-Kremlin content and facilitate heated discussions in the comments sections of news articles. Their goal is to counter negative media and "Western influence." While the goal of some trolls is to simply disrupt negative content, other trolls promote completely false content.
- **Bots.** Another way Russia manipulates the information space is through the use of bots. Bots are automated pushers of content on social media. These bots vary in sophistication and can continuously push content or imitate real life patterns. Bots can drown out unwanted content or push a specific message. Bots have the ability to overwhelm the information space and discourage readers from looking for real content.

Information Defense

The Russian Federation Security Council's 2016 Information Security Doctrine mandates protecting Russian citizens from outside threats to the information sphere. The doctrine aims to secure Russian information freedom and protect information technologies from foreign influence, cyberattacks, intelligence collection, and terrorism. The doctrine emphasizes the need to develop a national system for government control of the Russian internet, information warfare forces, and cyber weapons.

Since at least 1999, Russia has attempted to gain consensus on international governance of the internet and international norms and rules guiding the behavior

of states in the information space. A major component of the proposal pertains to a state's ability to govern its information space as a means of maintaining state sovereignty and preventing an arms race in cyberspace. Although state sovereignty traditionally refers to domestic enforcement law, Russia commonly uses this term to denounce other nations meddling in their internal affairs. Russia also proposed a code of conduct for cyberspace with specific dictums regarding non-state cyber-actors, such as criminal hackers involved in cyber activities.

Media Laws—A Hedge Against Instability

In the past decade, Russia has implemented numerous laws curbing domestic media in broadcast, print, and cyber media, taking an abrupt turn from the post-Soviet glasnost policies of media "openness" and its own constitutional guarantees of freedom of speech. The use of social media to organize opposition street protests in 2011 and 2012 prompted a reappraisal of official internet policy. Since then, the authorities have treated the internet as a serious threat, pushing through laws increasing government controls over technology and content giving the state powers to block content, ban websites, monitor online activity, and limit media ownership. The ultimate goal of this policy appears to be to create what some have called a "sovereign internet."

The Kremlin's strategy of reducing foreign influence on the media has not been confined to the internet. Numerous other pieces of legislation have been passed restricting the level of foreign ownership of the media, impeding the work of the foreign NGOs supporting independent media in Russia and forcing Russian media to account for any foreign funding they receive. A recent law has even banned foreign companies from conducting TV audience research in Russia.

SOURCE: U.S. Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations* (Bethesda, MD: Government Printing Office, 2017), 37–41, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf?ver=2017-06-28-144235-937

ANALYSIS

While the People's Republic of China tends to maintain a tight control over its cyber forces, the Russian approach is much looser, allowing its hackers to determine their own activities. Russian attacks tend to focus upon brute-force tactics, such as distributed denial of service (DDoS) attacks, rather than long-term cyber espionage. However, Russian cyberattacks are also more often linked to cybercrime organizations, with or without the sanction and protection of the Russian government. Russian cyberattacks are more likely to be coordinated efforts to shape the information aspect of the cyber domain, meaning Russian cyber operators are far more likely to engage in propaganda campaigns, influence peddling, and efforts to disrupt democratic processes.

- ***Document 34:*** *Military and Security Developments Involving the Democratic People's Republic of Korea*
- ***When:*** December 2017
- ***Where:*** Washington, D.C.
- ***Significance:*** The U.S. DOD periodically analyzes the military capabilities, intentions, and technological developments of peer contenders and potential adversaries. In recent iterations, the cyber capabilities of those nations have become an increasingly important portion of the reports.

DOCUMENT

The Capabilities and Modernization Goals of North Korea's Military Forces

Cyberwarfare Capabilities. North Korea possesses increasingly sophisticated cyber warfare capabilities, including offensive capabilities, which are capable of damaging and disruptive cyberattacks. North Korean cyber effects operations have been implicated in malicious cyber activity since 2009 and challenge widely recognized norms of state behavior in cyberspace. North Korea has invested in developing its cyber capabilities and probably views cyber operations as an appealing, cost-effective, and deniable means by which to collect intelligence and cause disruption against its highly networked adversaries, notably the ROK [Republic of Korea], Japan, and the United States. North Korea likely believes it can conduct cyber effects operations with little risk of reprisal, in part because its networks are largely separated from the internet and disruption of internet access would have minimal impact on its economy. In November 2014, North Korean cyber actors using the nom de guerre "Guardians of Peace" attacked Sony Pictures Entertainment, shutting down employee access and deleting data. For these types of attacks, North Korea likely uses internet infrastructure from third-party nations.

Pyongyang probably is increasingly using cybercrime to offset financial losses resulting from international sanctions, especially given stricter Chinese enforcement of these sanctions. For example, North Korea probably was involved in the theft of $81 million from the Central Bank of Bangladesh in February 2016. North Korean cyber actors also are using malware to blackmail individuals and companies into paying large fees to keep sensitive information (such as personally identifiable information) from being publicly released. In 2017, North Korea carried out the malicious "WannaCry" ransomware attack that spread across the world damaging civilian infrastructure, including the United Kingdom's National Health Service and Chinese firms. North Korea exploited an existing vulnerability that allowed it to encrypt a target's hard drive, then demanded payment in cryptocurrency within a set time period or else the users' data would be wiped. Even individuals and firms which paid the ransom did not recover their data.

Intelligence Services. North Korean intelligence and security services collect political, military, economic, and technical information through open sources, human intelligence, cyber intrusions, and signals intelligence capabilities. North Korea's primary intelligence collection targets remain the ROK, the United States, and Japan. They likely operate anywhere North Korea has a diplomatic or sizable economic overseas presence.

The **Reconnaissance General Bureau** (RGB) is North Korea's primary foreign intelligence service, responsible for collection and clandestine operations. The RGB comprises six bureaus with compartmented functions, including operations, reconnaissance, technology and cyber capabilities, overseas intelligence, inter-Korean talks, and service support.

The **Ministry of State Security** (MSS) is North Korea's primary counterintelligence service and is an autonomous agency of the North Korean Government reporting directly to Kim Jong Un. The MSS is responsible for operating North Korean prison camps, investigating cases of domestic espionage, repatriating defectors, and conducting overseas counterespionage activities in North Korea's foreign missions.

The **United Front Department** (UFD) overtly attempts to establish pro–North Korean groups in the ROK, such as the Korean AsiaPacific Committee and the Ethnic Reconciliation Council. The UFD is also the primary department involved in managing inter-Korean dialogue and North Korea's policy toward the ROK.

The **225th Bureau** is responsible for training agents to infiltrate the ROK and establish underground political parties focused on fomenting unrest and revolution.

DID YOU KNOW?

Sony Hack of 2014

In November 2014, hackers from the People's Democratic Republic of Korea (DPRK) launched an attack against the Sony Pictures Entertainment computer networks. They were likely provoked, at least in part, by the impending release of *The Interview*, a satirical film that included an assassination attempt upon the DPRK's leader, Kim Jong Un. The attack demonstrated the extreme vulnerability of Sony and other entertainment corporations as the company had done very little to secure its internal network. The attackers managed to compromise almost the entire internal network and steal enormous amounts of data such as digital copies of unreleased films including *The Interview*. Showing surprising patience, the attackers slowly downloaded the stolen, unencrypted data from the Sony networks, hiding it in legitimate data traffic.

Sony did not become aware of the attack until a previously unknown group, the Guardians of Peace, deliberately revealed itself by playing a short video taunting Sony on the company's networked computers. The video was followed by a malware attack that effectively erased the data on half of Sony's computers and servers, and caused the network to crash in dramatic fashion. Sony was forced to conduct business through archaic methods while building an entirely new computer network with much stronger protocols at a cost of more than $40 million. Less than a week after the attack, the Guardians of Peace began leaking the stolen data, including internal emails from Sony executives and unreleased entertainment projects.

Command, Control, and Communications. North Korea exercises control of the KPA through overlapping state, military, and party organizations. North Korea's State Affairs Commission is the official state authority over the North's military and security services. The Ministry of People's Armed Forces is the KPA's administrative superior, and the General Staff Department exercises operational command and control.

North Korea has a nationwide fiber-optic network and has invested in a modern nationwide cellular network. However, telecommunication services and access are strictly controlled, and all networks are available for military use.

SOURCE: Office of the Secretary of Defense, *Military and Security Developments Involving the Democratic People's Republic of Korea* (Washington, D.C.: Government Printing Office, 2017), 13–15, https://media.defense.gov/2018/May/22/2001920587/-1/-1/1/REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-DEMOCRATIC-PEOPLES-REPUBLIC-OF-KOREA-2017.PDF

ANALYSIS

One of the most intriguing aspects of North Korea's approach to cyber warfare is how asymmetrical the nation's capabilities are within cyberspace, relative to its minimal vulnerabilities. There are a very small number of internet-authorized citizens in North Korea, and the government keeps a very tight control over the websites that they are allowed to utilize. There is very little internet-dependent commerce in North Korea, and if the nation lost its entire connection to the internet, it would have very little effect upon the economy or society as a whole. In addition to this almost invulnerable position relative to external attack, the North Korean government has been under heavy sanctions for decades, which means that it has learned to adapt to its diminished circumstances. Short of a full-scale military invasion, which is no doubt deterred by North Korea's development of nuclear weapons, there is very little that North Korea's enemies can do to the Hermit Kingdom. As a result, the North Korean military feels a certain impunity in launching cyberattacks, knowing that cyber retaliation will likely have no significant effect. Recent North Korean cyberattacks have demonstrated a complete disregard for the norms of state behavior in cyberspace, even toward antagonists. North Korea is one of the few state actors in cyberspace that engages in the most basic of criminal activity, including ransomware attacks and other forms of cyber extortion, largely for the purpose of obtaining currency that can be utilized in illicit trading relationships.

- ***Document 35:*** *China Military Power*
- ***When:*** 2019
- ***Where:*** Bethesda, MD
- ***Significance:*** The U.S. DOD periodically analyzes the military capabilities, intentions, and technological developments of peer contenders and potential adversaries. In recent iterations, the cyber capabilities of those nations have become an increasingly important portion of the reports.

DOCUMENT

Cyberspace

Authoritative PLA writings identify controlling the "information domain"—sometimes referred to as "information dominance"—as a prerequisite for achieving victory in a modern war and as essential for countering outside intervention in a conflict. The PLA's broader concept of the information domain and of information operations encompasses the network, electromagnetic, psychological, and intelligence

domains, with the "network domain" and corresponding "network warfare" roughly analogous to the current U.S. concept of the cyber domain and cyberwarfare.

The PLA Strategic Support Force (SSF) may be the first step in the development of a cyberforce by combining cyber reconnaissance, cyberattack, and cyberdefense capabilities into one organization to reduce bureaucratic hurdles and centralize command and control of PLA cyber units. Official pronouncements offer limited details on the organization's makeup or mission. President Xi simply said during the SSF founding ceremony on 31 December 2015 that the SSF is a "new-type combat force to maintain national security and [is] an important growth point for the PLA's combat capabilities." The SSF probably was formed to consolidate cyber elements of the former PLA General Staff Third (Technical Reconnaissance) and Fourth (Electronic Countermeasures and Radar) Departments and Informatization Department.

. . .

Appendix E: PLA Strategic Support Force

In December 2015, Beijing established the Strategic Support Force (SSF) to provide the PLA with cyber, aerospace, and electronic warfare capabilities. The SSF forms the core of China's information warfare force, supports the entire PLA, and reports directly to the CMC. The force's formation appears to be the outcome of debate in the PLA since the 1980s regarding PLA needs in a potential conflict with peer nations. According to a Ministry of National Defense spokesman, "The SSF will integrate reconnaissance, early warning, communications, command, control, [and] navigation . . . and will provide strong support for joint operations for each military service branch."

A key aspect of the SSF is that the new body unites previously dispersed elements, providing more centralized command and control of China's cyber, space, and electronic warfare capabilities. Before the 2015 structural reforms, for example, responsibility for space, cyber, and electronic warfare missions rested with offices across the former General Armaments Department and the General Staff Department (GSD), including the GSD Technical Department and GSD Electronic Countermeasures and Radar Department.

The SSF constitutes the first steps in the development of a cyberforce by combining cyber reconnaissance, cyberattack, and cyberdefense capabilities into one organization to reduce bureaucratic hurdles and centralize command and control. The SSF also appears to be in line with PLA efforts to support and execute modern informatized warfare.

The PLA's 90th anniversary parade in July 2017 included the participation of an SSF electronic reconnaissance formation, which reportedly provides highly mobile, integrated, flexible, multidomain information warfare capabilities. The unit's mission reportedly is seizing and maintaining battlefield information control. This focus on the SSF and one of its premier units suggests that the PLA is increasing the priority and prominence of the SSF and its assigned missions to tackle the military's deficiencies in controlling complex electromagnetic environments.

SOURCE: U.S. Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (Bethesda, MD: Government Printing Office, 2019), 45, 97, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf

ANALYSIS

The People's Republic of China has been the most aggressive nation-state to launch cyberattacks against the United States since the development of the internet. In part, this seems to be driven by efforts to attain comparable levels of military technology. On the other hand, it seems to be in support of economic competition as the Chinese government maintains extremely close ties with a number of major development corporations that engage in international competition. While the People's Liberation Army has not created a separate service dedicated to cyber operations to date, this report seems to suggest that the Strategic Support Force may grow into such an independent service in the relatively near future. The Chinese approach to cyberattacks has been to maintain tight control over state-level campaigns, such that the cyber intrusions are conducted as military operations, with very careful oversight from the nation's political leadership. This is in marked contrast to the approach preferred by Russia, the other major peer competitor in the cyber domain.

3

U.S. POLICIES, DOCTRINE, AND REPORTS

- ***Document 36:*** *Presidential Decision Directive/NSC-63*
- ***When:*** May 22, 1998
- ***Where:*** Washington, D.C.
- ***Significance:*** In 1998, the internet was still a relatively new and unexplored technological development. Although e-commerce was becoming more common, it was not a particularly large portion of the national economy. However, technological pioneers clearly understood that the nation's computer networks would grow at an exponential rate and that as more and more critical systems were networked, new vulnerabilities might arise. President William Clinton attempted to plan for the protection of the nation's critical infrastructure by providing guidance and deadlines to federal agencies regarding an enhanced defensive posture.

DOCUMENT

A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today the United States shall have achieved and shall maintain the ability to protect the nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services.
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, we should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector or counterpart (Sector Coordinator) to represent their sector.

DID YOU KNOW?

MS Blaster Worm

In 2003, one of the most devastating computer worms in the history of cyberattacks first appeared. Approximately one hundred thousand computers were infected with MS Blaster in a very short period of time, including a substantial number of U.S. government systems. The worm infected computers through a security flaw in Microsoft's Distributed Component Object Model (DCOM) program. Infected computers developed a variety of problems and typically became inoperable. Although Microsoft quickly released software patches to prevent further infections, the short-lived worm caused millions of dollars in damages and created significant chaos throughout the internet. The creator of MS Blaster remains a mystery, as does the purpose behind its creation and release. The MS Blaster experience demonstrated why network operators needed to place greater emphasis upon internal security—too many users assumed that the external network defenses provided all of the necessary protections, and found to their dismay that once a single node of a network is penetrated, the entire system is at risk of further damages.

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;
- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies.

. . .

Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorities to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorities.

No later than 180 days from the issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical infrastructure Coordination Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect critical infrastructure.

SOURCE: William J. Clinton, *Presidential Decision Directive/NSC-63* (Washington, D.C., May 22, 1998), https://fas.org/irp/offdocs/pdd/pdd-63.htm

ANALYSIS

This directive was part of a much broader effort to improve the protection of critical elements of U.S. society, as well as the networks tied directly to the functions of the federal government. By setting specific deadlines and benchmarks for

compliance, this directive forced federal agencies to give serious consideration to their own vulnerabilities and to engage in policy planning for their own defenses. However, the speed of cyber development far outstripped the federal government's ability to plan for adequate defenses, and the shift to an active war footing in the aftermath of the September 11 attacks derailed the long-term efforts to improve cybersecurity for the nation's critical infrastructure—meaning that future presidents would confront even greater security dilemmas regarding the same installations and potential targets for hostile cyber activities.

- ***Document 37:*** *Cyber Threat Source Descriptions*
- ***When:*** May 2005
- ***Where:*** Washington, D.C.
- ***Significance:*** In 2005, the Government Accountability Office (GAO) prepared a list of cyber threat sources for members of Congress and the general public to better understand the specific nature of security risks in the cyber domain. The list provided a broad understanding of how each type of potential attacker might create inherent instability within computer networks, and it supplied a quick summary of the inherent challenges associated with countering each.

DOCUMENT

Cyber Threat Source Descriptions

Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. To protect against these threats, it is necessary to create a secure cyber-barrier around the Industrial Control System (ICS). Though other threats exist, including natural disasters, environmental, mechanical failure, and inadvertent actions of an authorized user, this discussion will focus on the deliberate threats mentioned above.

National Governments

National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm US interests. These threats range from

DID YOU KNOW?

Classified Information

In the United States, classified information is placed into one of three levels, which helps to illustrate its importance to national security and the level of damage expected if the classified information is released (known as a "breach"). The highest level, "Top Secret," applies to information that could reasonably be expected to cause exceptionally grave damage to national security if it was released into the public. "Secret" information refers to classified material that, if released, could reasonably be expected to cause serious damage to national security. "Confidential" information, if disclosed, can be expected to cause damage to national security. Most cyber programs, and in particular their capabilities, are classified, making public discussion almost impossible except in broad terms. As a result, publicly released documents regarding cyber issues tend to be very broad and vague, with little indication of the actual operational capabilities of cyber organizations.

propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyber threats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to U.S. critical infrastructures.

The tradecraft needed to effectively employ technology and tools remains an important limiting factor, particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to attack critical infrastructures.

Their goal is to weaken, disrupt or destroy the U.S. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the US economy, full scale attack of the infrastructure when attacked by the U.S. to damage the ability of the US to continue its attacks.

Terrorists

Traditional terrorist adversaries of the U.S., despite their intentions to damage U.S. interests, are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries. They are likely, therefore, to pose only a limited cyber threat. Since bombs still work better than bytes, terrorists are likely to stay focused on traditional attack methods in the near term. We anticipate more substantial cyber threats are possible in the future as a more technically competent generation enters the ranks.

Their goal is to spread terror throughout the U.S. civilian population. Their sub-goals include: attacks to cause 50,000 or more casualties within the U.S. and attacks to weaken the U.S. economy to detract from the Global War on Terror.

Industrial Spies and Organized Crime Groups

International corporate spies and organized crime organizations pose a medium-level threat to the US through their ability to conduct industrial espionage and large-scale monetary theft as well as their ability to hire or develop hacker talent.

Their goals are profit based. Their sub-goals include attacks on infrastructure for profit to competitors or other groups listed above, theft of trade secrets, and gain access and blackmail affected industry using potential public exposure as a threat.

Hacktivists

Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-U.S. motives. They pose a medium-level threat of carrying out an isolated but damaging attack. Most international hacktivist

groups appear bent on propaganda rather than damage to critical infrastructures. Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their cause.

Hackers

Although the most numerous and publicized cyber intrusions and other incidents are ascribed to lone computer-hacking hobbyists, such hackers pose a negligible threat of widespread, long-duration damage to national-level infrastructures. The large majority of hackers do not have the requisite tradecraft to threaten difficult targets such as critical U.S. networks and even fewer would have a motive to do so. Nevertheless, the large worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage, including extensive property damage or loss of life. As the hacker population grows, so does the likelihood of an exceptionally skilled and malicious hacker attempting and succeeding in such an attack.

In addition, the huge worldwide volume of relatively less skilled hacking activity raises the possibility of inadvertent disruption of a critical infrastructure.

For the purposes of this discussion, hackers are subdivided as follows:

- Sub-communities of hackers
- Script kiddies are unskilled attackers who do NOT have the ability to discover new vulnerabilities or write exploit code, and are dependent on the research and tools from others. Their goal is achievement. Their sub-goals are to gain access and deface web pages.
- Worm and virus writers are attackers who write the propagation code used in the worms and viruses but not typically the exploit code used to penetrate the systems infected. Their goal is notoriety. Their sub-goals are to cause disruption of networks and attached computer systems.
- Security researcher and white hat have two sub-categories; bug hunters and exploit coders. Their goal is profit. Their sub-goals are to improve security, earn money, and achieve recognition with an exploit.
- Professional hacker-black hat who gets paid to write exploits or actually penetrate networks; also falls into the two sub-categories-bug hunters and exploit coders. Their goal is profit.

Nature of the Computer Security Community

Hackers and researchers interact with each other to discuss common interests, regardless of color of hat. Hackers and researchers specialize in one or two areas of expertise and depend on the exchange of ideas and tools to boost their capabilities in other areas. Information regarding computer security research flows slowly from the inner circle of the best researchers and hackers to the general IT security world, in a ripple-like pattern.

SOURCE: Government Accountability Office, *Cyber Threat Source Descriptions* (Washington, D.C., 2005), https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

ANALYSIS

Although providing common definitions of important categories of threats in the cyber domain was a useful function, the GAO also supplied some extremely varied suppositions regarding the objectives and motivations of actors within the cyber domain. For example, the pronouncement that terror organizations seek to cause 50,000 casualties seems to be a figure drawn from thin air—the combined casualties of every terrorism incident to date in 2005 would not come close, and the deadliest terror attack in history caused less than 10 percent of that number. Likewise, attempting to distill the motivations of individual categories of hackers down to such oversimplified generalizations probably undercut the general thrust of this summary and minimized the threat in an unmerited fashion. However, given that 2005 was relatively early in terms of major cyber intrusions, particularly from nation-states, it is noteworthy that the GAO even created such a document and supplied it to the legislative branch, which had done little, if anything, to consider the dangers of cyberattacks.

- ***Document 38:*** *The Comprehensive National Cybersecurity Initiative*
- ***When:*** 2009
- ***Where:*** Washington, D.C.
- ***Significance:*** President Barack Obama entered his first term with a firm grasp of the inherent difficulties of defending the nation's cyber assets and keeping critical infrastructure safe from attack via the internet. In his first year, he announced a Comprehensive National Cybersecurity Initiative, with a series of specific goals to improve the nation's cybersecurity.

DOCUMENT

CNCI Initiative Details

Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections. The Trusted Internet Connections (TIC) initiative, headed by the Office of Management and Budget and the Department of Homeland Security, covers the consolidation of the Federal Government's external access points (including those to the internet). This consolidation will result in a common security solution which includes: facilitating the reduction of external access points, establishing baseline security capabilities; and, validating agency adherence to those security capabilities. Agencies participate in the

TIC initiative either as TIC Access Providers (a limited number of agencies that operate their own capabilities) or by contracting with commercial Managed Trusted IP Service (MTIPS) providers through the GSA [Government Services Agency]-managed NETWORX contract vehicle.

Initiative #2. Deploy an intrusion detection system of sensors across the Federal enterprise. Intrusion Detection Systems using passive sensors form a vital part of U.S. Government network defenses by identifying when unauthorized users attempt to gain access to those networks. DHS is deploying, as part of its EINSTEIN 2 activities, signature-based sensors capable of inspecting internet traffic entering Federal systems for unauthorized accesses and malicious content. The EINSTEIN 2 capability enables analysis of network flow information to identify potential malicious activity while conducting automatic full packet inspection of traffic entering or exiting U.S. Government networks for malicious activity using signature-based intrusion detection technology. Associated with this investment in technology is a parallel investment in manpower with the expertise required to accomplish DHS's expanded network security mission. EINSTEIN 2 is capable of alerting US-CERT in real time to the presence of malicious or potentially harmful activity in federal network traffic and provides correlation and visualization of the derived data. Due to the capabilities within EINSTEIN 2, US-CERT analysts have a greatly improved understanding of the network environment and an increased ability to address the weaknesses and vulnerabilities in Federal network security. As a result, US-CERT has greater situational awareness and can more effectively develop and more readily share security relevant information with network defenders across the U.S. Government, as well as with security professionals in the private sector and the American public. The Department of Homeland Security's Privacy Office has conducted and published a Privacy Impact Assessment for the EINSTEIN 2 program.

Initiative #3. Pursue deployment of intrusion prevention systems across the Federal enterprise. This Initiative represents the next evolution of protection for civilian Departments and Agencies of the Federal Executive Branch. This approach, called EINSTEIN 3, will draw on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision-making on network traffic entering or leaving these Executive Branch networks. The goal of EINSTEIN 3 is to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response. It will have the ability to automatically detect and respond appropriately to cyber threats before harm is done, providing an intrusion prevention system supporting dynamic defense. EINSTEIN 3 will assist DHS US-CERT in defending, protecting and reducing vulnerabilities on Federal Executive Branch networks and systems.

DID YOU KNOW?

EINSTEIN

EINSTEIN is a cyber-security system devised and managed by the Department of Homeland Security as a means to protect federal computer networks. EINSTEIN has been gradually improved, moving from a system designed to monitor traffic and assist in investigations into hacking activities, and becoming a full-scale security system with traffic-blocking capabilities. In addition to detecting and blocking commercially available malware, EINSTEIN can also detect common malware signatures and block the related traffic, even if the specific malware has not yet been diagnosed. EINSTEIN's continued development led to a 2014 inclusion of the program into the Border Gateway Protocol (BGP) backbone of the internet, allowing it to observe an enormous percentage of federal civilian traffic, further enhancing its defensive function. Although EINSTEIN is not capable of stopping all malicious traffic, it provides a substantial portion of the federal cyber defense baseline for government computer networks, preventing most low-level incursions and speeding the response to more sophisticated attacks.

The EINSTEIN 3 system will also support enhanced information sharing by US-CERT with Federal Departments and Agencies by giving DHS the ability to automate alerting of detected network intrusion attempts and, when deemed necessary by DHS, to send alerts that do not contain the content of communications to the National Security Agency (NSA) so that DHS efforts may be supported by NSA exercising its lawfully authorized missions. This initiative makes substantial and long-term investments to increase national intelligence capabilities to discover critical information about foreign cyber threats and use this insight to inform EINSTEIN 3 systems in real time. DHS will be able to adapt threat signatures determined by NSA in the course of its foreign intelligence and DoD information assurance missions for use in the EINSTEIN 3 system in support of DHS's federal system security mission. Information sharing on cyber intrusions will be conducted in accordance with the laws and oversight for activities related to homeland security, intelligence, and defense in order to protect the privacy and rights of U.S. citizens.

DHS is currently conducting an exercise to pilot the EINSTEIN 3 capabilities described in this initiative based on technology developed by NSA and to solidify processes for managing and protecting information gleaned from observed cyber intrusions against civilian Executive Branch systems. Government civil liberties and privacy officials are working closely with DHS and US-CERT to build appropriate and necessary privacy protections into the design and operational deployment of EINSTEIN 3.

Initiative #4: Coordinate and redirect research and development (R&D) efforts. No single individual or organization is aware of all of the cyber-related R&D activities being funded by the Government. This initiative is developing strategies and structures for coordinating all cyber R&D sponsored or conducted by the U.S. government, both classified and unclassified, and to redirect that R&D where needed. This Initiative is critical to eliminate redundancies in federally funded cybersecurity research, and to identify research gaps, prioritize R&D efforts, and ensure the taxpayers are getting full value for their money as we shape our strategic investments.

Initiative #5. Connect current cyber ops centers to enhance situational awareness. There is a pressing need to ensure that government information security offices and strategic operations centers share data regarding malicious activities against federal systems, consistent with privacy protections for personally identifiable and other protected information and as legally appropriate, in order to have a better understanding of the entire threat to government systems and to take maximum advantage of each organization's unique capabilities to produce the best overall national cyber defense possible. This initiative provides the key means necessary to enable and support shared situational awareness and collaboration across six centers that are responsible for carrying out U.S. cyber activities. This effort focuses on key aspects necessary to enable practical mission bridging across the elements of U.S. cyber activities: foundational capabilities and investments such as upgraded infrastructure, increased bandwidth, and integrated operational capabilities; enhanced collaboration, including common technology, tools, and procedures; and enhanced shared situational awareness through shared analytic and collaborative technologies.

The National Cybersecurity Center (NCSC) within the Department of Homeland Security will play a key role in securing U.S. Government networks and systems under this initiative by coordinating and integrating information from the six centers to provide cross-domain situational awareness, analyzing and reporting on the state of U.S. networks and systems, and fostering interagency collaboration and coordination.

Initiative #6. Develop and implement a government-wide cyber counterintelligence (CI) plan. A government-wide cyber counterintelligence plan is necessary to coordinate activities across all Federal Agencies to detect, deter, and mitigate the foreign-sponsored cyber intelligence threat to U.S. and private sector information systems. To accomplish these goals, the plan establishes and expands cyber CI education and awareness programs and workforce development to integrate CI into all cyber operations and analysis, increase employee awareness of the cyber CI threat, and increase counterintelligence collaboration across the government. The Cyber CI Plan is aligned with the National Counterintelligence Strategy of the United States of America (2007) and supports the other programmatic elements of the CNCI.

Initiative #7. Increase the security of our classified networks. Classified networks house the Federal Government's most sensitive information and enable crucial war-fighting, diplomatic, counterterrorism, law enforcement, intelligence, and homeland security operations. Successful penetration or disruption of these networks could cause exceptionally grave damage to our national security. We need to exercise due diligence in ensuring the integrity of these networks and the data they contain.

Initiative #8. Expand cyber education. While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge.

Initiative #9. Define and develop enduring "leap-ahead" technology, strategies, and programs. One goal of the CNCI is to develop technologies that provide increases in cybersecurity by orders of magnitude above current systems and which can be deployed within 5 to 10 years. This initiative seeks to develop strategies and programs to enhance the component of the government R&D portfolio that pursues high-risk/high-payoff solutions to critical cybersecurity problems. The Federal Government has begun to outline Grand Challenges for the research community to help solve these difficult problems that require "out of the box" thinking. In dealing with the private sector, the government is identifying and communicating common needs that should drive mutual investment in key research areas.

Initiative #10. Define and develop enduring deterrence strategies and programs. Our Nation's senior policymakers must think through the long-range strategic options available to the United States in a world that depends on assuring the use of cyberspace. To date, the U.S. Government has been implementing traditional approaches to the cybersecurity problem—and these measures have not achieved the level of security needed. This Initiative is aimed at building an approach to cyber defense strategy that deters interference and attack in cyberspace by improving warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors.

Initiative #11. Develop a multi-pronged approach for global supply chain risk management. Globalization of the commercial information and communications technology marketplace provides increased opportunities for those intent on harming the United States by penetrating the supply chain to gain unauthorized access to data, alter data, or interrupt communications. Risks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices. This initiative will enhance Federal Government skills, policies, and processes to provide departments and agencies with a robust toolset to better manage and mitigate supply chain risk at levels commensurate with the criticality of, and risks to, their systems and networks.

Initiative #12. Define the Federal role for extending cybersecurity into critical infrastructure domains. The U.S. Government depends on a variety of privately owned and operated critical infrastructures to carry out the public's business. In turn, these critical infrastructures rely on the efficient operation of information systems and networks that are vulnerable to malicious cyber threats. This Initiative builds on the existing and ongoing partnership between the Federal Government and the public and private sector owners and operators of Critical Infrastructure and Key Resources (CIKR). The Department of Homeland Security and its private-sector partners have developed a plan of shared action with an aggressive series of milestones and activities. It includes both short-term and long-term recommendations, specifically incorporating and leveraging previous accomplishments and activities that are already underway. It addresses security and information assurance efforts across the cyber infrastructure to increase resiliency and operational capabilities throughout the CIKR sectors. It includes a focus on public-private sharing of information regarding cyber threats and incidents in both government and CIKR.

SOURCE: White House, *The Comprehensive National Cybersecurity Initiative* (Washington, D.C., 2009), 2–5, https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf

ANALYSIS

The Comprehensive National Cybersecurity Initiative contained a wide variety of overarching goals, some of which seemed quite straightforward and relatively short term, if not necessarily easy to achieve. Calling for improvements to the nation's classified computer networks was a clear objective, but given the size and connectivity of those networks, and the number of terminals connected to them, upgrading the security of the full networks proved to be an extremely costly initiative. Others were much longer projects designed to improve the foundation of the nation's cyber resources. For example, an initiative to expand the nation's cyber education programs might provide a much-improved base of citizens with the necessary skills to contribute to cyber defense—but it might take years or even decades to implement and show progress. Also, given the federal government's role (or lack thereof) in education, such an initiative required the willing partnership of a wide variety of educational institutions, which in turn might not be able to call upon the necessary expertise to expand their efforts in the short term. However, this document ultimately served to illustrate the administration's priorities for cybersecurity, demonstrating the aspects deemed most important by the federal government.

- ***Document 39:*** *Resilient Military Systems and the Advanced Cyber Threat*
- ***When:*** January 2013
- ***Where:*** Washington, D.C.
- ***Significance:*** In 2013, the Defense Science Board (DSB), a Department of Defense office tasked with remaining current regarding scientific and technological advances, particularly in military systems, warned that some potential adversaries may be capable of disrupting U.S. information technology systems, especially on a local level. In its report, the DSB suggested that the Department of Defense should take the lead in producing a new information technology network and urged lawmakers to provide the necessary resources to commence it.

DOCUMENT

Executive Summary

The United States cannot be confident that our critical Information Technology (IT) systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and

intelligence capabilities (a "full spectrum" adversary). While this is also true for others (e.g. Allies, rivals, and public/private networks), this Task Force strongly believes the DoD needs to take the lead and build an effective response to measurably increase confidence in the IT systems we depend on (public and private) and at the same time decrease a would-be attacker's confidence in the effectiveness of their capabilities to compromise DoD systems. We have recommended an approach to do so, and we need to start now!

While DoD takes great care to secure the use and operation of the "hardware" of its weapon systems, these security practices have not kept up with the cyber adversary tactics and capabilities. Further, the same level of resource and attention is not spent on the complex network of information technology (IT) systems that are used to support and operate those weapons or critical cyber capabilities embedded within them. This Task Force was asked to review and make recommendations to improve the resilience of DoD systems to cyber attacks and to develop a set of metrics that the Department could use to track progress and shape investment priorities.

Over the past 18 months, the Task Force received more than 50 briefings from practitioners and senior officials throughout the DoD, Intelligence Community (IC), commercial practitioners, academia, national laboratories, and policymakers. As a result of its deliberations, the Task Force concludes that:

- The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War
- The cyber threat is also insidious, enabling adversaries to access vast new channels of intelligence about critical U.S. enablers (operational and technical; military and industrial) that can threaten our national and economic security
- Current DoD actions, though numerous, are fragmented. Thus, DoD is not prepared to defend against this threat ν DoD red teams, using cyber attack tools which can be downloaded from the internet, are very successful at defeating our systems
- U.S. networks are built on inherently insecure architectures with increasing use of foreign-built components
- U.S. intelligence against peer threats targeting DoD systems is inadequate
- With present capabilities and technology it is not possible to defend with confidence against the most sophisticated cyber attacks
- It will take years for the Department to build an effective response to the cyber threat to include elements of deterrence, mission assurance and offensive cyber capabilities.

. . .

Background

The adversary is in our networks. Then Deputy Secretary of Defense William Lynn's 2010 Foreign Affairs article documented a significant compromise of DoD classified networks in 2008 through the simple insertion of an infected flash drive. Moreover, adversaries exploit more than military operational systems, but intellectual property relevant to our commercial industries as well.

The DoD, and its contractor base are high priority targets that have sustained staggering losses of system design information incorporating years of combat knowledge and experience. Employing reverse engineering techniques, adversaries can exploit weapon system technical plans for their benefit. Perhaps even more significant, they gained insight to operational concepts and system use (e.g., which processes are automated and which are person controlled) developed from decades of U.S. operational and developmental experience—the type of information that cannot simply be recreated in a laboratory or factory environment. Such information provides tremendous benefit to an adversary, shortening time for development of countermeasures by years.

In addition, there is evidence of attacks that exploit known vulnerabilities in the domestic power grid and critical infrastructure systems. DoD, and the United States, is extremely reliant on the availability of its critical infrastructure.

Exploitation is not a new threat. For years adversaries have infiltrated U.S. systems, sometimes detected, sometimes deflected, but almost never deterred. A recently declassified Soviet Union operation against the United States serves as an effective example. Starting in the late 1970s, the Gunman operation exploited an operationally introduced vulnerability resulting in the transmission to Soviet intelligence of every keystroke in 16 IBM Selectric typewriters located in the U.S. Embassy in Moscow and the U.S. Mission in Leningrad. More recently, in 2010, the 2nd International Conference on Information Engineering and Computer Science (ICIECS), published an article titled "Towards Hardware Trojan: Problem Analysis and Trojan Simulation" authored by members of the Department of Computer Science and Technology Zhengzhou Institute of Information Science and Technology, in Zhengzhou, China which outlined the technical approach elements for developing covertly modified hardware. The concept of hardware modification is so prevalent now that criminal elements routinely insert modified or replacement card readers to steal customer information from automated teller machines (ATMs), and other commercial activities.

Recent DoD and U.S. interest in counterfeit parts has resulted in the identification of widespread introduction of counterfeit parts into DoD systems through commercial supply chains. Since many systems use the same processors and those processors are typically built overseas in untrustworthy environments, the challenge to supply chain management in a cyber-contested environment is significant.

Identification of operationally introduced vulnerabilities in complex systems is extremely difficult technically, and as a result, cost prohibitive. The United States only learned of Project GUNMAN via a tipoff from a liaison intelligence service. The ability of intelligence to provide unique and specific information provides some mitigation against a Tier V-VI adversary's ability to introduce vulnerabilities.

DoD is in the process of institutionalizing a Supply Chain Risk Management (SCRM) strategy that prioritizes scarce security resources on critical mission systems and components, provides intelligence analysis to acquisition programs and incorporates vulnerability risk mitigation requirements into system designs.

The success of DoD red teams against its operational systems should also give pause to DoD leadership. During exercises and testing, DoD red teams, using only small teams and a short amount of time, are able to significantly disrupt the "blue

team's" ability to carry out military missions. Typically, the disruption is so great, that the exercise must be essentially reset without the cyber intrusion to allow enough operational capability to proceed. These stark demonstrations contribute to the Task Force's assertion that the functioning of DoD's systems is not assured in the presence of even a modestly aggressive cyber attack.

The DSB 2010 Summer Study addressed the issue of degraded operations and the need to include cyber attacks in realistic exercises. The Chairman, Joint Chiefs of Staff, issued an instruction in February 20116 mandating that all DoD exercises begin to include realistic cyber attacks into their war games. If this level of damage can be done by a few smart people, in a few days, using tools available to everyone, imagine what a determined, sophisticated adversary with large amounts of people, time, and money could do.

New is the wide spread knowledge of the destructive ability of cyber attacks (e.g. Aurora, Stuxnet, etc.). The cyber world has moved from exploitation and disruption to destruction.

The benefits to an attacker using cyber exploits are potentially spectacular. Should the United States find itself in a full-scale conflict with a peer adversary, attacks would be expected to include denial of service, data corruption, supply chain corruption, traitorous insiders, kinetic and related non-kinetic attacks at all altitudes from underwater to space. U.S. guns, missiles, and bombs may not fire, or may be directed against our own troops. Resupply, including food, water, ammunition, and fuel may not arrive when or where needed. Military Commanders may rapidly lose trust in the information and ability to control U.S. systems and forces. Once lost, that trust is very difficult to regain.

The impact of a destructive cyber attack on the civilian population would be even greater with no electricity, money, communications, TV, radio, or fuel (electrically pumped). In a short time, food and medicine distribution systems would be ineffective; transportation would fail or become so chaotic as to be useless. Law enforcement, medical staff, and emergency personnel capabilities could be expected to be barely functional in the short term and dysfunctional over sustained periods. If the attack's effects were reversible, damage could be limited to an impact equivalent to a power outage lasting a few days. If an attack's effects cause physical damage to control systems, pumps, engines, generators, controllers, etc., the unavailability of parts and manufacturing capacity could mean months to years are required to rebuild and reestablish basic infrastructure operation.

The DoD should expect cyber attacks to be part of all conflicts in the future, and should not expect competitors to play by our version of the rules, but instead apply their rules (e.g. using surrogates for exploitation and offense operations, sharing IP with local industries for economic gain, etc.).

Based upon the societal dependence on these systems, and the interdependence of the various services and capabilities, the Task Force believes that the integrated impact of a cyber attack has the potential of existential consequence. While the manifestation of a nuclear and cyber attack are very different, in the end, the existential impact to the United States is the same.

. . .

Recommendations

An overview of the Task Force's recommendations is included in this executive summary. Recommendation details, including proposed organizational assignments and due dates, are described further in the main body of the report.

1. Protect the Nuclear Strike as a Deterrent (for existing nuclear armed states and existential cyber attack).

    - Secretary of Defense (SECDEF) assign United States Strategic Command (USSTRATCOM) the task to ensure the availability of Nuclear Command, Control and Communications (C3) and the Triad delivery platforms in the face of a fullspectrum Tier V-VI attack—including cyber (supply chain, insiders, communications, etc.).

Our nuclear deterrent is regularly evaluated for reliability and readiness. However most of the systems have not been assessed (end-to-end) against a Tier V-VI cyber attack to understand possible weak spots. A 2007 Air Force study addressed portions of this issue for the ICBM leg of the U.S. triad but was still not a complete assessment against a high-tier threat.

The Task Force believes that our capacity for deterrence will remain viable into the foreseeable future, only because cyber practitioners that pose Tier V-VI level threats are limited to a few state actors who have much to hold at risk, combined with confidence in our ability to attribute an existential level attack.

2. Determine the Mix of Cyber, Protected-Conventional, and Nuclear Capabilities Necessary for Assured Operation in the Face of a Full-Spectrum Adversary.

    - SECDEF and Chairman, Joint Chiefs of Staff (CJCS) designate a mix of forces necessary for assured operation.

To ensure the President has options beyond a nuclear-only response to a catastrophic cyber attack, the DoD must develop a mix of offensive cyber and high-confidence conventional capabilities. Cyber offense may provide the means to respond in-kind. The protected conventional capability should provide credible and observable kinetic effects globally. Forces supporting this capability are isolated and segmented from general purpose forces to maintain the highest level of cyber resiliency at an affordable cost. Nuclear weapons would remain the ultimate response and anchor the deterrence ladder. This strategy builds a real ladder of capabilities and alleviates the need to protect all of our systems to the highest level requirements, which is unaffordable for the nation. Similar to the prior argument regarding the cyber resiliency of the nuclear deterrent, DoD must ensure that some portion of its conventional capability is able to provide assured operations for theater and regional operations within a full-spectrum, cyber-stressed environment.

Because of the expected cost of implementation, the protected-conventional capability must support a limited number of cyber critical survivable missions. This Task Force recommends improving the cyber resiliency of a mix of the following systems for assured operation in the face of a full spectrum adversary: global selective

strike systems e.g. penetrating bombers, submarines with long range cruise missiles, Conventional Prompt Global Strike (CPGS), survivable national and combatant command (CCMD) C2.

- Segment Sufficient Forces to Assure Mission Execution in a Cyber Environment

Segmentation must differentiate only sufficient forces required to assure mission execution; it is not required across an entire capability. For example, if long range strike is a component of the protected-conventional capability, then DoD should segment a sufficient quantity that is designated as a cyber critical survivable mission. Notionally, 20 aircraft designated by tail number, out of a fleet of hundreds, might be segregated and treated as part of the cyber critical survivable mission force. Segmented forces must remain separate and isolated from the general purpose forces, with no dual purpose missions (e.g. the current B-52 conventional/nuclear mission).

DoD must engage multi-agency counterparts for an updated Strategic Deterrence Strategy, including the development of cyber escalation scenarios and thin lines.

3. Refocus Intelligence Collection and Analysis to Understand Adversarial Cyber Capabilities, Plans and Intentions, and to Enable Counterstrategies.
    - SECDEF in coordination with the Directors of CIA, FBI, and DHS, should require the Director of National Intelligence (DNI) to support enhanced intelligence collection and analysis on high-end cyber threats.

Intelligence must include the identification and understanding of adversarial cyber weapon development organizations, tools, leadership, and intentions, and the development of targeting information to support initiatives to counter cyber weaponization. Mitigating a Tier V-VI threat is impossible without filling these intelligence gaps. Therefore, the Intelligence Community (IC) should increase the priority of its intelligence collection and reporting requirements in this domain.

4. Build and Maintain World-Class Cyber Offensive Capabilities (with appropriate authorities).
    - United States Cyber Command (USCYBERCOM) develop capability to model, game and train for full-scale cyber warfare.
    - Under Secretary of Defense for Personnel and Readiness (USD(P&R)) establish a formal career path for civilian and military personnel engaged in offensive cyber actions.

Today, the United States is a leader in cyber offensive capabilities. However, most training and engagements are very limited and in controlled environments. Preparing for full-scale force-onforce cyber battle is not well understood. Challenges range from the scale of numbers of expected sorties to uncertainty of triggering mechanisms, trust and capability recovery timelines, and potential blowback of attacks all happening within the fog of war. To prepare, DoD must first begin to understand the full complexities of cyber war.

Recommendations include developing the capability to model, war game, red team and eventually train for full scale peer-on-peer cyber warfare. A policy framework should be established for offensive cyber actions, to include who has the authority and under what circumstances and controls to act.

Finally, DoD needs to significantly increase the number of qualified "cyber warriors" and enlarge the offensive cyber infrastructure commensurate with the size of threat. Professionalizing the cyber offense skill set and providing career ladders in this new field will be a key element toward growing the human resources required to compete effectively. This report is especially concerned with developing top-tier talent who can be certified to perform at the elite or extreme cyber conflict levels. The United States needs such world class performers in substantial numbers—some of whom may not be eligible for security clearances.

5. Enhance Defenses to Protect Against Low and Mid-Tier Threats.

    - DoD Chief Information Officer (CIO) in collaboration with the Military Departments and Agencies establish an enterprise security architecture, including appropriate "Building Codes and Standards," that ensure the availability of enabling enterprise missions.

Some adversaries will not be deterred (e.g., terrorist organizations and lone wolves); DoD must defend its systems against these low- and mid-tier threats. Therefore, the Task Force recommends that the DoD CIO establish a DoD-wide "Enterprise" architecture, including "building codes and standards" that ensure availability of mission operations during peace-time and full-spectrum wartime events. The building code analogy suggests that DoD should not make every network across the DoD identical, but instead should ensure that all networks, even when tailored by the Military Departments and end-users, meet a robust set of minimum standards that ensure a reasonable system network defense can be provided. U.S. networks also need requirements for instrumentation to increase the probability of detection of attacks and create situational awareness to speed remediation. Existing acquisition programs should be influenced, to the maximum extent feasible, with the new requirements. Audits should be conducted to the standard, and conducting in-process reviews to develop migration and mitigation strategies are critical. Legacy systems that cannot be maintained in a timely manner, (and DoD has many of them) must be enclaved and firewalled from the Global Information Grid (GIG).

Commercial technologies that enable the automation of some network maintenance activities and provide real-time mitigation of detected malware are available today. The Task Force believes that use of these technologies would actually drive network operation costs down and free up resources to hunt on the network for intruders.

6. Change DoD's Culture Regarding Cyber and Cyber Security.

    - SECDEF/CJCS establish a DoD-wide policy, communication, education and enforcement program to change the culture regarding cyber and cyber security

Establish a DoD-wide policy, communication, and education program to change the cyber culture. When focused, DoD can be one of the most disciplined large organizations in the world. It is this discipline that enables DoD to establish and execute processes that ensure the physical fitness of the armed forces, the safe and secure handling of weapons and the effective management of classified material. The same level of importance and discipline has not been applied to cyber hygiene and security. We will not succeed in securing our systems against even low- and mid-tier threats without changing this dynamic.

Communication of the critical importance of DoD cyber hygiene must be led by the SECDEF, CJCS, and their direct reports. Updated policies and training programs, and providing clear, punitive consequences for breach of policy will be necessary to move DoD to a higher level of cyber readiness.

7. Build a Cyber Resilient Force.
    - Deputy Secretary of Defense (DEPSECDEF) should direct specific actions to introduce cyber resiliency requirements throughout DoD force structure to include:
    - Build a set of standards/requirements that incorporate cyber resiliency into the cyber critical survivable mission systems identified in Recommendation 2, (Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), DoD CIO)

The DoD CIO, in coordination with USD(AT&L), should establish a resiliency standard to design, build and measure capability against. The Joint Staff will use the standard to inform the requirements process. The cyber resiliency standard should be applied to sufficient segments of the force structure identified as the conventional components of the escalation ladder (see Recommendation 2) to achieve a credible deterrent effect.

- Apply a subset of the cyber resiliency standard developed above to all other DoD programs (USD(AT&L), DOD CIO, Service Acquisition Executives (SAEs))
- Increase feedback from testing, red teaming, the Intelligence Community, and modeling and simulation as a development mechanism to build-out DoD's cyber resilient force (USD(AT&L), Undersecretary of Defense for Intelligence (USD(I)), DOT&E, SAEs, CJCS)
- Develop a DoD-wide cyber technical workforce to support the build out of the cyber critical survivable mission capability and rollout to DoD force structure (USD(AT&L), CIO, SAEs, Director, Operational Test and Evaluation (DOT&E), USD(I), USD(P&R))
- Science and Technology community establish secure system design project with Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), academia, commercial and defense industry (Assistant Secretary of Defense for Research and Engineering (ASD(R&E))
- Intelligence community should initiate a supply chain collection activity (USD(I))

SOURCE: U.S. Department of Defense, Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2013), 1, 3–6, 7–11, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

ANALYSIS

By 2013, it was clear that U.S. computer networks would be under attack on an almost continuous basis from threats ranging from individual hackers to nation-states. Even in times of relative peace, cyber incursions continued to strike across the range of U.S. cyber operations, and if the United States found itself in a major conflict with a global power, such as Russia or China, the consequences for the poorly protected information technology system would likely be disastrous. As such, the DSB presented a list of strongly worded recommendations to attempt to stimulate the U.S. government, and the Department of Defense in particular, to proactively build a much more robust and defensible network suitable for maintaining key functions even in a degraded environment.

- ***Document 40:*** *Executive Order 13636—Improving Critical Infrastructure Cybersecurity*
- ***When:*** February 12, 2013
- ***Where:*** Washington, D.C.
- ***Significance:*** Presidential Executive Orders tend to be utilized as a means of effecting immediate change over a current or developing problem before the legislative process can create a more permanent solution. Every president has issued such orders on an almost limitless selection of topics. In 2013, President Barack Obama chose to issue Executive Order 13636 to take emergency action to protect the nation's critical infrastructure from cyberattack.

DOCUMENT

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and

resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.

. . .

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

(b) The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them. The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a system for tracking the production, dissemination, and disposition of these reports.

(c) To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary, consistent with 6 U.S.C. 143 and in collaboration with the Secretary of Defense, shall, within 120 days of the date of this order, establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible critical infrastructure companies or commercial service providers that offer security services to critical infrastructure.

(d) The Secretary, as the Executive Agent for the Classified National Security Information Program created under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities), shall expedite the processing of security clearances to appropriate personnel employed by critical infrastructure owners and operators, prioritizing the critical infrastructure identified in section 9 of this order.

(e) In order to maximize the utility of cyber threat information sharing with the private sector, the Secretary shall expand the use of programs that bring private sector subject-matter experts into Federal service on a temporary basis. These subject matter experts should provide advice regarding the content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks.

. . .

Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and OMB Circular A-119, as revised.

(b) The Cybersecurity Framework shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Framework shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure. The Cybersecurity Framework will also identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. To enable technical innovation and account for organizational differences, the Cybersecurity Framework will provide guidance that is technology neutral and that enables critical infrastructure sectors to benefit from a competitive market for products and services that meet the standards, methodologies, procedures, and processes developed to address cyber risks. The Cybersecurity Framework shall include guidance for measuring the performance of an entity in implementing the Cybersecurity Framework.

(c) The Cybersecurity Framework shall include methodologies to identify and mitigate impacts of the Cybersecurity Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

(d) In developing the Cybersecurity Framework, the Director shall engage in an open public review and comment process. The Director shall also consult with the Secretary, the National Security Agency, Sector-Specific Agencies and other interested agencies including OMB, owners and operators of critical infrastructure, and other stakeholders through the consultative process established in section 6 of this order. The Secretary, the Director of National Intelligence, and the heads of other relevant agencies shall provide threat and vulnerability information and technical expertise to inform the development of the Cybersecurity Framework. The Secretary shall provide performance goals for the Cybersecurity Framework informed by work under section 9 of this order.

(e) Within 240 days of the date of this order, the Director shall publish a preliminary version of the Cybersecurity Framework (the "preliminary Framework"). Within 1 year of the date of this order, and after coordination with the Secretary to ensure suitability under section 8 of this order, the Director shall publish a final version of the Cybersecurity Framework (the "final Framework").

(f) Consistent with statutory responsibilities, the Director will ensure the Cybersecurity Framework and related guidance is reviewed and updated as necessary, taking into consideration technological changes, changes in cyber risks, operational feedback from owners and operators of critical infrastructure, experience from the implementation of section 8 of this order, and any other relevant factors.

SOURCE: Barack Obama, *Executive Order 13636—Improving Critical Infrastructure Cybersecurity* (Washington, D.C., 2013). https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

ANALYSIS

Because the president is the head of the executive branch of government, he or she has the power to issue direct orders to all of the executive federal agencies. When a president wishes to issue a blanket order to all agencies at once, the most common mechanism is an Executive Order. These pronouncements can be overridden or modified through legislative action, if necessary, although legislative fixes to the same problems have often followed the same approach as the preceding presidential directives. In this case, President Obama expected the U.S. Congress to create some form of legislation mandating a greater effort on the part of federal agencies to undertake the cyber defense mission for critical infrastructure and to coordinate the efforts of private organizations toward the same goal. However, given the then-recent spate of cyberattacks against a wide variety of critical targets, in which the owners and operators of those targets had not done sufficient work to protect themselves, he issued this order to solve the immediate crisis.

- ***Document 41:*** *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*
- ***When:*** February 2013
- ***Where:*** Washington, D.C.
- ***Significance:*** The Government Accountability Office (GAO) is a legislative branch that provides audit services to the federal government. In this document, the GAO's perspective on the state of the nation's cyber defense systems is clearly provided. Because the GAO is outside of the executive branch, it has the unique position to provide an unbiased evaluation of how well other federal agencies were performing in their efforts to cooperate toward cyber defense.

DOCUMENT

Conclusions

Given the range and sophistication of the threats and potential exploits that confront government agencies and the nation's cyber critical infrastructure, it is critical that the government adopt a comprehensive strategic approach to mitigating the risks of successful cybersecurity attacks. Such an approach would not only define priority problem areas but also set a roadmap for allocating and managing appropriate resources, making a convincing business case to justify expenses, identifying organizations' roles and responsibilities, linking goals and priorities, and holding participants accountable for achieving results. However, the federal government's efforts at defining a strategy for cybersecurity have often not fully addressed these key elements, lacking, for example, milestones and performance measures, identified costs and sources of funding, and specific roles and responsibilities. As a result, the government's cybersecurity strategy remains poorly articulated and incomplete. In fact, no integrated, overarching strategy exists that articulates priority actions, assigns responsibilities for performing them, and sets time frames for their completion. In the absence of an integrated strategy, the documents that comprise the government's current strategic approach are of limited value as a tool for mobilizing actions to mitigate the most serious threats facing the nation.

Previous GAO and inspector general reviews as well as federal CIOs and experts have made recommendations to address challenges faced by federal agencies and the private sector in effectively implementing a comprehensive approach to cybersecurity and reducing the risk of successful cybersecurity attacks. Many of these recommendations have not yet been fully addressed, leaving much room for more progress in addressing cybersecurity challenges. In many cases, the causes of these challenges are closely related to the key elements that are missing from the government's cybersecurity strategy. For example, the persistence of shortcomings in agency cybersecurity risk management processes indicates that agencies have not been held accountable for effectively implementing such processes and that oversight mechanisms have not been clear. It is just such oversight and accountability that is poorly defined in cybersecurity strategy documents. Clarifying oversight responsibilities is a topic that could be effectively addressed through legislation.

An overarching strategy that better addresses key desirable characteristics could establish an improved framework to implement national cybersecurity policy and ensure that stated goals and priorities are actively pursued by government agencies and better supported by key private sector entities. To be successful such a strategy would include a clearer process for OMB oversight of agency risk management processes and a roadmap for improving the cybersecurity challenge areas where previous concerns have not been fully addressed. The development and implementation of such a strategy would likely lead to significant progress in furthering strategic goals and lessening persistent weaknesses.

Recommendations for Executive Action

In order to institute a more effective framework for implementing cybersecurity activities, and to help ensure such activities will lead to progress in cybersecurity,

we recommend that the White House Cybersecurity Coordinator in the Executive Office of the President develop an overarching federal cybersecurity strategy that includes all key elements of the desirable characteristics of a national strategy, including

- milestones and performance measures for major activities to address stated priorities;
- cost, sources, and justification for needed resources to accomplish stated priorities;
- specific roles and responsibilities of federal organizations related to the strategy's stated priorities; and
- guidance, where appropriate, regarding how this strategy relates to priorities, goals, and objectives stated in other national strategy documents.

This strategy should also better ensure that federal departments and agencies are held accountable for making significant improvements in cybersecurity challenge areas, including designing and implementing risk-based programs; detecting, responding to, and mitigating cyber incidents; promoting education, awareness, and workforce planning; promoting R&D; and addressing international cybersecurity challenges. To address these issues, the strategy should (1) clarify how OMB will oversee agency implementation of requirements for effective risk management processes and (2) establish a roadmap for making significant improvements in cybersecurity challenge areas where previous recommendations have not been fully addressed.

SOURCE: U.S. Government Accountability Office, "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented" Report to Congressional Addressees, Washington, D.C., 2013, https://www.gao.gov/assets/660/652170.pdf

ANALYSIS

The GAO analysis succinctly points out the inherent flaws in many executive pronouncements regarding the need for enhanced security cooperation in the cyber domain. Although there were an enormous number of documents and directives calling for better coordination of federal agencies, few, if any, actually had any specific details regarding how such cooperation should be achieved. Instead, they tended to repeat the same platitudes and general statements without any concrete guidance of the expectations for the affected agencies. Unsurprisingly, the result was that very little was actually done to enhance cooperation, beyond public pronouncements of future intentions and the need for greater coordination. GAO's report has a very clear recommendation of how to proceed to actually improve the function of the nation's cyber defenses, in part by naming one agency, the Office of Management and Budget (OMB), to serve as the overarching agency coordinating the efforts.

- ***Document 42:*** *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience*
- ***When:*** 2013
- ***Where:*** Washington, D.C.
- ***Significance:*** Critical infrastructure assets present a particularly thorny problem when it comes to cybersecurity. The catastrophic damage that might occur if a cyberattack destroyed a nuclear power station or a major rail hub or a substantial portion of the nation's electrical grid means that it is in the federal government's interest to devote assets to the cybersecurity of such assets, even if they are not explicitly owned by the federal government. Some major efforts require a whole-of-government approach to be effective. This plan was devised to create such an approach regarding the potential for cyberattacks against critical infrastructure in the United States.

DOCUMENT

Risk Environment

The risk environment affecting critical infrastructure is complex and uncertain; threats, vulnerabilities, and consequences have all evolved over the last 10 years. For example, critical infrastructure that has long been subject to risks associated with physical threats and natural disasters is now increasingly exposed to cyber risks, which stems from growing integration of information and communications technologies with critical infrastructure operations and an adversary focus on exploiting potential cyber vulnerabilities.

The Strategic National Risk Assessment (SNRA) defines numerous threats and hazards to homeland security in the broad categories of adversarial/human-caused, natural, and technological/ accidental threats. Critical assets, systems, and networks face many of the threats categorized by the SNRA, including terrorists and other actors seeking to cause harm and disrupt essential services through physical and cyber attacks, severe weather events, pandemic influenza or other health crises, and the potential for accidents and failures due to infrastructure operating beyond its intended lifespan. The potential for interconnected events with unknown consequences adds uncertainty in addition to the known risks analyzed as part of the SNRA.

Growing interdependencies across critical infrastructure systems, particularly reliance on information and communications technologies, have increased the potential vulnerabilities to physical and cyber threats and potential consequences

resulting from the compromise of underlying systems or networks. In an increasingly interconnected world, where critical infrastructure crosses national borders and global supply chains, the potential impacts increase with these interdependencies and the ability of a diverse set of threats to exploit them.

In addition, the effects of extreme weather pose a significant risk to critical infrastructure—rising sea levels, more severe storms, extreme and prolonged drought conditions, and severe flooding combine to threaten infrastructure that provides essential services to the American public. Ongoing and future changes to the climate have the potential to compound these risks and could have a major impact on infrastructure operations.

Finally, vulnerabilities also may exist as a result of a retiring work force or lack of skilled labor. Skilled operators are necessary for infrastructure maintenance and, therefore, security and resilience. These various factors influence the risk environment and, along with the policy and operating environments, create the backdrop against which decisions are made for critical infrastructure security and resilience.

. . .

Operating Environment

The extent to which infrastructure is interconnected shapes the environment for critical infrastructure security and resilience by necessitating collaboration in both planning and action. The Nation's critical infrastructure has become much more interdependent, continuing to move from an operating environment characterized by disparate assets, systems, and networks to one in which cloud computing, mobile devices, and wireless connectivity have dramatically changed the way infrastructure is operated. Interdependencies may be operational (e.g., power required to operate a water pumping station) or physical (e.g., colocated infrastructure, such as water and electric lines running under a bridge span). Interdependencies may be limited to small urban or rural areas or span vast regions, crossing jurisdictional and national boundaries, including infrastructure that require accurate and precise positioning, navigation, and timing (PNT) data. PNT services are critical to the operations of multiple critical infrastructure sectors and are vital to incident response.

The Nation has benefited from the investments made in increased security and resilience by both public and private sector owners and operators. Much of the critical infrastructure community continues to integrate cybersecurity into core business practices, making significant investments to increase security and resilience. In other areas, however, despite public and private sector expenditures to operate and maintain critical infrastructure systems, the level of investment has not been adequate, as evidenced by the deteriorating condition of many infrastructure systems. The National Academy of Sciences reported that the Nation's earlier heavy investment in the design, construction, and operation of critical infrastructure systems—water, wastewater, energy, transportation, and telecommunications—has not been matched with the funds necessary to keep these systems in good condition or to upgrade them to meet the demands of a growing and shifting population.

Critical infrastructure assets, systems, and networks, as well as other key resources, reside in particular jurisdictions, but their resulting information, products, services, and functions can be provided worldwide. The nature of critical infrastructure

ownership and operations is also distributed, and the need for joint planning and investment is becoming more common and necessary on the international level. These global connections inform the way that the critical infrastructure community should plan to work together, within and across sectors, and across jurisdictions and national borders, to increase the security and resilience of critical infrastructure. Information security and privacy considerations also shape the operating environment. The increasing availability of data and information essential to operating and maintaining infrastructure and related technologies enables more efficient and effective practices. This information is vulnerable to unauthorized access that could affect its confidentiality, integrity, or availability. The distribution of such information to those entities that can use it for efficient and effective risk management remains a challenge. It is critical to maintain the availability of information and distribute it to those who can use and protect it properly. This entails being transparent about information-sharing practices; protecting sources and methods; and ensuring privacy and protecting civil liberties, while also enabling law enforcement investigations.

This complex environment underscores the challenge in securing and strengthening the resilience of the Nation's critical infrastructure. Because of the dynamic nature of this environment, the ability to consistently partner to take advantage of unique skills and capabilities across the community remains the foundation for critical infrastructure security and resilience efforts.

. . .

Core Tenets

The *National Plan* establishes seven core tenets, representing the values and assumptions the critical infrastructure community should consider (at the national, regional, SLTT [State, Local, Tribal, and Territorial], and owner and operator levels) when planning for critical infrastructure security and resilience.

1. **Risk should be identified and managed in a coordinated and comprehensive way across the critical infrastructure community to enable the effective allocation of security and resilience resources.**
   Collaboratively managing risk requires sharing information (including smart practices), promoting more efficient and effective use of resources, and minimizing duplication of effort. It enables the development and execution of more comprehensive measures to secure against, disrupt, and prepare for threats; mitigate vulnerabilities; and reduce consequences across the Nation. To ensure a comprehensive approach to risk management, the critical infrastructure community considers strategies to achieve risk mitigation, as well as other ways to address risk, including acceptance, avoidance, or transference.
2. **Understanding and addressing risks from cross-sector dependencies and interdependencies is essential to enhancing critical infrastructure security and resilience.**
   The way infrastructure sectors interact, including through reliance on shared information and communications technologies (e.g., cloud services),

shapes how the Nation's critical infrastructure partners should collectively manage risk. For example, all critical infrastructure sectors rely on functions provided by energy, communications, transportation, and water systems, among others. In addition, interdependencies flow both ways, as with the dependence of energy and communications systems on each other and on other functions. It is important for the critical infrastructure community to understand and appropriately account for dependencies and interdependencies when managing risk.

3. **Gaining knowledge of infrastructure risk and interdependencies requires information sharing across the critical infrastructure community.**
   Through their operations and perspectives, stakeholders across the critical infrastructure community possess and produce diverse information useful to the enhancement of critical infrastructure security and resilience. Sharing and jointly planning based on this information is imperative to comprehensively address critical infrastructure security and resilience in an environment of increasing interconnectedness. For that to happen, appropriate legal protections, trusted relationships, enabling technologies, and consistent processes must be in place.
4. **The partnership approach to critical infrastructure security and resilience recognizes the unique perspectives and comparative advantages of the diverse critical infrastructure community.**
   The public-private partnership is central to maintaining critical infrastructure security and resilience. A well-functioning partnership depends on a set of attributes, including trust; a defined purpose for its activities; clearly articulated goals; measurable progress and outcomes to guide shared activities; leadership involvement; clear and frequent communication; and flexibility and adaptability. All levels of government and the private and nonprofit sectors bring unique expertise, capabilities, and core competencies to the national effort. Recognizing the value of different perspectives helps the partnership more distinctly understand challenges and solutions related to critical infrastructure security and resilience.
5. **Regional and SLTT partnerships are crucial to developing shared perspectives on gaps and actions to improve critical infrastructure security and resilience.**
   The *National Plan* emphasizes partnering across institutions and geographic boundaries to achieve security and resilience. Risks often have local consequences, making it essential to execute initiatives on a regional scale in a way that complements and operationalizes the national effort. This requires locally based public, private, and non-profit organizations to provide their perspectives in the assessment of risk and mitigation strategies. Local partnerships throughout the country augment the efforts of existing partnerships at the national level and are essential to a true national effort to strengthen security and resilience.
6. **Infrastructure critical to the United States transcends national boundaries, requiring cross-border collaboration, mutual assistance, and other cooperative agreements.**

The United States benefits from and depends upon a global network of infrastructure that enables the Nation's security and way of life. The distributed nature and interconnectedness of these assets, systems, and networks create a complex environment in which the risks the Nation faces are not distinctly contained within its borders. This is increasingly the case as services provided by critical infrastructure are often dependent on information gathered, stored, or processed in highly distributed locations. It is imperative that the government, private sector, and international partners work together. This includes collaborating to fully understand supply chain vulnerabilities and implement coordinated, and not competing, global security and resilience measures. The National Plan is focused on domestic efforts in critical infrastructure security and resilience, while recognizing the international aspects of the national approach.

7. **Security and resilience should be considered during the design of assets, systems, and networks.**
   As critical infrastructure is built and refreshed, those involved in making design decisions, including those related to control systems, should consider the most effective and efficient ways to identify, deter, detect, disrupt, and prepare for threats and hazards; mitigate vulnerabilities; and minimize consequences. This includes considering infrastructure resilience principles.

SOURCE: U.S. Department of Homeland Security, *National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: Government Printing Office, 2013), 8–10, 13–14, https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

ANALYSIS

Disasters are an unfortunate part of human existence. However, in the case of cyberattacks against critical infrastructure, potential disasters are entirely human made and are theoretically preventable. At the very least, their effects can be mitigated in ways that might not be possible for naturally occurring events. The rapid development of computer networks, and the tendency to place incredibly complex systems onto those networks without inherently considering the need for security against cyberattack, has made critical infrastructure assets significantly more vulnerable to attack. At the same time, this has enabled far more efficient processes and procedures, making the electrical grid more responsive to changing needs for power generation, or transportation hubs capable of moving far more people in an efficient manner. Naturally, critical infrastructure represents a key target for potential adversaries—such has always been true in warfare. However, cyberattacks have made it possible to create effects that previously would have required an enormous investment of physical resources, as well as undertaking the inherent risk associated with launching a military operation. In the twenty-first century, it is theoretically possible to obtain the same effects from the safety of one's own borders, and possibly masking responsibility for the attack (or even shifting blame for it to a different

adversary). Thus, the federal government created a plan that recognizes that some critical assets that benefit the nation as a whole require specific security efforts, and those efforts will be more efficient and effective if they are coordinated by a single entity.

- ***Document 43:*** *Presidential Policy Directive 21—Critical Infrastructure Security and Resilience*
- ***When:*** February 12, 2013
- ***Where:*** Washington, D.C.
- ***Significance:*** The concept of a "cyber Pearl Harbor" has been present in the public debate over cyberwarfare for more than a decade. Typically, the idea revolves around a devastating attack upon critical infrastructure, possibly involving a compromise of the nation's electrical grid. Multiple presidential administrations have tried to find solutions to the thorny problem of providing adequate security for critical infrastructure, with mixed results. In 2013, President Obama issued a policy directive attempting to emphasize the importance of planning for coordinated cyber defense.

DOCUMENT

Three Strategic Imperatives

1) Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience

An effective national effort to strengthen critical infrastructure security and resilience must be guided by a national plan that identifies roles and responsibilities and is informed by the expertise, experience, capabilities, and responsibilities of the SSAs [Sector-Specific Agencies], other Federal departments and agencies with critical infrastructure roles, SLTT entities, and critical infrastructure owners and operators.

During the past decade, new programs and initiatives have been established to address specific infrastructure issues, and priorities have shifted and expanded. As a result, Federal functions related to critical infrastructure security and resilience shall be clarified and refined to establish baseline capabilities that will reflect this evolution of knowledge, to define relevant Federal program functions, and to facilitate collaboration and information

exchange between and among the Federal Government, critical infrastructure owners and operators, and SLTT entities.

As part of this refined structure, there shall be two national critical infrastructure centers operated by DHS—one for physical infrastructure and another for cyber infrastructure. They shall function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure. Just as the physical and cyber elements of critical infrastructure are inextricably linked, so are the vulnerabilities. Accordingly, an integration and analysis function (further developed in Strategic Imperative 3) shall be implemented between these two national centers.

The success of these national centers, including the integration and analysis function, is dependent on the quality and timeliness of the information and intelligence they receive from the SSAs and other Federal departments and agencies, as well as from critical infrastructure owners and operators and SLTT entities.

These national centers shall not impede the ability of the heads of Federal departments and agencies to carry out or perform their responsibilities for national defense, criminal, counterintelligence, counterterrorism, or investigative activities.

2) Enable Efficient Information Exchange by Identifying Baseline Data and Systems Requirements for the Federal Government

A secure, functioning, and resilient critical infrastructure requires the efficient exchange of information, including intelligence, between all levels of governments and critical infrastructure owners and operators. This must facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents. The goal is to enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities should there be a disruption in the primary systems.

Greater information sharing within the government and with the private sector can and must be done while respecting privacy and civil liberties. Federal departments and agencies shall ensure that all existing privacy principles, policies, and procedures are implemented consistent with applicable law and policy and shall include senior agency officials for privacy in their efforts to govern and oversee information sharing properly.

3) Implement an Integration and Analysis Function to Inform Planning and Operational Decisions Regarding Critical Infrastructure

The third strategic imperative builds on the first two and calls for the implementation of an integration and analysis function for critical infrastructure that includes operational and strategic analysis on incidents, threats, and emerging risks. It shall reside at the intersection of the two national centers as identified in Strategic Imperative 1, and it shall include the capability

to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information to:

a. Aid in prioritizing assets and managing risks to critical infrastructure;
b. Anticipate interdependencies and cascading impacts;
c. Recommend security and resilience measures for critical infrastructure prior to, during, and after an event or incident; and
d. Support incident management and restoration efforts related to critical infrastructure.

This function shall not replicate the analysis function of the IC or the National Counterterrorism Center, nor shall it involve intelligence collection activities. The IC, DOD, DOJ, DHS, and other Federal departments and agencies with relevant intelligence or information shall, however, inform this integration and analysis capability regarding the Nation's critical infrastructure by providing relevant, timely, and appropriate information to the national centers. This function shall also use information and intelligence provided by other critical infrastructure partners, including SLTT and nongovernmental analytic entities.

Finally, this integration and analysis function shall support DHS's ability to maintain and share, as a common Federal service, a near real-time situational awareness capability for critical infrastructure that includes actionable information about imminent threats, significant trends, and awareness of incidents that may affect critical infrastructure.

SOURCE: Barack Obama, *Presidential Policy Directive 21—Critical Infrastructure Security and Resilience* (Washington, D.C., February 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

ANALYSIS

The Obama administration was particularly concerned with the possibility of a hostile nation choosing to plant malware into the computer networks of critical infrastructure within the United States, effectively lying in wait for a command that might trigger a cascade of failures at a key moment. Although no such attack has been carried out to date, there have been plenty of probing attempts to penetrate sensitive networks and possibly plant software. Thus, the Obama administration sought to clarify which federal agencies should take the lead in protecting the critical elements of the United States and its infrastructure. In particular, the Department of Homeland Security, an organization created in the aftermath of the September 11 attacks, was designated as the key federal organization tasked with protection of the critical infrastructure of the nation. However, being given responsibility to defend networks did not inherently carry with it the authority to take the kinds of actions necessary for such a defense, and this document served as a major step in the direction of enhanced defenses against cyberattack.

- ***Document 44:*** *Deterrence in the Age of Surprise*
- ***When:*** January 2014
- ***Where:*** Maxwell Air Force Base, AL
- ***Significance:*** Because most military installations located within the United States are tied to the existing infrastructure of the surrounding areas, these installations are subject to indirect effects of cyberattacks upon electrical grids, water treatment, and other potential targets. This paper, prepared by members of the Air Force Research Institute, illustrates the inherent challenges associated with modern military operations if a base relies upon local infrastructure for its daily operations.

DOCUMENT

Threats in the Age of Surprise

As a result of this increasing speed of interaction and data sharing, we have entered an "age of surprise." While it is possible to see the broad outlines of the future and to define the strategic planning space, this speed of change is making the specific details harder to see. Whether we call these details "turbulence" or a form of chaos in complex systems, we have entered a period of inevitable surprises. We can discern the outlines of some in advance. The key is to understand some of these potential surprises and know how to deal with the resultant challenges.

Cyberspace

Much of the critical infrastructure in the United States is dependent on cyberspace. To research exactly how vulnerable this infrastructure is, the Department of Energy created a National Critical Infrastructure Test Range as part of the Idaho National Laboratories. In 2007 a test of the robustness of our electrical grids against cyber attacks was first conducted on the lab's 860-square-mile test range. Dubbed "Aurora," the attack simulated a single cyber attacker tapping into a supervisory control and data acquisition (SCADA) system controlling an electrical power generator similar to those used in the power plants across the United States. The result of the attack was a loss of control of systems critical to generator operation, which caused the generator to be destroyed.

It is important to note that large electrical-generation components like the generator in the Aurora test are typically custom manufactured. Utility companies often have spare wire on hand, but spare generators are rare. The usual time to receive a new generator from the time the order is placed is around 18 months, assuming,

DID YOU KNOW?

Flame Worm

The Flame worm is an extremely sophisticated and dangerous form of malware that was almost certainly developed using the resources of a nation-state. It has also been called Da Flame, Flamer, and Skywiper, depending upon how it has been detected. Flame was first discovered in 2012 by a cyber-security cooperative led by Kaspersky Lab that was hired to investigate Iranian Oil Ministry computers. Although it was found throughout the Middle East, the majority of detections were within the Islamic Republic of Iran.

Flame can be spread through a computer network, or propagated via USB flash drives. It has an enormous number of capabilities, including recording audio, video, screenshots, keyboard activity, and network traffic. It can also copy data and utilize infected computers to attempt connections to nearby Bluetooth devices. Copied data is exfiltrated to one of several servers around the globe, where it can be downloaded, presumably by Flame's creators. Flame shares a substantial amount of code with Stuxnet, the targeted virus that attacked Iranian uranium-enrichment centers. In particular, Flame exploits many of the same operating system flaws as its predecessor. However, its increased capabilities came at a massive cost of data—Flame is twenty megabytes in size, making it forty times larger than Stuxnet. Although its creators remain a mystery, Flame contains many of the hallmarks of Western intelligence services, and almost certainly required the cyber resources of a nation-state.

of course, that the plant that manufactures them has electricity in the first place. In a large cyber attack, this assumption may be invalid.

This demonstration is disturbing on three grounds. First, it is not unique. Several instances of system malfunctions, arguably because of hacking into these types of systems, have already occurred and have caused damage to various infrastructures. Second, the US Air Force is heavily reliant on the national critical infrastructure, and if it were to incur a massive failure, it is highly likely the Air Force would be unable to carry out its principal core functions. Lastly, very little has been or is being done to mitigate this problem.

There have been several attacks on critical infrastructure worldwide, many of which predated the Idaho test by years. Among those known to be intentional attacks on SCADA systems for the purpose of causing damage is an attack on the Maroochy Shire's sewage treatment system in Queensland, Australia, in January 2000. During this attack, more than 264,000 gallons of sewage spilled over a period of several weeks, just after a new control system had been installed. Pumps were opening and closing without being commanded to do so. Only after months of investigation and 46 successful attacks was the source of the problem traced to a disgruntled employee who was trying to gain employment as the troubleshooter of misbehaving control systems. In March 1997, a teenager managed to hack into the Bell Atlantic Computer and shut down the air traffic control system in and around Worcester, Massachusetts. In addition, hacking attacks have disrupted natural gas pipelines in the former Soviet Union (1982) and Russia (2000). The 1982 event resulted in an explosion known as a "logic bomb." There are other events that were also likely deliberate, as recent speculation regarding the Stuxnet and Flame malware programs suggests. It is important to realize that SCADA systems offer a path into the internal logic of the critical infrastructure; in fact, attacking these systems is easy enough that even a single hacker can accomplish it.

The Air Force is dependent on these systems. If such outages are sporadic and/or localized, such inconveniences are easily overcome. If, however, the outage is part of a coordinated attack and if it affects the whole nation, then current planning is insufficient. A disabled national critical infrastructure affects not only electrical generation but also, over time, the systems that enable water transport, heating systems, sewage systems, and the financial and banking industries upon which modern economies depend. Distribution of foodstuffs, gasoline, and fresh water all require electricity at some stage, even if it is merely to distribute and pump the gasoline to power the trucks. Similarly, communications are electricity dependent. Without it,

cell towers and landlines cannot operate. While most Air Force bases have means to recall their members even if there are no communications, the study team could find no one who could articulate how the Air Force would conduct a deployment without the ability to communicate from one base to another.

The Air Force also depends on these systems to carry out missions other than deployment. Cyberspace is likely the future domain in which most intelligence, surveillance, and reconnaissance (ISR) will be conducted. The rapid increase in the number of cameras and pictures that are both geographically and chronologically referenced, combined with the current ability to fuse these images seamlessly together, will enable a new method of creating real-time, three-dimensional images of almost any major city on Earth. As most of these pictures are available on the internet, the ability to "play" these three-dimensional views back in time will enable the tracking of many activities of military significance back to their sources. In addition, cyberspace and the pictures that exist therein enable reconnaissance in ways impossible via either air or space. Office-space layouts, interior building configurations, and the locations of telephone junctions and circuit breaker boxes are all pieces of data that can be found in a picture on the internet. These are pieces of data that one will never see from a satellite image. As a result, ISR in cyberspace may become the principal means of obtaining intelligence data in the future, making the survival of the national critical infrastructure even more important.

Perhaps most disturbing is the lack of a sense of urgency in addressing the problem. While research protocols require anonymity, CSAT has interviewed senior executives in several utility companies across the southeastern United States regarding the protective measures they are taking to stop potential cyberspace attacks. To a person, we received the same answer— "nothing." When we queried these leaders (chief executive officers and chief operating officers) as to why they were not taking action to protect their systems, the answer was also unanimous. Protective action costs money, and such money would have to come from shareholders' dividends. In short the market incentives that currently exist are a powerful disincentive for leaders of the private companies to do anything to protect against the vulnerabilities that have long been known to exist. As a result, significant threats, not only of disruption but also of long-term destruction, exist and will likely remain for some time in cyberspace.

SOURCE: John P. Geis, II, Grant T. Hammond, Harry A. Foster, Theodore C. Hailes, *Deterrence in the Age of Surprise* (Maxwell Air Force Base, AL: Air University Press, 2014), 11–13, https://apps.dtic.mil/dtic/tr/fulltext/u2/a603951.pdf

ANALYSIS

By pointing out a vulnerability of military bases that cannot be inherently corrected by military action alone, the authors of this document draw attention to a critical problem for the United States—Air Force, in particular, but also the Department of Defense, in general. Perhaps most disturbing in this report is the argument that there seems to be little, if any, urgency to rectify the situation—something that the nation's adversaries have no doubt noticed and planned to exploit. If nothing

else, this piece demonstrates the far-reaching consequence of a cyberattack upon the electrical grid, and the myriad of ways that such an attack might disrupt military operations through an indirect, but no less effective, means. If a hostile state can disrupt, degrade, or destroy electrical generation or transmission to military bases, the functions of those bases will decline in proportion, and within a few days, likely come to a complete standstill. Replicating such an attack upon a large scale would likely create so much chaos that the U.S. military might be deterred from taking any positive action beyond attempts to restore its own functions, essentially ceding a free hand to the adversary to conduct kinetic operations elsewhere with little possibility of interference.

- ***Document 45:*** *U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage*
- ***When:*** May 19, 2014
- ***Where:*** Pittsburgh, PA
- ***Significance:*** Prosecutions of cyber malefactors are notoriously difficult due to the problems associated with attributing cyberattacks and the additional challenge of walking jurors through the technical aspects of a case. In 2014, the U.S. Department of Justice still chose to indict five individual members of the People's Liberation Army, who had allegedly launched massive cyber campaigns against U.S. networks.

DOCUMENT

U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage
First Time Criminal Charges Are Filed Against Known State Actors for Hacking

A grand jury in the Western District of Pennsylvania (WDPA) indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries.

The indictment alleges that the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive,

internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.

"This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor in this type of hacking," U.S. Attorney General Eric Holder said. "The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response. Success in the global marketplace should be based solely on a company's ability to innovate and compete, not on a sponsor government's ability to spy and steal business secrets. This Administration will not tolerate actions by any nation that seeks to illegally sabotage American companies and undermine the integrity of fair competition in the operation of the free market."

"For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries," said FBI Director James B. Comey. "The indictment announced today is an important step. But there are many more victims, and there is much more to be done. With our unique criminal and national security authorities, we will continue to use all legal tools at our disposal to counter cyber espionage from all sources."

"State actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country's flag," said John Carlin, Assistant Attorney General for National Security. "Cyber theft is real theft and we will hold state sponsored cyber thieves accountable as we would any other transnational criminal organization that steals our goods and breaks our laws."

"This 21st century burglary has to stop," said David Hickton U.S. Attorney for the Western District of Pennsylvania. "This prosecution vindicates hard working men and women in Western Pennsylvania and around the world who play by the rules and deserve a fair shot and a level playing field."

Summary of the Indictment

Defendants: Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui, who were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army (PLA). The indictment alleges that Wang, Sun, and Wen, among others known and unknown to the grand jury, hacked or attempted to hack into U.S. entities named in the indictment, while Huang and Gu supported their conspiracy by, among other things, managing infrastructure (e.g., domain accounts) used for hacking.

Victims: Westinghouse Electric Co. (Westinghouse), U.S. subsidiaries of SolarWorld AG (SolarWorld), United States Steel Corp. (U.S. Steel), Allegheny Technologies Inc. (ATI), the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (USW) and Alcoa Inc.

Time Period: 2006–2014.

Crimes: Thirty one counts as follows (all defendants are charged in all counts).

SOURCE: U.S. Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (Pittsburgh, PA, May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

ANALYSIS

The indictment demonstrates the level of seriousness of the case being presented by the Department of Justice. The attorney general and the FBI director both had a personal interest in this particular case and offered commentary for the press release associated with the indictment. Of course, given that the People's Republic of China has shown no willingness to extradite individuals to face a trial in the United States, it is almost certain that the indicted individuals will never see the inside of a courtroom in the United States. Nevertheless, the decision to prosecute, even in absentia, signals an escalation on the part of the part of the U.S. government. The Chinese government has not presented retaliatory indictments, which may indicate that similar levels of government-sponsored cyber espionage are not occurring from the United States, or it may simply signify that the Chinese government is unable to identify individuals associated with such activities. To date, none of the five indicted individuals have been extradited to the United States—and it would be an unprecedented action if the Chinese government reversed its stance on such procedures.

- ***Document 46:*** *Joint Publication 3-13: Information Operations*
- ***When:*** 2014
- ***Where:*** Washington, D.C.
- ***Significance:*** Joint doctrine is created to guide the decision-making of all the U.S. military services, particularly when the subject is one of mutual interest. Information operations include cyber operations, although they are not limited to the cyber domain. Comparing the broad category's doctrine with *Joint Publication 3-12: Cyberspace Operations* demonstrates the differences between the two concepts.

DOCUMENT

Introduction

a. The growth of communication networks has decreased the number of isolated populations in the world. The emergence of advanced wired and wireless information technology facilitates global communication by corporations, violent extremist organizations, and individuals. The ability to share information in near real time, anonymously and/or securely, is a capability that is both an asset and a potential vulnerability to us, our allies, and our adversaries. Information is a powerful tool to influence, disrupt, corrupt, or usurp an adversary's ability to make and share decisions.

b. The growth of communication networks has decreased the number of isolated populations in the world. The emergence of advanced wired and wireless

information technology facilitates global communication by corporations, violent extremist organizations, and individuals. The ability to share information in near real time, anonymously and/or securely, is a capability that is both an asset and a potential vulnerability to us, our allies, and our adversaries. Information is a powerful tool to influence, disrupt, corrupt, or usurp an adversary's ability to make and share decisions.

c. As the strategic environment continues to change, so does IO. Based on these changes, the Secretary of Defense now characterizes IO as the integrated employment, during military operations, of IRCs in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. This revised characterization has led to a reassessment of how essential the information environment can be and how IRCs can be effectively integrated into joint operations to create effects and operationally exploitable conditions necessary for achieving the joint force commander's (JFC's) objectives.

The Information Environment

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions which continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive (see Figure I-1). The JFC's operational environment is the composite of the conditions, circumstances, and influences that affect employment of capabilities and bear on the decisions of the commander (encompassing physical areas and factors of the air, land, maritime, and space domains) as well as the information environment (which includes cyberspace).

The Physical Dimension. The physical dimension is composed of command and control (C2) systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. It is the dimension where physical platforms and the communications networks that connect them reside. The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement. The physical dimension is not confined solely to military or even nation-based systems and processes; it is a defused network connected across national, economic, and geographical boundaries.

The Informational Dimension. The informational dimension encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information.

The Cognitive Dimension. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making. These elements are influenced by many factors, to include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences,

morals, education, mental health, identities, and ideologies. Defining these influencing factors in a given environment is critical for understanding how to best influence the mind of the decision maker and create the desired effects. As such, this dimension constitutes the most important component of the information environment.

. . .

Cyberspace Operations

(a) Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. CO are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace capabilities, when in support of IO, deny or manipulate adversary or potential adversary decision making, through targeting an information medium (such as a wireless access point in the physical dimension), the message itself (an encrypted message in the information dimension), or a cyber-persona (an online identity that facilitates communication, decision making, and the influencing of audiences in the cognitive dimension). When employed in support of IO, CO generally focus on the integration of offensive and defensive capabilities exercised in and through cyberspace, in concert with other IRCs, and coordination across multiple lines of operation and lines of effort.

(b) As a process that integrates the employment of IRCs across multiple lines of effort and lines of operation to affect an adversary or potential adversary decision maker, IO can target either the medium (a component within the physical dimension such as a microwave tower) or the message itself (e.g., an encrypted message in the informational dimension). CO is one of several IRCs available to the commander.

SOURCE: U.S. Department of Defense, *Joint Publication 3-13: Information Operations* (Washington, D.C.: Government Printing Office, 2014), I-1–I-3, II-9, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

ANALYSIS

As a subset of information operations, activities in the cyber domain are a key means of influencing the decision-making of adversaries and allies. However, there are other mechanisms that need to be utilized in concert with cyber operations in order to achieve the greatest effect. Likewise, while cybersecurity is important, the cyber domain is not the only vulnerability of military and civilian organizations and individuals regarding information operations. Cyber offers a tremendous capability to transfer enormous amounts of information and to reach a massive audience for a minimal investment—but other forms of information broadcast can also be utilized for both offensive and defensive operations, a key consideration for any military commander, regardless of service.

- ***Document 47:*** *Executive Order 13687—Imposing Additional Sanctions with Respect to North Korea*
- ***When:*** January 2, 2015
- ***Where:*** Washington, D.C.
- ***Significance:*** In November 2014, hackers operating from the Democratic People's Republic of Korea (North Korea) launched a massive attack against Sony Corporation, inflicting millions of dollars in damages in retaliation for the impending release of a film dubbed embarrassing to North Korea. Although several officials from the Obama administration had publicly proclaimed the right of the United States to retaliate for cyberattacks through the physical domain, the president chose instead to punish the North Korean transgression through economic sanctions.

DOCUMENT

I, BARACK OBAMA, President of the United States of America, find that the provocative, destabilizing, and repressive actions and policies of the Government of North Korea, including its destructive, coercive cyber-related actions during November and December 2014, actions in violation of UNSCRs 1718, 1874, 2087, and 2094, and commission of serious human rights abuses, constitute a continuing threat to the national security, foreign policy, and economy of the United States, and hereby expand the scope of the national emergency declared in Executive Order 13466 of June 26, 2008, expanded in scope in Executive Order 13551 of August 30, 2010, and relied upon for additional steps in Executive Order 13570 of April 18, 2011. To address this threat and to take further steps with respect to this national emergency, I hereby order:

Section 1. (a) All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in: any person determined by the Secretary of the Treasury, in consultation with the Secretary of State:

(i) to be an agency, instrumentality, or controlled entity of the Government of North Korea or the Workers' Party of Korea;
(ii) to be an official of the Government of North Korea;
(iii) to be an official of the Workers' Party of Korea;

(iv) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the Government of North Korea or any person whose property and interests in property are blocked pursuant to this order; or

(v) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, the Government of North Korea or any person whose property and interests in property are blocked pursuant to this order.

(b) The prohibitions in this order apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the effective date of this order.

Sec. 2. I hereby determine that the making of donations of the type of articles specified in section 203(b)(2) of IEEPA (50 U.S.C. 1702(b)(2)) by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to section 1 of this order would seriously impair my ability to deal with the national emergency declared in Executive Order 13466, and I hereby prohibit such donations as provided by section 1 of this order.

Sec. 3. The prohibitions in this order include but are not limited to:

(a) the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order; and

(b) the receipt of any contribution or provision of funds, goods, or services from any such person.

Sec. 4. I hereby find that the unrestricted immigrant and nonimmigrant entry into the United States of aliens determined to meet one or more of the criteria in section 1(a) of this order would be detrimental to the interests of the United States, and I hereby suspend entry into the United States, as immigrants or nonimmigrants, of such persons. Such persons shall be treated as persons covered by section 1 of Proclamation 8693 of July 24, 2011 (Suspension of Entry of Aliens Subject to United Nations Security Council Travel Bans and International Emergency Economic Powers Act Sanctions).

Sec. 5. (a) Any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order is prohibited.

(b) Any conspiracy formed to violate any of the prohibitions set forth in this order is prohibited.

Sec. 6. For the purposes of this order:

(a) the term "person" means an individual or entity;

(b) the term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization;

(c) the term "United States person" means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States; and

(d) the term "Government of North Korea" means the Government of the Democratic People's Republic of Korea and its agencies, instrumentalities, and controlled entities.

Sec. 7. For those persons whose property and interests in property are blocked pursuant to this order who might have a constitutional presence in the United States, I find that because of the ability to transfer funds or other assets instantaneously, prior notice to such persons of measures to be taken pursuant to this order would render those measures ineffectual. I therefore determine that for these measures to be effective in addressing the national emergency declared in Executive Order 13466, there need be no prior notice of a listing or determination made pursuant to section 1 of this order.

Sec. 8. The Secretary of the Treasury, in consultation with the Secretary of State, is hereby authorized to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by IEEPA, as may be necessary to carry out the purposes of this order. The Secretary of the Treasury may redelegate any of these functions to other officers and agencies of the United States Government consistent with applicable law. All agencies of the United States Government are hereby directed to take all appropriate measures within their authority to carry out the provisions of this order.

Sec. 9. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

SOURCE: Barack Obama, *Executive Order 13687—Imposing Additional Sanctions With Respect To North Korea*, January 2, 2015, https://www.govinfo.gov/content/pkg/FR-2015-01-06/pdf/2015-00058.pdf

ANALYSIS

This executive order likely had little practical effect, although it provided a substantial demonstration of the president's willingness to inflict a collective punishment upon the government of North Korea, its employees, and anyone associated with the ruling party. Because the order built upon tight sanctions from 2011, there were likely few new targets to be hit by the increased sanctions—but the order demonstrated the president's determination to hold the entire North Korean government and ruling party responsible for attacks that originated within the country. There is a long precedent for political and military action to punish physical attacks upon private corporations and citizens, and in that regard, the Obama administration was effectively serving notice that cyberattacks did not carry any form of immunity from response solely because they did not involve any physical damage. This reinforced previous messages regarding the willingness to retaliate for cyberattacks through any mechanism available to the government—and at the same time, it did not place any additional military forces into danger.

- ***Document 48:*** *Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing*
- ***When:*** February 13, 2015
- ***Where:*** Washington, D.C.
- ***Significance:*** In 2015, in the aftermath of devastating cyberattacks originating out of North Korea and targeting Sony Corporation, President Obama issued an executive order seeking to create a mechanism for private companies to share information regarding cyberattacks through the creation of a voluntary association of cyber entities within the United States.

DOCUMENT

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy.* In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

This order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive–21 (PPD–21) of February 12, 2013 (Critical Infrastructure Security and Resilience).

Policy coordination, guidance, dispute resolution, and periodic in-progress reviews for the functions and programs described and assigned herein shall be provided through the interagency process established in Presidential Policy Directive–l (PPD–l) of February 13, 2009 (Organization of the National Security Council System), or any successor.

Sec. 2. *Information Sharing and Analysis Organizations*. (a) The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs).

(b) ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors, or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities.

(c) The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002 (the "Act"), shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents, addressing such risks and incidents, and strengthening information security systems consistent with sections 212 and 226 of the Act.

(d) In promoting the formation of ISAOs, the Secretary shall consult with other Federal entities responsible for conducting cybersecurity activities, including Sector-Specific Agencies, independent regulatory agencies at their discretion, and national security and law enforcement agencies.

Sec. 3. *ISAO Standards Organization*. (a) The Secretary, in consultation with other Federal entities responsible for conducting cybersecurity and related activities, shall, through an open and competitive process, enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization (SO), which shall identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under this order. The standards shall further the goal of creating robust information sharing related to cybersecurity risks and incidents with ISAOs and among ISAOs to create deeper and broader networks of information sharing nationally, and to foster the development and adoption of automated mechanisms for the sharing of information. The standards will address the baseline capabilities that ISAOs under this order should possess and be able to demonstrate. These standards shall address, but not be limited to, contractual agreements, business processes, operating procedures, technical means, and privacy protections, such as minimization, for ISAO operation and ISAO member participation.

(b) To be selected, the SO must demonstrate the ability to engage and work across the broad community of organizations engaged in sharing information related to cybersecurity risks and incidents, including ISAOs, and associations and private companies engaged in information sharing in support of their customers.

(c) The agreement referenced in section 3(a) shall require that the SO engage in an open public review and comment process for the development of the standards referenced above, soliciting the viewpoints of existing entities engaged in sharing information related to cybersecurity risks and incidents, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders.

(d) The Secretary shall support the development of these standards and, in carrying out the requirements set forth in this section, shall consult with the Office of Management and Budget, the National Institute of Standards and Technology in the Department of Commerce, Department of Justice, the Information Security Oversight Office in the National Archives and Records Administration, the

Office of the Director of National Intelligence, Sector-Specific Agencies, and other interested Federal entities. All standards shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113), and OMB Circular A–119, as revised.

Sec. 4. *Critical Infrastructure Protection Program.* (a) Pursuant to sections 213 and 214(h) of the Critical Infrastructure Information Act of 2002, I hereby designate the NCCIC as a critical infrastructure protection program and delegate to it authority to enter into voluntary agreements with ISAOs in order to promote critical infrastructure security with respect to cybersecurity.

(b) Other Federal entities responsible for conducting cybersecurity and related activities to address threats to the public health and safety, national security, and economic security, consistent with the objectives of this order, may participate in activities under these agreements.

(c) The Secretary will determine the eligibility of ISAOs and their members for any necessary facility or personnel security clearances associated with voluntary agreements in accordance with Executive Order 13549 of August 18, 2010 (Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities), and Executive Order 12829 of January 6, 1993 (National Industrial Security Program), as amended, including as amended by this order.

SOURCE: Barack Obama, *Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing*, February 13, 2015, https://www.govinfo.gov/content/pkg/FR-2015-02-20/pdf/2015-03714.pdf

ANALYSIS

The idea of issuing an order as a means of creating voluntary participation in an information-sharing collective is an interesting approach for the president to select. Of course, ordering private companies to share their information with the Department of Homeland Security, particularly in the aftermath of revelations about massive data-collection programs undertaken by U.S. intelligence agencies, would undoubtedly provoke a massive backlash and a host of lawsuits. However, by making participation strictly voluntary, the order requires the Department of Homeland Security to demonstrate utility and value to the organizations that choose to participate—and until that demonstration is obvious, the voluntary organization is likely to attract little attention and interest from private companies, even those that have been hit by major cyberattacks.

- ***Document 49:*** *Cyberwarfare and Cyberterrorism: In Brief*
- ***When:*** March 27, 2015
- ***Where:*** Washington, D.C.

- ***Significance:*** The Congressional Research service (CRS) prepared this brief for members of the U.S. Congress to facilitate their understanding of how the cyber domain has been and is being used for attacks upon the United States. In addition, this document illustrates the relevant U.S. statutes pertaining to cyber activities, and by extension, it pushes the reader toward legislative issues that might arise in any discussion of cyberwarfare.

DOCUMENT

Cyberterrorism

As with cyberwarfare, there is no consensus definition of what constitutes cyberterrorism. The closest in law is found in the USA PATRIOT Act 18 U.S.C. 2332b's definition of "acts of terrorism transcending national boundaries" and reference to some activities and damage defined in the Computer Fraud and Abuse Act (CFA) 18 U.S.C. 1030a-c. A notable aspect of this act is its discussion of the "punishment for an offense" entails fines or imprisonment and suggests the offending party is undertaking a criminal act rather than an act of terrorism, which some argue is an act of war if undertaken by a state actor. The CFA is written in such a manner that it could be applied to an individual or groups.

18 U.S.C. 1030(a)(1) finds it illegal for an entity to "knowingly access a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation." As noted in this section, it appears this statute only pertains to U.S. government networks or networks that may contain restricted data. There is not yet a precedent for an unauthorized computer-supported intrusion rising to the level of being described as a cyberattack.

Some legal analyses define cyberterrorism as "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives."[1] The USA PATRIOT Act's definition of "federal crime of terrorism" and reference to the CFA seem to follow this definition. However, these provisions are also criminal statutes and generally refer to individuals or organizations rather than state actors. Naval Post Graduate School defense analyst Dorothy Denning's definition of cyber terrorism focuses on the distinction between destructive and disruptive action.[2] Terrorism

[1] https://www.nato.int/structur/library/bibref/cyberterrorism.pdf

[2] Dorothy E. Denning, "Activism, Hacktivisim, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," http://www.nautilus.org/info-policy/workshop/papers/denning.html

DID YOU KNOW?

Distributed Denial of Service Attack (DDoS)

A Distributed Denial of Service Attack (DDoS) is a common form of cyberattack against system or resource availability. A network DDoS seeks to overwhelm a target's communication bandwidth, essentially blocking all legitimate traffic by placing too much stress upon the target's communications capability. DDoS attacks can also seek to overwhelm memory buffers, router processing, and memory capacity. Many DDoS attacks are carried out by coordinating a large number of internet-connected computers to request information from the target in a continuous, simultaneous fashion. These are very unsophisticated cyberattacks, but can be extremely frustrating because they are so easily created and carried out. Slightly more sophisticated attackers rely upon source address spoofing, making it harder to filter out illicit traffic and allow legitimate requests to be processed. DDoS protection can be enabled through heuristics and efforts to determine which connections involve a human user in addition to the computer requesting information. Such connections are then prioritized over entirely automated ones, rendering the DDoS less effective.

generates fear comparable to that of physical attack, and is not just a "costly nuisance."[3] Though a DDoS attack itself does not yield this kind of fear or destruction, the problem is the potential for second or third order effects. For example, if telecommunications and emergency services had been completely dismantled in a time of crisis, the effects of that sort of infrastructure attack could potentially be catastrophic. If an attack on the emergency services system had coincided with a planned real-world, kinetic event, cyber terror or even a Cyber Pearl Harbor event may be an appropriate metaphor. However in this case, the emergency service system itself is most likely not a target, but rather the result of collateral damage to a vulnerable telecommunications network.

There are a number of reasons that may explain why the term "cyberterrorism" has not been statutorily defined, including the difficulty in identifying the parameters of what should be construed applicable activities, whether articulating clear redlines would demand a response for lower-level incidents, and retaining strategic maneuverability so as not to bind future U.S. activities in cyberspace.

Use of the Military: Offensive Cyberspace Operations

The War Powers Resolution, P.L. 93-148, 87 Stat. 555, sometimes referred to as the War Powers Act, sets the conditions under which the President may exercise his authority as Commander in Chief of U.S. military forces. First, the Resolution stipulates that it be exercised only pursuant to a declaration of war, specific statutory authorization from Congress, or a national emergency created by an attack upon the United States (50 U.S.C. 1541). Second, the Resolution requires the President to consult with Congress before introducing U.S. Armed Forces into hostilities or situations where hostilities are imminent, and to continue such consultations as long as U.S. Armed Forces remain in such situations (50 U.S.C. 1542). Third, it mandates reporting requirements that the President must comply with any time he introduces U.S. Armed Forces into existing or imminent hostilities (50 U.S.C. 1543). Lastly, 50 U.S.C. 1544(b) requires that U.S. forces be withdrawn from hostilities within 60 days of the time a report is submitted or is required to be submitted under 50 U.S.C. 1543(a)(1), unless Congress acts to approve continued military action, or is physically unable to meet as a result of an armed attack upon the United States.

Title 10 of the United States Code is the authority under which the military organizes, trains and equips its forces for national defense. Section 954 of the National Defense Authorization Act for Fiscal Year 2012 affirms that "the Department of Defense has the capability, and upon direction by the President may conduct offensive

[3] Serge Krasavin, "What is Cyber-terrorism?" http://www.crime-research.org/library/Cyber-terrorism.htm

operations in cyberspace to defend our Nation, Allies and interests, subject to the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict and the War Powers Resolution." The House version (H.R. 1540) contained a provision in Section 962 that would have clarified that the Secretary of Defense has the authority to conduct clandestine cyberspace activities in support of military operations pursuant to the Authorization for the Use of Military Force (P.L. 107-40; title 50 United States Code, section 1541 note) outside of the United States or to defend against a cyberattack on an asset of the Department of Defense. Section 941of the House version (H.R. 4310) of the National Defense Authorization Act for Fiscal Year 2013 would have again affirmed the Secretary of Defense's authority to conduct military activities in cyberspace. In particular, it would have clarified that the Secretary of Defense has the authority to conduct clandestine cyberspace activities in support of military operations pursuant to a congressionally authorized use of force outside of the United States, or to defend against a cyberattack on an asset of the DOD. This provision was not in the final version (P.L. 112-239), but a requirement for the Secretary of Defense to provide quarterly briefings to the House and Senate Armed Services Committee on all offensive and significant defensive military operations remained in Section 939.

Another relevant authority through which troops may be dispatched resides in Title 50 of the U.S. Code. Under Title 50, a "covert action" is subject to presidential finding and Intelligence Committee notification requirements. 50 U.S.C. 3093 allows the President to authorize the conduct of a covert action if he determines such an action is necessary to support identifiable foreign policy objectives of the United States and is important to the U.S. national security, which determination shall be set forth in a finding that shall be in writing, "unless immediate action by the United States is required and time does not permit the preparation of a written finding, in which case a written record of the President's decision shall be contemporaneously made and shall be reduced to a written finding as soon as possible but in no event more than 48 hours after the decision is made."

50 U.S.C. 413b(e) defines "covert action" as "activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly." The definition then lists certain exclusions. Traditional military activity, although undefined, is an explicit exception to the covert action definition in 50 U.S.C. 413 as the identity of the sponsor of a traditional military activity may be well known.

According to the Joint Explanatory Statement of the Committee of Conference, H.R. 1455, July 25, 1991, traditional military activities

> include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding and related to hostilities which are either anticipated (meaning approval has been given by the National Command Authorities for the activities and or operational planning for hostilities) to involve U.S. military forces, or where such hostilities

involving United States military forces are ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly.

Multiple press sources have reported on a Pentagon plan for "the creation of three types of Cyber Mission Forces under the Cyber Command: 'national mission forces' to protect computer systems that undergird electrical grids, power plants and other infrastructure deemed critical to national and economic security; 'combat mission forces' to help commanders abroad plan and execute attacks or other offensive operations; and 'cyber protection forces' to fortify the Defense Department's networks." These multiservice Cyber Mission Forces numbered under 1,000 in 2013, when DOD announced plans to expand them to roughly 5,000 soldiers and civilians. The target number has since grown to 6,200, with a deadline at the end of FY2016. In early September 2014, a report was provided to Congress from DOD that reportedly stated, "additional capability may be needed for both surge capacity for the [Cyber Mission Forces] and to provide unique and specialized capabilities" for a whole-of-government and nation approach to security in cyberspace.

SOURCE: Congressional Research Service, *Cyberwarfare and Cyberterrorism: In Brief* (Washington, D.C.: Congressional Research Service, 2015), 8–11, https://fas.org/sgp/crs/natsec/R43955.pdf

ANALYSIS

By illustrating the key legislative actions that pertain to cyberwarfare, the authors of this document manage to highlight for members of Congress how they can affect the conduct and capabilities of cyberwarfare. This brief for Congress does not offer opinions regarding the correct strategy that might be useful in cyberspace because the creation of such a strategy is largely within the purview of the executive branch and its departments rather than Congress. However, by demonstrating the relevant legal frameworks that bound cyber activities within the United States, it also becomes clear how the legislative branch can widen or contract the alternatives available to executive branch agencies that are active in cyberspace.

- ***Document 50:*** *Department of Defense Law of War Manual*
- ***When:*** 2015
- ***Where:*** Washington, D.C.
- ***Significance:*** It is absolutely essential for Western military forces to understand the overarching laws of war that govern state-controlled applications of violence. Periodically, the U.S. Department of Defense updates its *Law of War Manual* to reflect any substantive changes in the laws of armed conflict. In the past two decades,

many of the laws pertaining to cyber conflicts have gradually developed, making their updates in the *Manual* an important part of the decision to reissue it in revised form.

DOCUMENT

Introduction

This Chapter addresses the law of war and cyber operations. It addresses how law of war principles and rules apply to relatively novel cyber capabilities and the cyber domain.

As a matter of U.S. policy, the United States has sought to work internationally to clarify how existing international law and norms, including law of war principles, apply to cyber operations.

Precisely how the law of war applies to cyber operations is not well-settled, and aspects of the law in this area are likely to continue to develop, especially as new cyber capabilities are developed and States determine their views in response to such developments.

. . .

Application of the Law of War to Cyber Operations

Specific law of war rules may apply to cyber operations, even though those rules were developed before cyber operations were possible. When no more specific law of war rule or other applicable rule applies, law of war principles provide a general guide for conduct during cyber operations in armed conflict.

Application of Specific Law of War Rules to Cyber Operations. Specific law of war rules may be applicable to cyber operations, even though these rules were developed long before cyber operations were possible.

The law of war affirmatively anticipates technological innovation and contemplates that its existing rules will apply to such innovation, including cyber operations. Law of war rules may apply to new technologies because the rules often are not framed in terms of specific technological means. For example, the rules on conducting attacks do not depend on what type of weapon is used to conduct the attack. Thus, cyber operations may be subject to a variety of law of war rules depending on the rule and the nature of the cyber operation. For example, if the physical consequences of a cyber attack constitute the kind of physical damage that would be caused by dropping a bomb or firing a missile, that cyber attack would equally be subject to the same rules that apply to attacks using bombs or missiles.

Cyber operations may pose challenging legal questions because of the variety of effects they can produce. For example, cyber operations could be a non-forcible means or method of conducting hostilities (such as information gathering), and would be regulated as such under rules applicable to non-forcible means and methods of warfare. Other cyber operations could be used to create effects that amount to an attack and would be regulated under the rules on conducting attacks. Moreover,

another set of challenging issues may arise when considering whether a particular cyber operation might be regarded as a seizure or destruction of enemy property and should be assessed as such.

Application of Law of War Principles as a General Guide to Cyber Operations. When no specific rule applies, the principles of the law of war form the general guide for conduct during war, including conduct during cyber operations. For example, under the principle of humanity, suffering, injury, or destruction unnecessary to accomplish a legitimate military purpose must be avoided in cyber operations.

Certain cyber operations may not have a clear kinetic parallel in terms of their capabilities and the effects they create. Such operations may have implications that are quite different from those presented by attacks using traditional weapons, and those different implications may well yield different conclusions.

Cyber Operations and *Jus Ad Bellum*

Cyber operations may present issues under the law of war governing the resort to force (i.e., jus ad bellum).

Prohibition on Cyber Operations That Constitute Illegal Uses of Force Under Article 2(4) of the Charter of the United Nations. Article 2(4) of the Charter of the United Nations states that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

Cyber operations may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law. For example, if cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force under *jus ad bellum*, then such cyber operations would likely also be regarded as a use of force. Such operations may include cyber operations that: (1) trigger a nuclear plant meltdown; (2) open a dam above a populated area, causing destruction; or (3) disable air traffic control services, resulting in airplane crashes. Similarly, cyber operations that cripple a military's logistics systems, and thus its ability to conduct and sustain military operations, might also be considered a use of force under jus ad bellum. Other factors, besides the effects of the cyber operation, may also be relevant to whether the cyber operation constitutes a use of force under *jus ad bellum*.

Cyber operations that constitute uses of force within the meaning of Article 2(4) of the Charter of the United Nations and customary international law must have a proper legal basis in order not to violate *jus ad bellum* prohibitions on the resort to force.

Peacetime Intelligence and Counterintelligence Activities. International law and long-standing international norms are applicable to State behavior in cyberspace, and the question of the legality of peacetime intelligence and counterintelligence activities must be considered on a case-by-case basis. Generally, to the extent that cyber operations resemble traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information, then such cyber operations would likely be treated similarly under international law. The United States conducts such activities via cyberspace, and

such operations are governed by long-standing and well-established considerations, including the possibility that those operations could be interpreted as a hostile act.

Responding to Hostile or Malicious Cyber Operations. A State's inherent right of self-defense, recognized in Article 51 of the Charter of the United Nations, may be triggered by cyber operations that amount to an armed attack or imminent threat thereof. As a matter of national policy, the United States has expressed the view that when warranted, it will respond to hostile acts in cyberspace as it would to any other threat to the country.

Measures taken in the exercise of the right of national self-defense in response to an armed attack must be reported immediately to the U.N. Security Council in accordance with Article 51 of the Charter of the United Nations.

Use of Force Versus Armed Attack. The United States has long taken the position that the inherent right of self-defense potentially applies against any illegal use of force. Thus, any cyber operation that constitutes an illegal use of force against a State potentially gives rise to a right to take necessary and proportionate action in self-defense.

No Legal Requirement for a Cyber Response to a Cyber Attack. There is no legal requirement that the response in self-defense to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality.

Responses to Hostile or Malicious Cyber Acts That Do Not Constitute Uses of Force. Although cyber operations that do not constitute uses of force under jus ad bellum would not permit injured States to use force in self-defense, those injured States may be justified in taking necessary and appropriate actions in response that do not constitute a use of force. Such actions might include, for example, a diplomatic protest, an economic embargo, or other acts of retorsion.

Attribution and Self-Defense Against Cyber Operations. Attribution may pose a difficult factual question in responding to hostile or malicious cyber operations because adversaries may be able to hide or disguise their activities or identities in cyberspace more easily than in the case of other types of operations.

A State's right to take necessary and proportionate action in self-defense in response to an armed attack originating through cyberspace applies whether the attack is attributed to another State or to a non-State actor.

Authorities Under U.S. Law to Respond to Hostile Cyber Acts. Decisions about whether to invoke a State's inherent right of self-defense would be made at the national level because they involve the State's rights and responsibilities under international law. For example, in the United States, such decisions would generally be made by the President.

The Standing Rules of Engagement for U.S. forces have addressed the authority of the U.S. armed forces to take action in self-defense in response to hostile acts or hostile intent, including such acts perpetrated in or through cyberspace.

. . .

Cyber Operations and *Jus In Bello*

This section addresses *jus in bello* rules and cyber operations.

Cyber Operations That Constitute "Attacks" for the Purpose of Applying Rules on Conducting Attacks. If a cyber operation constitutes an attack, then the law

of war rules on conducting attacks must be applied to those cyber operations. For example, such operations must comport with the requirements of distinction and proportionality.

For example, a cyber attack that would destroy enemy computer systems could not be directed against ostensibly civilian infrastructure, such as computer systems belonging to stock exchanges, banking systems, and universities, unless those computer systems met the test for being a military objective under the circumstances. A cyber operation that would not constitute an attack, but would nonetheless seize or destroy enemy property, would have to be imperatively demanded by the necessities of war.

Assessing Incidental Injury or Damage During Cyber Operations. The proportionality rule prohibits attacks in which the expected loss of life or injury to civilians, and damage to civilian objects incidental to the attack, would be excessive in relation to the concrete and direct military advantage expected to be gained.

For example, in applying the proportionality rule to cyber operations, it might be important to assess the potential effects of a cyber attack on computers that are not military objectives, such as private, civilian computers that hold no military significance, but that may be networked to computers that are valid military objectives.

In assessing incidental injury or damage during cyber operations, it may be important to consider that remote harms and lesser forms of harm, such as mere inconveniences or temporary losses, need not be considered in applying the proportionality rule. For example, a minor, brief disruption of internet services to civilians that results incidentally from a cyber attack against a military objective generally would not need to be considered in a proportionality analysis. In addition, the economic harms in the belligerent State resulting from such disruptions, such as civilian businesses in the belligerent State being unable to conduct e-commerce, generally would not need to be considered in a proportionality analysis.

Even if cyber operations that constitute attacks are not expected to result in excessive incidental loss of life or injury or damage such that the operation would be prohibited by the proportionality rule, the party to the conflict nonetheless would be required to take feasible precautions to limit such loss of life or injury and damage in conducting those cyber operations.

Cyber Operations That Do Not Amount to an "Attack" Under the Law of War. A cyber operation that does not constitute an attack is not restricted by the rules that apply to attacks. Factors that would suggest that a cyber operation is not an "attack" include whether the operation causes only reversible effects or only temporary effects. Cyber operations that generally would not constitute attacks include:

- defacing a government webpage;
- a minor, brief disruption of internet services;
- briefly disrupting, disabling, or interfering with communications; and
- disseminating propaganda.

Since such operations generally would not be considered attacks under the law of war, they generally would not need to be directed at military objectives, and may be directed at civilians or civilian objects. Nonetheless, such operations must not be directed against enemy civilians or civilian objects unless the operations are

militarily necessary. Moreover, such operations should comport with the general principles of the law of war. For example, even if a cyber operation is not an "attack" or does not cause any injury or damage that would need to be considered under the proportionality rule, that cyber operation still should not be conducted in a way that unnecessarily causes inconvenience to civilians or neutral persons.

Duty to Take Feasible Precautions and Cyber Operations. Parties to a conflict must take feasible precautions to reduce the risk of incidental harm to the civilian population and other protected persons and objects. Parties to the conflict that employ cyber operations should take precautions to minimize the harm of their cyber activities on civilian infrastructure and users.

The obligation to take feasible precautions may be of greater relevance in cyber operations than other law of war rules because this obligation applies to a broader set of activities than those to which other law of war rules apply. For example, the obligation to take feasible precautions to reduce the risk of incidental harm would apply to a party conducting an attack even if the attack would not be prohibited by the proportionality rule. In addition, the obligation to take feasible precautions applies even if a party is not conducting an attack because the obligation also applies to a party that is subject to attack.

Cyber Tools as Potential Measures to Reduce the Risk of Harm to Civilians or Civilian Objects. In some cases, cyber operations that result in non-kinetic or reversible effects can offer options that help minimize unnecessary harm to civilians. In this regard, cyber capabilities may in some circumstances be preferable, as a matter of policy, to kinetic weapons because their effects may be reversible, and they may hold the potential to accomplish military goals without any destructive kinetic effect at all.

As with other precautions, the decision of which weapon to use will be subject to many practical considerations, including effectiveness, cost, and "fragility," *i.e.*, the possibility that once used an adversary may be able to devise defenses that will render a cyber tool ineffective in the future. Thus, as with special kinetic weapons, such as precision-guided munitions that have the potential to produce less incidental damage than other kinetic weapons, cyber capabilities usually will not be the only type of weapon that is legally permitted.

. . .

Legal Review of Weapons that Employ Cyber Capabilities

DoD policy requires the legal review of the acquisition of weapons or weapon systems. This policy would include the review of weapons that employ cyber capabilities to ensure that they are not *per se* prohibited by the law of war. Not all cyber capabilities, however, constitute a weapon or weapons system. Military Department regulations address what cyber capabilities require legal review.

The law of war does not prohibit the development of novel cyber weapons. The customary law of war prohibitions on specific types of weapons result from State practice and *opinio juris* demonstrating that a type of weapon is illegal; the mere fact that a weapon is novel or employs new technology does not mean that the weapon is illegal.

Although which issues may warrant legal analysis would depend on the characteristics of the weapon being assessed, a legal review of the acquisition or procurement

of a weapon that employs cyber capabilities likely would assess whether the weapon is inherently indiscriminate. For example, a destructive computer virus that was programmed to spread and destroy uncontrollably within civilian internet systems would be prohibited as an inherently indiscriminate weapon.

SOURCE: U.S. Department of Defense, *Department of Defense Law of War Manual* (Washington, D.C.: Government Printing Office, 2015), 985–999, https://dod.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf

ANALYSIS

Adapting the laws of war to new innovations can be a significant challenge, depending upon how those innovations manifest in periods of conflict. However, the overarching principles of self-defense, prohibitions upon unprovoked aggression, and the expectation that nations will resolve their grievances without resorting to force apply just as well to cyber conflicts as to those carried out exclusively in the physical domain. Likewise, in a period of war, the guiding principles of military necessity, discrimination, and proportionality apply to cyberattacks. Nations are expected to control the applications of force that they authorize and to remain in command of the personnel tasked with carrying them out, whether they are physical or nonkinetic in nature.

One of the fundamental questions that pertains to cyber warfare is whether it is possible to define a cyberattack as a use of force. While a handful of controlled experiments have demonstrated a limited ability to inflict physical damage through cyberattacks, to date, no cyberattack has caused physical harm to a human, much less killed a person. Thus, it is difficult to make a definitive case that a cyberattack, without accompanying physical action, can constitute an act of war and hence allow the victim to invoke the right of self-defense.

- ***Document 51:*** *Presidential Policy Directive 41: United States Cyber Incident Coordination*
- ***When:*** July 26, 2016
- ***Where:*** Washington, D.C.
- ***Significance:*** Presidential Policy Directives are somewhat akin to Executive Orders, although they are often for much smaller and more manageable issues. When a president issues such a directive, he or she is effectively ordering one or more federal agencies how to respond to a specific problem or stimulus. In this case, a number of private companies in the United States had been subjected to

large-scale cyberattacks, and President Obama wished to clarify precisely what role federal agencies should play in the event of such attacks.

DOCUMENT

July 26, 2016
PRESIDENTIAL POLICY DIRECTIVE/PPD-41
SUBJECT: United States Cyber Incident Coordination

The advent of networked technology has spurred innovation, cultivated knowledge, encouraged free expression, and increased the Nation's economic prosperity. However, the same infrastructure that enables these benefits is vulnerable to malicious activity, malfunction, human error, and acts of nature, placing the Nation and its people at risk. Cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure located in the United States and abroad.

United States preparedness efforts have positioned the Nation to manage a broad range of threats and hazards effectively. Every day, Federal law enforcement and those agencies responsible for network defense in the United States manage, respond to, and investigate cyber incidents in order to ensure the security of our information and communications infrastructure. The private sector and government agencies have a shared vital interest in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences. The nature of cyberspace requires individuals, organizations, and the government to all play roles in incident response. Furthermore, effective incident response efforts will help support an open, interoperable, secure, and reliable information and communications infrastructure that promotes trade and commerce, strengthens international security, fosters free expression, and reinforces the privacy and security of our citizens.

While the vast majority of cyber incidents can be handled through existing policies, certain cyber incidents that have significant impacts on an entity, our national security, or the broader economy require a unique approach to response efforts. These significant cyber incidents demand unity of effort within the Federal Government and especially close coordination between the public and private sectors.

. . .

Principles Guiding Incident Response

In carrying out incident response activities for any cyber incident, the Federal Government will be guided by the following principles:

A. Shared Responsibility. Individuals, the private sector, and government agencies have a shared vital interest and complementary roles and responsibilities in protecting the Nation from malicious cyber activity and managing cyber incidents and their consequences.

B. Risk-Based Response. The Federal Government will determine its response actions and the resources it brings to bear based on an assessment of the risks posed to an entity, our national security, foreign relations, the broader economy, public confidence, civil liberties, or the public health and safety of the American people.

C. Respecting affected entities. To the extent permitted under law, Federal Government responders will safeguard details of the incident, as well as privacy and civil liberties, and sensitive private sector information, and generally will defer to affected entities in notifying other affected private sector entities and the public. In the event a significant Federal Government interest is served by issuing a public statement concerning an incident, Federal responders will coordinate their approach with the affected entities to the extent possible.

D. Unity of Governmental Effort. Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be brought to bear on cyber incidents. These efforts must be coordinated to achieve optimal results. Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident. State, local, tribal, and territorial (SLTT) governments also have responsibilities, authorities, capabilities, and resources that can be used to respond to a cyber incident; therefore, the Federal Government must be prepared to partner with SLTT governments in its cyber incident response efforts. The transnational nature of the internet and communications infrastructure requires the United States to coordinate with international partners, as appropriate, in managing cyber incidents.

E. Enabling Restoration and Recovery. Federal response activities will be conducted in a manner to facilitate restoration and recovery of an entity that has experienced a cyber incident, balancing investigative and national security requirements, public health and safety, and the need to return to normal operations as quickly as possible.

Concurrent Lines of Effort

In responding to any cyber incident, Federal agencies shall undertake three concurrent lines of effort: threat response; asset response; and intelligence support and related activities. In addition, when a Federal agency is an affected entity, it shall undertake a fourth concurrent line of effort to manage the effects of the cyber incident on its operations, customers, and workforce.

A. Threat response activities include conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.

B. Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region,

including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.

Threat and asset responders will share some responsibilities and activities, which may include communicating with affected entities to understand the nature of the cyber incident; providing guidance to affected entities on available Federal resources and capabilities; promptly disseminating through appropriate channels intelligence and information learned in the course of the response; and facilitating information sharing and operational coordination with other Federal Government entities.

C. Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.

D. An affected Federal agency shall engage in a variety of efforts to manage the impact of a cyber incident, which may include maintaining business or operational continuity; addressing adverse financial impacts; protection of privacy; managing liability risks; complying with legal and regulatory requirements (including disclosure and notification); engaging in communications with employees or other affected individuals; and dealing with external affairs (e.g., media and congressional inquiries). The affected Federal agency will have primary responsibility for this line of effort.

When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but it will remain cognizant of the affected entity's response activities, consistent with the principles above and in coordination with the affected entity. The relevant sector-specific agency (SSA) will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

SOURCE: Barack Obama, Presidential Policy Directive 41, *United States Cyber Incident Coordination* (Washington, D.C., 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

ANALYSIS

Cybersecurity typically requires a certain degree of collective action—when one entity detects a potential vulnerability, for example, the norm is to publicize that vulnerability to other organizations that might be affected. Thus, when a new form of computer virus is detected by an antivirus company, that company is likely to notify other antivirus companies, rather than keeping the information to itself, because all the companies benefit by sharing such information and protecting their consumers in the process. Likewise, if one federal agency is affected by a cyberattack, other agencies need to be aware of what was done and how it was accomplished, if only to protect themselves from follow-on attacks. Coordinating cyber responses at the national level absolutely requires federal involvement, although there is no

compelling reason for the federal government to assume the responsibility for protecting every aspect of the internet or its users. In this directive, President Obama clarified the overarching rules of engagement for federal organizations, and how they might interact with one another and private users.

- ***Document 52:*** *Executive Order 13800—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*
- ***When:*** May 11, 2017
- ***Where:*** Washington, D.C.
- ***Significance:*** Federal agencies are notoriously slow to adopt new information technology, in part due to constrained resources and a byzantine contracting system as well as due to simple inertia. Given the rapid pace of technological advances, it is extremely difficult for a large system such as the federal government to keep up with the changes. Further, the attraction of private employment in the technology sector makes it even harder for the government to attract skilled professionals to oversee the continual upgrades of technology required. In this executive order, President Trump sought to force the issue of improving cybersecurity by threatening to hold the heads of federal agencies responsible for the cybersecurity of their organizations.

DOCUMENT

Section 1. Cybersecurity of Federal Networks.

(a) Policy.

The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) Findings.

(i) Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and

other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents. Information sharing facilitates and supports all of these activities.

(ii) The executive branch has for too long accepted antiquated and difficult–to-defend IT.

(iii) Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity.

(iv) Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies (agencies). Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance.

(v) Effective risk management requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources.

DID YOU KNOW?

Botnets

Botnets are groups of internet-connected computers that have been compromised, willingly or illicitly, to follow the commands of an external user. Normally, botnets are composed of a disparate group of machines whose owners are unaware of the compromise, and the fact that their computers are being used for malicious purposes. Botnets are often the core component of distributed denial of service (DDoS) attacks, as they can all be directed to send digital inquiries to targeted websites, routers, or networks, overwhelming the target's ability to respond and triggering a shutdown. Although most botnets are relatively small, consisting of a few dozen compromised computers, massive botnets of up to one million computers have been detected. Their controllers, called "botmasters," have been known to sell the services of the botnet to anyone willing to pay for its utilization. Occasionally, botnets comprise computers voluntarily contributed to a cause. Examples include the Israeli Patriot botnet, whose controllers used their network to attack anti-Israeli websites. The Russian-backed GeorBot launched attacks against the Republic of Georgia, and included thousands of computers owned by Russian expatriates who downloaded software to knowingly infect their systems and be part of the Russia-Georgia dispute.

(c) Risk Management.

(i) Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. They will also be held accountable by the President for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code.

(ii) Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk. Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and

Budget (OMB) within 90 days of the date of this order. The risk management report shall:

(A) document the risk mitigation and acceptance choices made by each agency head as of the date of this order, including:
(1) the strategic, operational, and budgetary considerations that informed those choices; and
(2) any accepted risk, including from unmitigated vulnerabilities; and
(B) describe the agency's action plan to implement the Framework.

(iii) The Secretary of Homeland Security and the Director of OMB, consistent with chapter 35, subchapter II of title 44, United States Code, shall jointly assess each agency's risk management report to determine whether the risk mitigation and acceptance choices set forth in the reports are appropriate and sufficient to manage the cybersecurity risk to the executive branch enterprise in the aggregate (the determination).

(iv) The Director of OMB, in coordination with the Secretary of Homeland Security, with appropriate support from the Secretary of Commerce and the Administrator of General Services, and within 60 days of receipt of the agency risk management reports outlined in subsection (c)(ii) of this section, shall submit to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the following:

(A) the determination; and
(B) a plan to:
(1) adequately protect the executive branch enterprise, should the determination identify insufficiencies;
(2) address immediate unmet budgetary needs necessary to manage risk to the executive branch enterprise;
(3) establish a regular process for reassessing and, if appropriate, reissuing the determination, and addressing future, recurring unmet budgetary needs necessary to manage risk to the executive branch enterprise;
(4) clarify, reconcile, and reissue, as necessary and to the extent permitted by law, all policies, standards, and guidelines issued by any agency in furtherance of chapter 35, subchapter II of title 44, United States Code, and, as necessary and to the extent permitted by law, issue policies, standards, and guidelines in furtherance of this order; and
(5) align these policies, standards, and guidelines with the Framework.

(v) The agency risk management reports described in subsection (c)(ii) of this section and the determination and plan described in subsections (c)(iii) and (iv) of this section may be classified in full or in part, as appropriate.

(vi) Effective immediately, it is the policy of the executive branch to build and maintain a modern, secure, and more resilient executive branch IT architecture.

(A) Agency heads shall show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.
(B) The Director of the American Technology Council shall coordinate a report to the President from the Secretary of Homeland Security, the Director of OMB, and the Administrator of General Services, in consultation with the Secretary of Commerce, as appropriate, regarding modernization of Federal IT. The report shall:
(1) be completed within 90 days of the date of this order; and
(2) describe the legal, policy, and budgetary considerations relevant to — as well as the technical feasibility and cost effectiveness, including timelines and milestones, of — transitioning all agencies, or a subset of agencies, to:
(aa) one or more consolidated network architectures; and
(bb) shared IT services, including email, cloud, and cybersecurity services.
(C) The report described in subsection (c)(vi)(B) of this section shall assess the effects of transitioning all agencies, or a subset of agencies, to shared IT services with respect to cybersecurity, including by making recommendations to ensure consistency with section 227 of the Homeland Security Act (6 U.S.C. 148) and compliance with policies and practices issued in accordance with section 3553 of title 44, United States Code. All agency heads shall supply such information concerning their current IT architectures and plans as is necessary to complete this report on time.

> (vii) For any National Security System, as defined in section 3552(b)(6) of title 44, United States Code, the Secretary of Defense and the Director of National Intelligence, rather than the Secretary of Homeland Security and the Director of OMB, shall implement this order to the maximum extent feasible and appropriate. The Secretary of Defense and the Director of National Intelligence shall provide a report to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism describing their implementation of subsection (c) of this section within 150 days of the date of this order. The report described in this subsection shall include a justification for any deviation from the requirements of subsection (c), and may be classified in full or in part, as appropriate.

Sec. 2. Cybersecurity of Critical Infrastructure.
(a) Policy. It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure (as defined in section 5195c(e) of title 42, United States Code) (critical infrastructure entities), as appropriate.
(b) Support to Critical Infrastructure at Greatest Risk. The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate sector-specific agencies, as defined in Presidential

Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience) (sector-specific agencies), and all other appropriate agency heads, as identified by the Secretary of Homeland Security, shall:

> (i) identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities);
> (ii) engage section 9 entities and solicit input as appropriate to evaluate whether and how the authorities and capabilities identified pursuant to subsection (b)(i) of this section might be employed to support cybersecurity risk management efforts and any obstacles to doing so;
> (iii) provide a report to the President, which may be classified in full or in part, as appropriate, through the Assistant to the President for Homeland Security and Counterterrorism, within 180 days of the date of this order, that includes the following:

(A) the authorities and capabilities identified pursuant to subsection (b)(i) of this section;
(B) the results of the engagement and determination required pursuant to subsection (b)(ii) of this section; and
(C) findings and recommendations for better supporting the cybersecurity risk management efforts of section 9 entities; and

> (iv) provide an updated report to the President on an annual basis thereafter.

(c) Supporting Transparency in the Marketplace. The Secretary of Homeland Security, in coordination with the Secretary of Commerce, shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, that examines the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities, with a focus on publicly traded critical infrastructure entities, within 90 days of the date of this order.
(d) Resilience Against Botnets and Other Automated, Distributed Threats. The Secretary of Commerce and the Secretary of Homeland Security shall jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets). The Secretary of Commerce and the Secretary of Homeland Security shall consult with the Secretary of Defense, the Attorney General, the Director of the Federal Bureau of Investigation, the heads of sector-specific agencies, the Chairs of the Federal Communications Commission and Federal Trade Commission, other interested agency heads, and appropriate stakeholders in carrying out this subsection. Within

240 days of the date of this order, the Secretary of Commerce and the Secretary of Homeland Security shall make publicly available a preliminary report on this effort. Within 1 year of the date of this order, the Secretaries shall submit a final version of this report to the President.

(e) Assessment of Electricity Disruption Incident Response Capabilities. The Secretary of Energy and the Secretary of Homeland Security, in consultation with the Director of National Intelligence, with State, local, tribal, and territorial governments, and with others as appropriate, shall jointly assess:

> (i) the potential scope and duration of a prolonged power outage associated with a significant cyber incident, as defined in Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination), against the United States electric subsector;
> (ii) the readiness of the United States to manage the consequences of such an incident; and
> (iii) any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident.

The assessment shall be provided to the President, through the Assistant to the President for Homeland Security and Counterterrorism, within 90 days of the date of this order, and may be classified in full or in part, as appropriate.

(f) Department of Defense Warfighting Capabilities and Industrial Base. Within 90 days of the date of this order, the Secretary of Defense, the Secretary of Homeland Security, and the Director of the Federal Bureau of Investigation, in coordination with the Director of National Intelligence, shall provide a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks. The report may be classified in full or in part, as appropriate.

Sec. 3. Cybersecurity for the Nation.

(a) Policy. To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.

(b) Deterrence and Protection. Within 90 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, and the United States Trade Representative, in coordination with the Director of National Intelligence, shall jointly submit a report to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, on the Nation's strategic options for deterring adversaries and better protecting the American people from cyber threats.

(c) International Cooperation. As a highly connected nation, the United States is especially dependent on a globally secure and resilient internet and must work with allies and other partners toward maintaining the policy set forth in this section. Within 45 days of the date of this order, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Secretary of Commerce, and the Secretary of Homeland Security, in coordination with the Attorney General and the Director of the Federal Bureau of Investigation, shall submit reports to the President on their international cybersecurity priorities, including those concerning investigation, attribution, cyber threat information sharing, response, capacity building, and cooperation. Within 90 days of the submission of the reports, and in coordination with the agency heads listed in this subsection, and any other agency heads as appropriate, the Secretary of State shall provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, documenting an engagement strategy for international cooperation in cybersecurity.
(d) Workforce Development. In order to ensure that the United States maintains a long-term cybersecurity advantage:

> (i) The Secretary of Commerce and the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the Office of Personnel Management, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security, shall:

(A) jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and
(B) within 120 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.

> (ii) The Director of National Intelligence, in consultation with the heads of other agencies identified by the Director of National Intelligence, shall:

(A) review the workforce development efforts of potential foreign cyber peers in order to help identify foreign workforce development practices likely to affect long-term United States cybersecurity competitiveness; and
(B) within 60 days of the date of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism on the findings of the review carried out pursuant to subsection (d)(ii)(A) of this section.

> (iii) The Secretary of Defense, in coordination with the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence, shall:

(A) assess the scope and sufficiency of United States efforts to ensure that the United States maintains or increases its advantage in national-security-related cyber capabilities; and
(B) within 150 days of the date of this order, provide a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations on the assessment carried out pursuant to subsection (d)(iii)(A) of this section.

(iv) The reports described in this subsection may be classified in full or in part, as appropriate.

SOURCE: Donald Trump, *Executive Order 13800—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

ANALYSIS

President Trump seems, through the text of this order, to believe that federal agencies had deliberately mishandled their cyber defenses. By giving the issue personal attention and setting specific deadlines for the delivery of reports regarding the status quo and planned upgrades, this order probably stimulated a substantial response from most agencies susceptible to cyberattack. Perhaps most interesting in the order is the requirement that agencies pursue shared capabilities, to include reliance upon cloud applications, as much as possible. Unless the federal government devises its own cloud storage system, this would offload much of the federal computer security problem to one or more private corporations—but it also provides a central repository for which cyber defenses can be more effectively developed. While the key reports prepared in response to this order remain classified, the mere fact that they were created meant that individual agencies had to confront their own failures regarding cybersecurity and develop coherent plans to fix the problems discovered in the process.

- ***Document 53:*** *Information Warfare: Issues for Congress*
- ***When:*** March 5, 2018
- ***Where:*** Washington, D.C.
- ***Significance:*** This document serves as an effective orientation for members of Congress regarding the major adversarial relationships that the United States faces in cyberspace. By providing summaries of major antagonists such as Russia, China, North Korea, Iran, and the Islamic State, this piece also frames cyber conflicts in the same

terms as the existing national strategy documents of the same time period. The Trump administration placed substantial emphasis upon a return to great power rivalries, rather than a focus upon small wars, and the cyber domain proved to be no exception to that rule.

DOCUMENT

Nation States and Terrorist Organizations

Both nation states and terrorist organizations pursue information warfare to achieve strategic objectives. The following examples highlight the ways in which their IW strategies may already be in effect. These threats are prioritized in the recent National Defense Strategy, which refers specifically to information warfare as a means through which "competitors and adversaries seek to optimize their targeting of our battle networks and operational concepts, while also using other areas of competition short of open warfare to achieve their ends."

Russia

Russia is engaging in activities that it describes in doctrine as information warfare. A 2011 Russian strategy document, the Convention on International Information Security, defines IW as "a conflict between two or more States in the information space with the goal of inflicting damage to information systems as well as carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents."[1] An "information weapon" is information technology, means, and methods intended for use in information warfare. Russian doctrine typically refers to a holistic concept of "information war," which is used to accomplish two primary aims:

- to achieve political objectives without the use of military force, and
- to shape a favorable international response to the deployment of its military forces, or military forces with which Moscow is allied.

To accomplish these goals, Russia appears to be using social media tools to spread a mix of propaganda, misinformation, and deliberately misleading or corrupted disinformation. Tactics also include data breaches of servers of U.S. political parties and other groups, releases and possible manipulation of sensitive documents in an attempt to influence the U.S. presidential election, and the manipulation of publicly available information on Russian activities in Ukraine.

On January 6, 2017, the Office of the Director of National Intelligence (ODNI) released a declassified report on Russian activities and intentions related to the 2016

[1] http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666.

U.S. presidential election. The report states that the Central Intelligence Agency, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) have "high confidence" that Russian President Vladimir Putin "ordered an influence campaign in 2016 aimed at the US presidential election" in order to "undermine public faith in the US democratic process, denigrate Clinton, and harm her electability and potential presidency." While much of the reporting refers to the cyber element of Russian activities, the series of network intrusions, reconnaissance, and data releases appear to be tactical weapons used in support of a broader information warfare campaign around the U.S. presidential election.

Data exfiltration from the networks belonging to both political parties could offer the Russian government insight into the negotiating strategies, redlines, foreign policy goals, and platforms of an incoming administration, whatever the election outcome. Cyber tools were also used to create psychological effects in the American population. The likely collateral effects of these activities include compromising the fidelity of information, sowing discord and doubt in the American public about the validity of intelligence community reports, and prompting questions about the legitimacy of the democratic process itself.

In February 2018, Special Counsel Robert Mueller indicted 13 Russian nationals for their involvement in the U.S. election. These individuals were said to have worked for the Internet Research Agency (IRA), a Russia-based organization that focused most of its efforts toward the United States. The indictment alleges that the IRA sought to conduct what it called "information warfare" on the U.S. population through "fictitious U.S. personas on social media platforms and other Internet-based media." The indictment alleges that U.S. citizens unknowingly counseled these Russian operatives as to how to focus their activities.

The operatives also reportedly used social media to widen social divides, exploiting existing fractures in American society. Over 3,000 Russian-bought Facebook ads heightened tensions and fomented discord among racial, religious, and political groups, by targeting messages to users based on their demographics and political preferences.

Some analysts contend that given the success of past efforts and the absence of retaliatory action, Russia will continue to pursue its election-related information warfare. As Director of National Intelligence Dan Coats said in February, 2018, "there should be no doubt" that Russia sees the 2018 U.S. midterm congressional elections as a target. "We expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokesmen and other means to influence, to try to build on its wide range of operations and exacerbate social and political fissures in the United States."

The nature of these activities, particularly tampering with a sovereign nation's internal democratic processes and systems, has raised questions as to whether they constitute an act of war or espionage. While some Russian doctrine suggests that these subversive activities are a way to "prepare the battlefield" in advance of a conflict, it may also be the conflict itself: information warfare is a way to weaken a militarily superior adversary without firing a single bullet.

Other activities conducted outside of cyberspace include production of pro-Russia television shows and broadcasts in Russian speaking areas of NATO, deploying

soldiers in Ukraine for propaganda purposes, and the use of "little green men," armed soldiers without insignia, allowing plausible deniability of a military incursion in Crimea while creating fear and intimidation among the local population.

China

The Chinese strategy of information warfare focuses on the use of what China calls "strategems" to build and maintain information superiority. These strategems help China compensate for its deficiencies in technology-based weapons, and may contain efforts to create cognitive errors and to influence the contents, process, and direction of thinking of an adversary. Cyberspace operations are used to achieve information dominance through reconnaissance and espionage, conducting network intrusions to steal and possibly alter data.

The Chinese concept of "Unrestricted Warfare" combines elements of information operations, cyberspace operations, irregular warfare, lawfare, and foreign relations, carried out in peacetime, as well as in conflict. The United States is viewed as a militarily superior foe whose advantages can be overcome through strategy and information operations. The U.S. reliance on technology, both in the military and in the civilian population, creates a vulnerability that can be exploited, along with "theoretical blind spots" and "thought errors," such as the absence of a comprehensive theory in DOD doctrine that combines all elements of information warfare.

In cyberspace, computer network espionage plays a large role in Chinese efforts to pursue a competitive advantage. In 2009, China was suspected of stealing large terabytes of design data for the F-35 Joint Strike Fighter from defense contractor Lockheed Martin's computers. In 2012, a Chinese version, the J-31, appeared to rival the F-35. In 2014, a Chinese national was indicted for theft of sensitive trade secrets defense contractors, particularly data relating to Boeing's C-17 military transport aircraft. Industrial espionage such as this yields economic benefits, as well as military and national security advantages for China, while eroding the technical superiority of the United States. Another concern with this type of espionage is that detailed knowledge of the F-35 and C-17 platforms could afford China the ability to hack a plane's command and control system, to alter its course or possibly disable it in a time of crisis. In addition, a network intrusion could allow an undetectable cyber weapon to be planted, lying dormant until activated during a conflict.

On the defensive side, China employs a combination of legal policies and information technology for censorship and surveillance of dissenters in a program called "The Golden Shield." This is often referred to as "The Great Firewall" of China. In addition, the People's Republic of China actively promotes the idea of "cyber sovereignty," putting borders on the internet based on territorial integrity. This may be a way for the government to bypass the democratic free-flow of information that the internet represents.

Reportedly, the CIA has chronicled China's information warfare activities inside the United States, where financial incentives such as personnel and support in funding are aimed at academic institutions and think tanks to dissuade them from research that paints China in a negative light. In a February 2018 hearing before the Senate Intelligence Committee, FBI Director Christopher Wray described so-called

Confucius Institutes, Chinese language and cultural centers at universities that may be used as espionage tools to influence public opinion or to stifle academic freedom by limiting or disallowing discussions on certain topics. China has invested heavily in the motion picture industry as a way to gain cultural and economic influence, though reportedly China's relationship with Hollywood has started to cool.

China has also been propagating an image of itself as a peaceful, nonthreatening nation focused on internal development rather than the pursuit of international power. UN Statements such as President Xi Jinping's that China "will never pursue hegemony, expansion, or sphere of influence" exemplify these attempts at influencing perception. Chinese information warfare doctrine suggests that these tactics are part of a broader strategy of encouraging complacency in potential adversaries. Other tactics include using international fora to promote the idea of arms control for "information weapons" in order to maintain control over its own information apparatus and to level the playing field with technologically advanced powers.

Islamic State

The Islamic State (IS) has pursued an IW strategy of accessing U.S. government computer systems for a variety of purposes. IS pursues five primary categories of activity when targeting United States computer systems: defacement, distributed denial of service, data theft, disabling websites, and data breaches.

The "Cyber Caliphate," a group of pro-Islamic State hackers also known as the "Islamic Cyber Army" (ICA) or "Islamic State Hacking Division," has a history of conducting a variety of operations within the information environment. The Department of Homeland Security and the FBI issued a joint statement in December 2014 warning members of the U.S. military that the Islamic State of Iraq and Syria (ISIS) may be mining social media to create "kill lists" of human targets or identify potential sympathizers for recruitment.

In 2015, the U.S. Central Command's social media sites such as Twitter and Facebook were taken over for a short period of time by hackers claiming to be affiliated with the Islamic State. While this hack may have caused no damage to Central Command's operations, it was apparently designed to create a perception of vulnerability and weak U.S. national security capabilities. In April 2017, a pro-ISIS group claims to have hacked the State Department's website, stolen data, and released a kill list of U.S. government officials. In addition, defacing government websites and redirecting web traffic are tactics used by the Islamic State to project its power online.

For the past several years, propaganda units of IS have been actively spreading their message through social media platforms such as Twitter, Facebook, and YouTube, as well as through radio broadcasts and news services. Videos showing the beheadings of Western hostages and the immolation of a caged Jordanian fighter pilot have made international headlines. Most recently, IS released a propaganda video showing an attack on U.S. soldiers in Niger that killed four Americans. Parts of this video were aired on television news shows. Videos such as these appear intended to convey the perception of IS as winning against a weakened and vulnerable U.S. military. Islamic State's media arm itself is intended to appear to be a

formalized, bureaucratic organization, thereby legitimizing IS and giving the appearance of an actual state. In 2015, then-FBI Director James B. Comey described these propaganda units as legitimate military targets.

North Korea

Since its founding in 1949, North Korea has conducted an array of IW activities designed to promote its interests. These have been particularly active in South Korea and Japan, where North Korea has cultivated sympathetic followers. Its actions were particularly influential during South Korea's period of military dictatorship, which ended in 1988, but they have continued since then in an attempt to influence South Korean politics as well as the North Korea policies of outside powers, including the United States. More recently, North Korea has been complementing these traditional information warfare activities with an increasingly capable cyber program.

In 2014, the run-up to the scheduled Christmas Day release of The Interview, a film depicting the assassination of North Korean leader Kim Jong Un, North Korea's Foreign Ministry called the film "the most blatant act of terrorism and war" and threatened a "merciless countermeasure." On November 24, 2014, Sony experienced a cyberattack that disabled its information technology systems, destroyed data, damaged computer workstations, and released internal emails. North Korea denied involvement in the attack but praised hackers, called the "Guardians of Peace," for having done a "righteous deed." Emails followed, threatening "9/11-style" terrorist attacks on theaters scheduled to show the film, leading some theaters to cancel screenings and for Sony to cancel its widespread release, although U.S. officials claimed to have "no specific, credible intelligence of such a plot." The FBI attributed the attacks to the North Korean government.

Independent of the level of economic and physical damage that Sony suffered as a result of these cyberattacks, one could argue that the incident represents a successful use of IW to achieve political ends. Some questioned whether North Korea had developed a sophisticated cyberattack force, using these attacks to demonstrate its increasing ability to pursue political goals and thereby raise its profile on the international stage. Others pointed to the common use of proxies or mercenary hackers to conduct relatively simple cyber operations as a form of political protest or "cyber riot." Whether or not the North Korean government conducted the attacks or outsourced to a proxy organization, the cyberattacks, in concert with threats of physical destruction, affected the decision-making process of a private company, exploited the human element of fear in a civilian population, imposed extra-territorial censorship, and triggered a response from the U.S. government.

North Korea appears to be engaging in increasingly hostile cyber activities, including theft, website vandalism, and denial of service attacks. Some cybersecurity analysts, however, question whether the country has developed the technical capability to conduct large-scale destructive attacks on critical infrastructure. Some observers suggest that, because there is little visibility into North Korea's activities, the possible threats from North Korean cyber activities are often inflated. An assessment released by the Korea Economic Institute found that the international community's "fears of the unknown increase the risk of threat inflation dramatically."

These analysts contend that while North Korea may have the capability to undertake global cyber nuisance or theft-motivated activities, the nation lacks the ability to undertake operations that are "complex or as devastating as the Stuxnet attack, a computer virus that disrupted Iran's nuclear program." The ambiguous threat of North Korean cyberattack ability, or fear of the unknown, creates a psychological effect that could perhaps deter some countries from conducting cyberspace operations on North Korean networks.

Outside of cyberspace, North Korean use of the information environment include its presence at the 2018 Winter Olympics, propaganda photos, videos, and claims in the media that place North Korea and its leadership in a favorable light, contrasting it with other countries such as South Korea and the United States. Some argue that U.S. journalists' coverage of North Korea and the Olympics suggest that the event was a propaganda win for North Korean leaders. Likewise, recent propaganda posters and stamps for the 70th anniversary of the founding of North Korea declare "Victory in all fronts." The North Korean government has also tried to use information campaigns to set the agendas of international negotiations such as inter-Korean dialogue and nuclear talks with the United States.

Iran

Similar to China, Iranian information operations target and discredit dissenters and adversaries, both domestic and foreign—to include journalists, online media activists, and human rights defenders—and limiting or prohibiting attempts by protesters to coordinate and organize. The Islamic Republic of Iran Broadcasting (IRIB) corporation runs the government's foreign media arms, which are largely considered propaganda tools as opposed to public diplomacy. In cyberspace, the Iranian government shut down social media platforms and disrupted internet access during nationwide protests in January 2018. Iran may also be seeking a capability to disable or destroy critical infrastructure through cyber means.

Beginning in 2011, a wave of cyberattacks on U.S. financial institutions disrupted banking operation and denied some customers from online access to their accounts. Roughly four dozen banks, including JPMorgan Chase, Bank of America, Capital One and PNC Bank, were besieged by crippling denial of service attacks that lasted for over a year. Some have speculated that these were conducted in retaliation for the Stuxnet worm, which disabled the computer systems that controlled nuclear centrifuges at Iran's main nuclear enrichment plant in 2010.

A cyber intrusion into the computer program controlling the sluice gate to the Bowman Dam in Rye, NY, appeared be an effort to take over the computer controls to the dam itself. Any attempt to do so failed, however, because the dam was under repair and offline.

According to an indictment by the U.S. Department of Justice, the perpetrators for both the bank and dam incidents are associated with Iran's Islamic Revolutionary Guards Corps, a unit of which is the Iranian Cyber Army (ICA), which runs military cyber operations. Iran openly encourages hacker groups to conduct offensive cyberspace operations. Hackers deface websites, steal and leak content, and may be involved in cyber espionage operations. The Iranian Cyber Army (ICA) has been

implicated in several website attacks, including one against Twitter in 2009 that proclaimed support for Iran's Supreme Leader Ali Khamenei. Other attack targets were the Voice of America in 2011 after the United States rhetorically supported Iran's opposition Green movement, and regime opposition websites in 2013 just before the presidential election.

SOURCE: Congressional Research Service, *Information Warfare: Issues for Congress* (Washington, D.C.: Congressional Research Service, 2018), 9–15, https://crsreports.congress.gov/product/pdf/R/R45142

ANALYSIS

In 2003, President George W. Bush referred to Iran, Iraq, and North Korea as an "Axis of Evil," although much of his presidency focused upon efforts to eradicate al Qaeda. President Trump's administration has made repeated references to the concept of "Four Plus One," suggesting that the greatest dangers to American interests come from China, Russia, Iran, North Korea, and violent extremist organizations such as the Islamic State. Although the CRS is an agency dedicated to serving the legislative branch, this report derived much of its conclusions from source materials initially created by the executive branch—and as a result, one can see the influence of the military and intelligence organizations when determining which threats merit significant discussion. It is worthwhile to note that each of those adversaries has its own approach to cyber warfare and widely disparate capabilities within the cyber domain. Unsurprisingly, the greatest competitors within the cyber realm are nation-states that are also competitive in a conventional and nuclear military sense—China and Russia. Compared to those global powers, the cyber efforts of Iran, North Korea, and the Islamic State all pale almost to insignificance.

- ***Document 54:*** *Cybersecurity: Selected Issues for the 115th Congress*
- ***When:*** March 9, 2018
- ***Where:*** Washington, D.C.
- ***Significance:*** The CRS provides background information for members of Congress, typically in response to Congressional requests. In this case, the CRS provided a background and summary of overarching cyber concepts, effectively creating a "primer" for members of Congress, who in turn are expected to create legislative solutions to vexing cyber problems.

DOCUMENT

Terrorist Use of Cyberspace

Terrorist use of cyberspace is growing both in terms of reliance for supporting organizational activities and for gaining expertise to achieve operational goals. While no publicly accessible report has been published regarding a confirmed cyberterrorist attack against the United States, the possibility of one exists. Tighter physical and border security may encourage terrorists and extremists to try to use novel weapons to attack the United States. Persistent internet and computer security vulnerabilities, which have been widely publicized, may gradually encourage terrorists to continue to enhance their computer skills, or develop alliances with criminal organizations and consider attempting a cyberattack against U.S. critical infrastructure, facilities, and activities that support global security interests.

Cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives. Transnational terrorist organizations have used the internet as a tool for planning attacks, radicalization and recruitment, a method of propaganda distribution, as a means of communication, and for disruptive purposes.

The vulnerability of critical life-sustaining control systems being accessed and destroyed via the internet has been demonstrated. In 2009, the Department of Homeland Security (DHS) conducted an experiment that revealed some of the vulnerabilities to the nation's control systems that manage electric power generators and grids. The experiment, known as the Aurora Project, entailed a computer-based attack on a power generator's control system that caused operations to cease and the equipment to be destroyed. Cyberterrorists may be seeking a destructive capability to exploit these types of vulnerabilities in critical infrastructure but progress toward this goal is uncertain. As noted in March 2017 by then-Federal Bureau of Investigation (FBI) Director James Comey, "terrorists have not yet figured out how to use the Internet as an instrument of destruction . . . eventually these knuckleheads will."

There is no consensus definition of what constitutes cyberterrorism. The closest in law is found in the USA PATRIOT Act statute governing "acts of terrorism transcending national boundaries," which includes in its definition of a "federal crime of terrorism" some violations of the Computer Fraud and Abuse Act (CFAA). One portion of the CFAA referenced by the USA PATRIOT Act makes it illegal for an entity to:

> knowingly [access] a computer without authorization or exceeding authorized access, and by means of such conduct . . . [obtain] information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation.

The other CFAA provision referenced in the USA PATRIOT Act prohibits transmitting "a program, information, code, or command" to certain computers (including

DID YOU KNOW?

Congressional Research Service

The Congressional Research Service (CRS) provides nonpartisan research and information assistance to the U.S. Congress. It was established in 1914 as the Legislative Reference Service, and renamed in a 1970 expansion of its responsibilities. All members of Congress are able to utilize the service, which maintains a strict confidentiality about inquiries. CRS experts provide timely, thorough, and objective responses to Congressional inquiries, and prepare larger research projects in response to Congressional requests. CRS employs more than four hundred analysts, attorneys, and subject-matter experts.

all government computers and most private ones) and thereby intentionally causing unauthorized damage.

Some cyberwarfare experts define cyberterrorism as "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." The USA PATRIOT Act's definition of "federal crime of terrorism," with its inclusion of certain CFAA violations as predicate acts, has some similarities to this definition, though the statute is limited to only those attacks with political objectives. However, these provisions are also criminal statutes and generally refer to individuals or organizations rather than state actors. Naval Post Graduate School Defense analyst Dorothy Denning's definition of cyberterrorism focuses on the distinction between destructive and disruptive action. Terrorism generates fear comparable to that of physical attack, and is not just a "costly nuisance." Though a DDOS attack itself does not yield this kind of fear or destruction, the broader issue is the potential for second- or third-order effects. For example, if telecommunications and emergency services were completely dismantled in a time of crisis, the effects of that sort of infrastructure attack could potentially be catastrophic. If an attack on the emergency services system were to coincide with a planned real-world event, then cyberterror may be an appropriate metaphor. However, in this case, the emergency service system itself would most likely not be a target, but rather the result of collateral damage to a vulnerable telecommunications network.

There are a number of reasons that may explain why the term "cyberterrorism" has not been statutorily defined, including the difficulty in identifying applicable activities, whether articulating clear red lines would demand a response for lower-level incidents, and retaining strategic maneuverability so as not to bind future U.S. activities in cyberspace.

Selected Policy Issues

Critical Infrastructure

Critical infrastructure (CI) is defined in 42 U.S.C. §5195c(e) as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Most U.S. CI is controlled by the private sector. Under the Homeland Security Act of 2002, as amended, DHS coordinates CI security, including cybersecurity.

CI is classified into sectors, most recently 16 under Presidential Policy Directive 21, issued in 2013, with each sector having a designated sector-specific agency. Some agencies have cross-sector responsibilities, such as DHS, DOJ and the Federal Trade Commission (FTC).

The increasing potential for attacks that might cripple components of CI or otherwise damage the national economy has led to debate about the best ways to protect those sectors. Some, such as the chemical and financial sectors, are subject to federal regulation. The protection of others, such as information technology, relies largely on voluntary efforts. The efficacy of that mix of voluntary and regulatory efforts has long been a source of controversy.

In 2013, Executive Order 13636 established an alternative approach, in which the National Institute of Standards and Technology (NIST) facilitated a public-private effort to develop a cybersecurity framework for CI sectors. Subsequently, Congress authorized the framework process in the Cybersecurity Enhancement Act of 2014 (P.L. 113-274). Issued in 2014, the framework consists of three parts: (1) a core set of activities and outcomes applicable to all the sectors, organized into five functions (identify, protect, detect, respond, and recover); (2) a profile describing an entity's current and target cybersecurity postures; and (3) implementation tiers that characterize the entity's current and intended practices. The DHS C3 (for Critical infrastructure Cyber Community) program works to facilitate its voluntary adoption, and NIST released a draft update in January 2017.

Before the development of the voluntary cybersecurity framework, debate about the role of federal regulation appeared to be a significant factor impeding the enactment of cybersecurity legislation. However, events associated with the rapidly evolving threat environment continue to draw attention to the question of the appropriate federal role in protecting CI. Attacks such as the ones in 2016 using the Mirai botnet have led to renewed calls by some observers for broad security regulations. Attempts attributed to Russia at interfering with the November 2016 federal election have renewed concerns about the security of the U.S. election infrastructure, leading to the controversial designation by DHS of state and local election systems as a subsector under the government facilities CI sector. The 115th Congress may be faced with the need to address such problems and resolve the controversies, which may be made more urgent by the expected continued evolution of cyberspace and more difficult by the unpredictable nature of emerging threats.

Data Breaches and Data Security

Congress has sought policy responses to the loss of data by both private sector companies and government agencies, prompted by high-profile breaches such as those at Equifax and the Securities and Exchange Commission (SEC). Breaches frequently occur because of the reliance of modern business practices on IT. An increasingly used catch-phrase among industry analysts is that today "all companies are technology companies," or "all companies are data companies." This concept reflects the role that IT and data play in enabling modern business practices that allow companies to compete and thrive in the marketplace. However, this reliance on IT and data also creates risk for corporate leadership to manage. Cybersecurity initiatives seek to control that risk.

Congress has held hearings to examine individual instances of breaches and encourage the breached entities to assist those whose data has been compromised. Additionally, some Members have introduced legislation to address a variety of elements around a data breach, such as standards for securing sensitive data, data

breach notification requirements, and the responsibilities affected entities have to those whose data has been breached.

Education and Training

Increasing awareness of cyberattacks—and the increasing connectedness of cyber and cyber-physical systems—have raised concerns about whether U.S. homes, businesses, and government are prepared to secure themselves in our digitally integrated world. Some of this attention to preparedness has focused on the sufficiency of cybersecurity education, training, and workforce development in the United States. Federal policymakers have grappled with questions about both the quality and the quantity of U.S. postsecondary education graduates with cybersecurity credentials (in general) and the civilian and military workforce needs of the federal government (in particular). Federal programs and policies have also sought to increase awareness of secure computing practices (e.g., don't re-use passwords); and policymakers and agency officials often view educational benefits (e.g., scholarships, training) as a tool for attracting and retaining federal military and civilian cybersecurity workers.

The federal effort in cybersecurity education, training, and workforce development has not been comprehensively inventoried. However, federal funding supports a wide variety of activities in this area. These activities, which are sometimes offered in partnership with multiple federal and non-federal entities, include cybersecurity awareness (StaySafeOnline.org), summer camps (GenCyber) and student competitions (CyberPatriot and the National Collegiate Cyber Defense Competition), scholarships for cybersecurity postsecondary students who agree to serve in government after graduation (CyberCorps), and professional development for federal personnel in specialized cybersecurity positions (College of Cyber and the Federal Virtual Training Environment). Federal programs not specifically designed to provide cybersecurity education and training—such as the TechHire and Advanced Technological Education programs—may also provide grants for these purposes.

Over the past decade, analysts seeking to document the scope and scale of the U.S. cybersecurity workforce came to realize that the federal government, private employers, and academics were not using the same language to describe cybersecurity jobs or the knowledge, skills, and abilities necessary to hold those positions. This lack of a common language was perceived as a potential barrier in the cybersecurity labor market and an impediment in federal hiring. In response, the National Initiative for Cybersecurity Education (NICE)—the federal coordinating body for cybersecurity education, training, and workforce development—undertook a multi-year effort to develop standard terms and uses. When finalized, the NICE Cybersecurity Workforce Framework (Framework) is to provide a standard vocabulary that can be used to better align education and employment in cybersecurity fields. Among its many other cybersecurity education-related activities, NICE also provides grants to regional education-employment partnerships for the purpose of aligning academic pathways with cybersecurity occupations.

One key policy issue for the 115th Congress may relate to the Framework's implementation. Although the central issue for the Framework is its use as a cybersecurity workforce management tool in federal agencies, cybersecurity education programs may begin to adopt the language (and align curriculum and grantee requirements)

during the next few years as well. Other policy topics that may be addressed during the 115th Congress include the role or expansion of educational benefits as tools for attracting and retaining federal cybersecurity personnel; as well as funding for federal cybersecurity education, training, and workforce development programs. Longer-term policy issues in cybersecurity education may include the ongoing challenge of ensuring that educational content evolves in tandem with the rapidly changing cyber defense and operations landscape; continued training of incumbent workers in the federal government in secure computing practices; and, potentially, the continuing development of existing certifications, or the creation of new, non-traditional educational credentials, such as micro-credentialing and digital badging.

Encryption

Encryption is a process to secure information from unwanted access or use. Encryption uses the art of cryptography to change information which can be read (plaintext) and make it so that it cannot be read (ciphertext). Decryption uses the same art of cryptography to change that ciphertext back to plaintext. Data that are in a state of being stored or transmitted are eligible for encryption. However, data that are in a state of being processed—that is being generated, altered, or otherwise used—are unable to be encrypted and remain in plaintext and vulnerable to unauthorized access.

Encryption as a Cybersecurity Tool

Encryption is used by a variety of users for a variety of purposes. Fundamentally, encryption enables information to remain confidential to a single user or between a user and multiple users. Encryption also enables a level of certainty that the communicating parties are who they say they are and that the communication is only available to intended recipients.

Individuals use encryption to keep aspects of their lives that are held on digital platforms private on their devices and among those with whom they share information. Businesses use encryption to ensure that their research is kept confidential from their competitors, and to ensure that their transactions with their suppliers and customers are authentic. Governments use encryption to assure their information is kept and handled in confidence. Even without a user's interaction, devices may use encryption when communicating to other devices to ensure that commands received from one device are authentic and safe to execute. However, those seeking to obscure their malicious activities from legal authorities may also employ encryption to thwart opportunities to disrupt their malicious activity.

Encryption and Law Enforcement Investigations

Changing technology presents opportunities and challenges for U.S. law enforcement. While some feel that law enforcement now has more information available to them than ever before, others contend that law enforcement is "going dark" as their investigative capabilities are outpaced by the speed of technological change. As such, law enforcement cannot access certain information they otherwise may be authorized to obtain. One such technology-related hurdle for law enforcement is strong, end-to-end (or what law enforcement has sometimes called "warrantproof") encryption.

The tension between law enforcement capabilities and technological change has received congressional attention for several decades. For instance, in the 1990s the "crypto wars" pitted the government against technology companies, and this tension was highlighted by proposals to build in vulnerabilities, or "back doors," to certain encrypted communications devices as well as to restrict the export of strong encryption code. In addition, Congress passed the Communications Assistance for Law Enforcement Act (CALEA; P.L. 103-414) in 1994 to help law enforcement maintain their ability to execute authorized electronic surveillance as telecommunications providers turned to digital and wireless technology.

There has been previous executive and congressional action aimed at helping law enforcement conduct investigations of cybercrimes in the face of changing technology that can hamper such investigations. The going dark debate originally focused on data in motion, or law enforcement's ability to intercept real-time communications. However, more recent technology changes have affected law enforcement's capacity to access not only communications but also stored content, or data at rest. The Obama Administration urged the technology community to develop a means to assist law enforcement in accessing encrypted data and took steps to bolster law enforcement's technology capabilities to do so. In addition, policymakers have been evaluating whether legislation may be an appropriate response to the problem of going dark—particularly with regards to encryption. The Encryption Working Group in the 114th Congress made several observations to set up the going dark discussion for the 115th Congress. It noted that (1) any measure to weaken encryption would work against the nation's interest, (2) encryption technology is widely used and increasingly available worldwide, (3) there is no one-size-fits-all solution to the encryption and going dark challenge, and (4) Congress should promote cooperation between the law enforcement and technology communities.

. . .

International Issues

Trade

Cybersecurity poses challenges in the international trade arena as more trade is conducted, or facilitated, online, potentially increasing the susceptibility of commerce to cyberattack and theft of information. Digital trade, including end-products like movies and video games, and services such as email and online banking, enhances the productivity and overall competitiveness of an economy, enabling technological shifts that are transforming businesses. According to one study, the global economic impact of the internet is estimated at $4.2 trillion in 2016, and would rank as the fifth-largest national economy in the world. According to the Bureau of Economic Analysis, in 2015, the United States exported $751 billion in services, of which over 60% were information and communication technology (ICT) and potentially ICT-enabled services.

The increase in digital trade also raises new challenges in U.S. trade policy, including how best to address new and emerging trade barriers and risks related to cybersecurity. For example, hacks into company databases and systems could disrupt worldwide business operations, global supply chains, and pose a threat to consumers whose personal information may be stolen or manipulated. Publicized cyberattacks

on firms may depress stock values. When governments of U.S. trading partners impose trade barriers such as data localization measures compelling companies to store data within the country's border, a U.S. firm's data may become fragmented, creating vulnerabilities and increasing the risk of a cyberattack.

The internet is a key driver of trade in intellectual property-related trade. However, it can make infringement of intellectual property rights (IPR) easier, and identifying those responsible for IPR infringement more challenging. Cyber theft of trade secrets can wipe out the value and competitive advantage of a firm's long-term research, presenting additional, increasingly prominent, barriers to digital trade. In May 2014, DOJ indicted five Chinese individuals for government-sponsored cyber espionage against U.S. companies and theft of proprietary information to aid the competitiveness of Chinese state-owned enterprises (SOEs).

U.S. companies see potential challenges as countries develop new cyber regimes, such as China's new cybersecurity law, passed in November 2016. The law imposes several restrictions on internet firms including requiring operators of critical information infrastructure (defined as sectors such as telecommunications, energy, and finance) to store certain data in China, and requiring companies to assist Chinese police and national security agencies. The law's security reviews may force companies to disclose source code, a concern of many U.S. firms who are hesitant to reveal proprietary information about their business intellectual property that could potentially expose them to further cyberattacks. The law states that a key goal is "secure and controllable" technology, a term some see as an attempt to promote local ICT providers and lock out foreign firms. U.S. companies and various U.S. officials, such as former National Security Adviser Susan Rice, have raised U.S. concerns about the potential impact of the law.

The United States holds high-level cyber dialogues with multiple bilateral partners, such as China, India, and the European Union, to focus on cybersecurity efforts. Recent bilateral and plurilateral agreements have begun to address digital trade rules and barriers more explicitly. For example, the proposed Trans-Pacific Partnership (TPP) promoted cooperation amongst the parties on cybersecurity issues and has new enforceable commitments to combat cyber theft of trade secrets and localization barriers. The United States also discusses digital trade and cybersecurity norms in forums such as the Group of 20 (G-20), the Organization for Economic Co-operation and Development (OECD), and the Asia-Pacific Economic Cooperation (APEC). The 2016 G-7 Joint Declaration endorsed the "G7 Principles and Actions on Cyber."

Congress has an interest in ensuring the global rules and norms of the internet economy align with U.S. laws and norms, and that U.S. trade policy on digital trade and cybersecurity advances U.S. interests. Congress may consider specific actions to uphold the G-7 commitments to serve as a model for other countries; hold hearings on trade barriers, negotiations, or international forums in relation to cybersecurity; conduct oversight of the relevant executive branch agencies; or consider legislation to respond to cybersecurity threats to U.S. trade and businesses, including the imposition of sanctions.

SOURCE: Congressional Research Service, *Cybersecurity: Selected Issues for the 115th Congress* (Washington, D.C.: Congressional Research Service, 2018), 4, 9–14, 16–17. https://fas.org/sgp/crs/misc/R45127.pdf

ANALYSIS

It is certainly important for Congressional members to be familiar with the broad parameters of cyberspace, as well as the potential national security risks that it can facilitate. As such, it is useful for members of Congress to be educated upon the subjects they are expected to legislate. This report is effectively a very basic primer—and yet, it represents the sum knowledge of many members of Congress regarding the cyber domain. It is illustrative that the authors of the report placed such a high emphasis upon cyber terrorism, even though there had been very few cyber terror events prior to its publication. Such a priority of placement within the document may have served to arouse Congressional interest in the subject of cybersecurity, and if so, it may have encouraged them to continue reading the report. But, it might also have placed far too much emphasis upon a minimal threat, while all but ignoring the very real challenges associated with nation-states engaging in aggressive activities through the cyber domain.

- ***Document 55:*** *Joint Publication 3-12: Cyberspace Operations*
- ***When:*** June 8, 2018
- ***Where:*** Washington, D.C.
- ***Significance:*** Doctrine is effectively the distillation of best practices and lessons learned within a military organization. It is meant to serve as a guide to future planning and action, rather than an absolute requirement. Joint doctrine is designed to unify the perspectives of the various services into a single vision—in this case, one designed to offer guidance regarding cyberspace.

DOCUMENT

Challenges to the Joint Force's Use of Cyberspace

The JFC faces a unique set of persistent challenges executing CO in a complex global security environment.

a. **Threats.** Cyberspace presents the JFC's operations with many threats, from nation-states to individual actors to accidents and natural hazards.

(1) **Nation-State Threat.** This threat is potentially the most dangerous because of nation-state access to resources, personnel, and time that may not be available to other actors. Some nations may employ cyberspace capabilities to attack or conduct espionage against the

US. Nation-state threats involve traditional adversaries; enemies; and potentially, in the case of espionage, even traditional allies. Nation-states may conduct operations directly or may outsource them to third parties, including front companies, patriotic hackers, or other surrogates, to achieve their objectives.

(2) **Non-State Threats.** Non-state threats are formal and informal organizations not bound by national borders, including legitimate nongovernmental organizations (NGOs), and illegitimate organizations such as criminal organizations, violent extremist organizations, or other enemies and adversaries. Non-state threats use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, undermine confidence in governments, conduct espionage, and conduct direct terrorist actions within cyberspace. Criminal organizations may be national or transnational in nature and steal information for their own use, including selling it to raise capital and target financial institutions for fraud and theft of funds. They may also be used as surrogates by nation-states or non-state threats to conduct attacks or espionage through cyberspace.

(3) **Individuals or Small Group Threat.** Even individuals or small groups of people can attack or exploit US cyberspace, enabled by affordable and readily available techniques and malware. Their intentions are as varied as the number of groups and individuals. These threats exploit vulnerabilities to gain access to discover additional vulnerabilities or sensitive data or maneuver to achieve other objectives. Ethical hackers may share the vulnerability information with the network owners, but, more frequently, these accesses are used for malicious intent. Some threats are politically motivated and use cyberspace to spread their message. The activities of these small-scale threats can be co-opted by more sophisticated threats, such as criminal organizations or nation-states, often without their knowledge, to execute operations against targets while concealing the identity of the threat/sponsor and also creating plausible deniability.

DID YOU KNOW?

USA PATRIOT Act

In the immediate aftermath of the terror attacks of September 11, 2001, the U.S. Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), which President George W. Bush signed into law on October 26. Ostensibly, the law served to allow the government greater surveillance powers as a means to deter and defeat terror attacks. It expanded upon the 1978 Foreign Intelligence Surveillance Act and the 1996 Antiterrorism Act, and was first proposed on September 13, passing after only 30 minutes of debate. Overwhelming support in both the House and the Senate accompanied a law that effectively rewrote the federal government's relationship with its citizens. In practice, the USA PATRIOT Act lowers the threshold necessary for search warrants, enables expanded wiretapping and tracking of electronic communications, and provides greater opportunities for intelligence agencies to operate on U.S. soil. Because it was passed just as the internet was becoming a central point of the economic and social life of the nation, the USA PATRIOT Act had a major influence over the way in which the government and citizens interacted with one another in the cyber domain.

(4) **Accidents and Natural Hazards.** The physical infrastructure of cyberspace is routinely disrupted by operator errors, industrial accidents, and natural disasters. These unpredictable events can have greater impact on joint operations than the actions of enemies. Recovery from accidents and hazardous incidents can be complicated by the requirement for significant coordination external to DOD and/or the temporary reliance on back-up systems with which operators may not be proficient.

b. **Anonymity and Difficulties with Attribution.** To initiate an appropriate defensive response, attribution of threats in cyberspace is crucial for any actions external to the defended cyberspace beyond that authorized as authorized self-defense. The most challenging aspect of attributing actions in cyberspace is connecting a particular cyber-persona or action to a named individual, group, or nation-state, with sufficient confidence and verifiability to hold them accountable. This effort requires significant analysis and, often, collaboration with non-cyberspace agencies or organizations. The nature of cyberspace, government policies, and laws, both domestic and international, presents challenges to determining the exact origin of cyberspace threats. The ability to hide the sponsor and/or the threat behind a particular malicious effect in cyberspace makes it difficult to determine how, when, and where to respond. The design of the internet lends itself to anonymity and, combined with applications intended to hide the identity of users, attribution will continue to be a challenge for the foreseeable future.

c. **Geography Challenges.** In cyberspace, there is no stateless maneuver space. Therefore, when US military forces maneuver in foreign cyberspace, mission and policy requirements may require they maneuver clandestinely without the knowledge of the state where the infrastructure is located. Because CO can often be executed remotely, through a virtual presence enabled by wired or wireless access, many CO do not require physical proximity to the target but use remote actions to create effects, which represents an increase in operational reach not available in the physical domains. This use of global reach applies equally to both external operations in red and gray cyberspace, as well as internal protection effects in blue cyberspace. The cumulative effects of some CO may extend beyond the initial target, a joint operations area (JOA), or outside of a single area of responsibility (AOR). Because of transregional considerations and the requirement for high-demand forces and capabilities, some CO are coordinated, integrated, and synchronized using centralized execution from a location remote from the supported commander.

d. **Technology Challenges.** Using a cyberspace capability that relies on exploitation of technical vulnerabilities in the target may reveal its functionality and compromise the capability's effectiveness for future missions. This has implications for both offensive cyberspace operations (OCO) and defensive cyberspace operations (DCO) missions.

Cyberspace capabilities without hardware components can be replicated for little or no cost. This means that once discovered, these capabilities will be widely available to adversaries, in some cases before security measures in the DODIN can be updated to account for the new threat. In addition, since similar technologies around the world share similar vulnerabilities, a single adversary may be able to exploit multiple targets at once using the same malware or exploitation tactic. Malware can be modified (or be designed to automatically modify itself), complicating efforts to detect and eradicate it.

e. **Private Industry and Public Infrastructure.** Many of DOD's critical functions and operations rely on contracted commercial assets, including internet service providers (ISPs) and global supply chains, over which DOD and its forces have no direct authority. This includes both data storage services and applications provided from a cloud computing architecture. Cloud computing enables DOD to consolidate infrastructure, leverage commodity IT functions, and eliminate functional redundancies while improving continuity of operations. But, the overall success of these initiatives depends upon well-executed risk mitigation and protection measures, defined and understood by both DOD components and industry. Dependency on commercial internet providers means DOD coordination with the Department of Homeland Security (DHS), other interagency partners, and the private sector is essential to establish and maintain security of DOD's information. DOD supports DHS, which leads interagency efforts to identify and mitigate cyberspace vulnerabilities in the nation's critical infrastructure. DOD has the lead for improving security of the defense industrial base (DIB) sector, which includes major sector contractors and major contractor support to operations regardless of corporate country of domicile and continues to support the development of whole-of-government approaches for its risk management. The global technology supply chain affects mission-critical aspects of the DOD enterprise, and the resulting IT risks can only be effectively mitigated through public-private sector cooperation.

(1) **Globalization.** The combination of DOD's global operations with its reliance on cyberspace and associated technologies means DOD often procures mission-essential IT products and services from foreign vendors. A prime example is our reliance on network backbones and transmission equipment in other countries, such as undersea cables, fiber optic networks and telecommunications services, satellite and microwave antennas, and leased channels on foreign satellites. These systems may normally be reliable and trustworthy, but they can also leave US forces vulnerable to access denial by service interruption, communications interception and monitoring, or infiltration and data compromise. Another example is DOD's use of commercial, globally interconnected, globally sourced IT components in mission-critical systems and networks.

Leveraging rapid technology development of the commercial marketplace remains a key DOD advantage. While globally sourced technology provides innumerable benefits to DOD, it also provides adversaries the opportunity to compromise the supply chain to access or alter data and hardware, corrupt products, and to intercept or deny communications and other mission-critical functions. Supply chain risks threaten all users and our collective security; therefore, DOD cannot ignore these risks to its missions. Globalization, including by US companies, introduces risks across the entire system lifecycle, to include design, manufacturing, production, distribution, operation and maintenance, and disposal of a system or component. Each of these lifecycle stages presents the opportunity to manipulate, deny, or collect information on such systems. It is not feasible to eliminate our reliance on foreign-owned services and products, but our reliance on them makes it essential every reasonable avenue for risk mitigation be pursued, to include user and commander education at all levels, encryption, C2 system redundancy, operations security (OPSEC), and careful inspection of vendor-provided equipment in accordance with (IAW) DOD IT procurement policy.

(2) **Mitigations.** DOD partners with the DIB to increase the security of information about DOD programs residing on or transiting DIB unclassified networks. The Department of Defense Cyber Crime Center (DC3) serves as DOD's operational focal point for voluntary cyberspace information sharing and incident reporting program. In addition, DOD is strengthening its acquisition regulations to require consideration of applicable cybersecurity policies during procurement of all DODIN components to reduce risks to joint operations.

SOURCE: U.S. Department of Defense, *Joint Publication 3-12: Cyberspace Operations* (Washington, D.C.: Government Printing Office, 2018), I–11, I–14, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

ANALYSIS

When the U.S. Department of Defense created U.S. Cyber Command (USCYBERCOM), it did so in large part to prevent the duplication of efforts being carried out by each of the services in its cyberspace operations. In addition to each service adopting different policies for cyber defense, none of the services held the responsibility for conducting offensive cyber operations against national adversaries. However, for an overarching organization like USCYBERCOM to be truly effective in the modern environment, it needs a common understanding of the mission, challenges faced, and most important considerations for its members. *Joint Publication 3-12* offered such a vision by establishing the parameters of cyber operations and

how they differ from other forms of military activities. Although most of the day-to-day operations of USCYBERCOM are of a classified nature, publicly sharing the doctrine of the organization makes it much easier for allies and adversaries to understand how the U.S. military perceives its role in the cyber domain.

- ***Document 56:*** *Developments in the Field of Information and Communications Technology in the Context of International Security*
- ***When:*** October 18, 2018
- ***Where:*** U.S. Delegation, United Nations, NY, US
- ***Significance:*** The United States offered a proposal at the United Nations to set the international norms for behavior within the cyber domain. The proposal, if adopted, had the potential to offer substantial advantages to the United States and, if followed by all nations, to curb the behaviors that the U.S. government finds most objectionable, particularly by attackers in the Russian Federation and the People's Republic of China.

DOCUMENT

Advancing responsible State behaviour in cyberspace in the context of international security

Calls upon Member States:

(a) To be guided in their use of information and communications technologies by the 2010, 2013 and 2015 reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security;

(b) To support the implementation of cooperative measures, as identified in the reports of the Group of Governmental Experts, to address the threats emerging in this field and ensure an open, interoperable, reliable and secure information and communications technology environment consistent with the need to preserve the free flow of information;

2. *Invites* all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts, to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(b) The content of the concepts mentioned in the reports of the Group of Governmental Experts;

3. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to be established in 2019 on the basis of equitable geographical distribution, proceeding from the assessments and recommendations contained in the above-mentioned reports, to continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence -building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States, and to submit a report on the results of the study, including an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by States, to the General Assembly at its seventy-sixth session;

4. *Requests* the Office for Disarmament Affairs of the Secretariat, through existing resources and voluntary contributions, on behalf of the members of the group of governmental experts, to collaborate with relevant regional organizations, such as the African Union, the European Union, the Organization of American States, the Organization for Security and Cooperation in Europe and the Regional Forum of the Association of Southeast Asian Nations, to convene a series of consultations to share views on the issues within the mandate of the group in advance of its sessions;

5. *Requests* the Chair of the group of governmental experts to organize two two-day informal consultative meetings, open-ended so that all Member States can engage in interactive discussions and share their views, which the Chair shall convey to the group of governmental experts for consideration;

6. *Decides* to include in the provisional agenda of its seventy-fourth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

SOURCE: United States Delegation to the United Nations, *Developments in the Field of Information and Communications Technology in the Context of International Security*, October 18, 2018, 2–3, https://undocs.org/A/C.1/73/L.37

ANALYSIS

The United States has not always been interested in utilizing the mechanisms of the United Nations to set limits upon national behavior, particularly in cyberspace. More cyberattacks are launched from the United States than any other nation, which might account for this hesitance (although most of the attacks in question are not of government origin). However, in recent years, the United States has become increasingly vocal in its criticisms of other nations that have launched massive cyber operations against American targets. This proposal represents a possible first step in curtailing such attacks or, at the very least, criminalizing them and making nations responsible for the behavior of their citizens. Unlike the competing Russian proposal (see Document 69 in this volume), this proposal, if adopted, would place the largest share of responsibility upon the governments of nations from which international cyberattacks originate.

4

NON-U.S. STRATEGY AND DOCUMENTS

- ***Document 57:*** *North Atlantic Treaty*
- ***When:*** 1949
- ***Where:*** Washington, D.C.
- ***Significance:*** In the aftermath of World War II, 12 European and North American states signed the North Atlantic Treaty, creating a defensive military alliance embodied in the North Atlantic Treaty Organization (NATO). Seventeen states have joined the alliance since its creation, including several former Soviet republics. Because an attack against one member state is considered an attack against all member states, there is some question whether the alliance extends to the cyber domain, and if so, with what limits.

DOCUMENT

Article 4

The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.

Article 5

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

SOURCE: North Atlantic Treaty Organization, Brussels, Belgium, 1949, http://www.nato.int/cps/en/natolive/official_texts_17120.htm

DID YOU KNOW?

Defense Advanced Research Projects Agency

In 1958, President Dwight D. Eisenhower authorized the creation of a Department of Defense research agency designed to pursue massive leaps forward in technological capabilities, particularly in space exploration. The Advanced Research Projects Agency (ARPA) soon relinquished the space projects to the National Aeronautics and Space Administration (NASA), but continued to pursue high-technology innovations, particularly in communications, computers, and surveillance capabilities. In 1970, ARPA established a four-node computer network, ARPANET, that eventually grew into the modern internet. Rechristened the Defense Advanced Research Projects Agency (DARPA) in 1972, the organization continued to pursue technological solutions to complex national security issues. Recent DARPA projects have examined artificial intelligence, speech recognition, and advanced computer designs, all proving to be key components in the current and future pursuit of cyber warfare.

ANALYSIS

NATO has never been truly tested as a military alliance in the face of a threat to national survival for any of its member states, which may be an indicator that it has had a significant deterrent value. The provisions of Article 4 have only been invoked a few times, and Article 5 has only been invoked once (by the United States in the aftermath of the September 11 attacks). In 2007, member state Estonia, which had joined NATO in 2004, considered an attempt to invoke Article 5 after a series of devastating cyberattacks attributed to the Russian Federation. However, the other member states of NATO responded instead by creating a cyber center for mutual cooperation and deterrence of future acts, rather than by launching a massive cyber assault against Russia.

- ***Document 58:*** *Unrestricted Warfare*
- ***When:*** 1999
- ***Where:*** Beijing, People's Republic of China
- ***Significance:*** After witnessing the performance of the U.S.-led coalition in Operation Desert Storm (1991), Chinese colonels Qiao Liang and Wang Ziangsui began to analyze the necessary means for the People's Republic of China to defend itself against a technologically superior rival, and possibly contest other geographic positions against an enemy possessing substantially better military equipment. They concluded that a nation such as China would need to harness all of the potential avenues of striking at an enemy, rather than restraining itself to the traditional aspects of military conflict. In particular, they recommended the utilization of economic attacks, weaponized legal activities such as protests at the United Nations and lawsuits within the United States, and the extensive use of cyber warfare in the event of any such conflict. In this section of their work, they discuss what they see as a coming revolution in information technology.

DOCUMENT

This revolution, however, will be upon us in full force soon enough. This time, technology is again running ahead of the military thinking. While no military thinker has yet put forth an extremely wide-ranging concept of the battlefield, technology is doing its utmost to extend the contemporary battlefield to a degree that

DID YOU KNOW?

Operation Shady Rat

Operation Shady Rat was a long-term cyber campaign conducted by Chinese hackers into a wide variety of targets, including defense contractors, electronics companies, energy corporations, and think tanks. It started as early as 2006, but was not detected until mid-2011, when McAfee Corporation released a report detailing the sophisticated campaign. Although McAfee did not specifically accuse the Chinese government of sponsoring or ordering the attacks, there is ample evidence that the hackers focused upon many issues that could only be of interest to the Chinese government, including the Olympic committees of five nations and the World Anti-Doping Agency. The effort to exfiltrate information from defense contractors regarding weapons technology and employment offered another substantial clue regarding the identity of the attackers. The full extent of Operation Shady Rat remains a mystery, but it was undoubtedly one of the longest and most successful cyber campaigns that has been publicly revealed to date.

is virtually infinite: there are satellites in space, there are submarines under the water, there are ballistic missiles that can reach anyplace on the globe, and electronic countermeasures are even now being carried out in the invisible electromagnetic spectrum space. Even the last refuge of the human race—the inner world of the heart—cannot avoid the attacks of psychological warfare. There are nets above and snares below, so that a person has no place to flee. All of the prevailing concepts about the breadth, depth and height of the operational space already appear to be old-fashioned and obsolete. In the wake of the expansion of mankind's imaginative powers and his ability to master technology, the battlespace is being stretched to its limits.

In spite of the situation described above, in military thinking, which is being drawn along by technology, there is still an unwillingness to simply stand still. Since technology has already served to open up more promising prospects for military thought, it is certainly not sufficient to simply expand the area of the battlefield in conventional "mesoscopic" [i.e., between macroscopic and microscopic] space. It is already clear that mechanical enlargement of the existing battlefield will not be the modus operandi for future battlefield change. The opinion that "the future battlefield expansion trend will be reflected in wars that are prosecuted in deeper parts of the oceans and at higher elevations in outer space" is merely a superficial point of view and conclusion that restricts itself to the level of general physics. The really revolutionary battlefield change stems from the expansion of the "non-natural space." There is no way that the electromagnetic spectrum space can be regarded as a battlespace in the former conventional sense. The electromagnetic spectrum space is a different kind of battlespace that stems from technological creativity and depends on technology. In this type of "man-made space," or "technological space," the concepts of length, width and height, or of land, sea, air and outer space, have all lost their significance. This is because of the special properties of electromagnetic signals whereby they can permeate and control conventional space without occupying any of this space. We can anticipate that every major alteration or extension of the battlespace of the future will depend on whether a certain kind of technological invention, or a number of technologies in combination, can create a brand new technological space. The "network space" is now drawing widespread attention among modern soldiers. Network space is a technological space that is formed by a distinctive combination of electronics technology, information technology and the application of specific designs. If one maintains that a war prosecuted in this space is still a war in which people control the outcome, then the "nanometer space" which is emerging hard on the heals of the network space, bodes well for the realization of mankind's dream—a war without the direct involvement of people. Some extremely imaginative and

creative soldiers are just now attempting to introduce these battlespaces, comprised of new technologies, into the warfare of the future. The time for a fundamental change in the battlefield—the arena of war—is not far off. Before very long, a network war or a nanometer war might become a reality right in our midst, a type of war that nobody even imagined in the past. It is likely to be very intense, but with practically no bloodshed. Nevertheless, it is likely to determine who is the victor and who the vanquished in an overall war. In more and more situations, this type of warfare will go along hand-in-hand with traditional warfare. The two types of battlespaces—the conventional space and the technological space—will overlap and intersect with each other, and will be mutually complementary as each develops in its own way. Thus, warfare will simultaneously evolve in the macroscopic, "mesoscopic," and microscopic spheres, as well as in various other spheres defined by their physical properties, which will all ultimately serve to make up a marvelous battlefield unprecedented in the annals of human warfare. At the same time, with the progressive breaking down of the distinction between military technology and civilian technology, and between the professional soldier and the non-professional warrior, the battlespace will overlap more and more with the non-battlespace, serving also to make the line between these two entities less and less clear. Fields that were formerly isolated from each other are being connected. Mankind is endowing virtually every space with battlefield significance. All that is needed is the ability to launch an attack in a certain place, using certain means, in order to achieve a certain goal. Thus, the battlefield is omnipresent. Just think, if it's even possible to start a war in a computer room or a stock exchange that will send an enemy country to its doom, then is there non-battlespace anywhere?

SOURCE: Qiao Liang and Wang Ziangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 41–43. https://www.c4i.org/unrestricted.pdf

ANALYSIS

By conceptualizing conflict as encompassing virtually every aspect of human behavior in modern society, the authors effectively sought to overturn prevailing assumptions about the limits of acceptable activities in wartime. The very title of the work was selected as a means to suggest that modern nation states should not confine their attacks to military targets on predefined battlefields, particularly if they faced a technologically or numerically superior enemy. To participate only on the terms most advantageous to the enemy would be to effectively cede the conflict to that enemy—and thus, it made substantially more strategic sense to launch attacks at targets that the enemy presumed to be "off-limits," which were then often more vulnerable to attack. Shortly after the creation of this work, the Chinese cyber enterprise became far more active, launching a series of extensive information-gathering campaigns as a means to improve the technological imbalance and, at the same time, penetrating an enormous number of private networks to develop economic opportunities for state-run and state-linked Chinese companies. For the past twenty years,

the U.S. national security establishment has been increasingly frustrated with Chinese cyberattacks—despite the fact that the blueprint for Chinese cyber campaigns was readily available for anyone who cared to read it, conveniently translated and published in English by the People's Liberation Army.

- ***Document 59:*** *Tallinn Manual on the International Law Applicable to Cyber Warfare*
- ***When:*** 2010
- ***Where:*** Tallinn, Estonia, NATO Cooperative Cyber Defence Centre of Excellence
- ***Significance:*** In the aftermath of devastating cyberattacks upon Estonia in 2007 and 2008, the small Baltic nation called for members of NATO to consider whether the North Atlantic Treaty applied to conflicts conducted entirely in the cyber domain. To that end, the center invited an "International Group of Experts" to debate and discuss the applicable laws of armed conflict and how they might be adapted to cyber warfare. The *Tallinn Manual*, which has subsequently been revised and expanded, was the first major attempt by the center to codify how the laws of warfare in the physical domain might apply in the digital realm.

DOCUMENT

Rule 5—Control of cyber infrastructure
A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.

1. This Rule establishes a standard of behaviour for States in relation to two categories of cyber infrastructure. (i) any cyber infrastructure (governmental or not in nature) located on their territory; and (ii) cyber infrastructure located elsewhere but over which the State in question has either de jure or de facto exclusive control. It applies irrespective of the attributability of the acts in question to a State (Rules 6 and 7).
2. The principle of sovereign equality entails an obligation of all States to respect the territorial sovereignty of other States. As the International Court of Justice held in the *Nicaragua* judgment, "Between independent States, respect for territorial sovereignty is an essential foundation of international relations."

3. The obligation to respect the sovereignty of another State, as noted in the International Court of Justice's *Corfu Channel* judgment, implies that a State may not "allow knowingly its territory to be used for acts contrary to the rights of other States." Accordingly, States are required under international law to take appropriate steps to protect those rights. This obligation applies not only to criminal acts harmful to other States, but also, for example, to activities that inflict serious damage, or have the potential to inflict such damage, on persons and objects protected by the territorial sovereignty of the target State.
4. These requirements are complicated by the nature of harmful cyber acts, especially time and space compression, and their often-unprecedented character. There may be circumstances in which it is not feasible for a State to prevent injury to another State. For example, State A may know that a harmful cyber attack is being prepared and will be launched from its territory against State B. However, because it has not identified the attack's exact signature and timing, the only effective option may be to isolate the network that will be used in the attack from the internet. Doing so will often result in a "self-denial" of service to State A. The nature, scale, and scope of the (potential) harm to both States must be assessed to determine whether this remedial measure is required. The test in such circumstances is one of reasonableness.
5. As to scope of application, this Rule covers all acts that are unlawful and that have detrimental effects on another State (whether those effects occur on another State's territory or on objects protected by international law). The term "unlawful" is used in this Rule to denote an activity that is contrary to the legal rights of the affected State. The International Group of Experts deliberately chose not to limit the prohibition to narrower concepts, such as the use of force (Rule 11) or armed attack (Rule 13), in order to emphasize that the prohibition extends to all cyber activities from one State's territory that affect the rights of other States and have detrimental effects on another State's territory. In particular, there is no requirement that the cyber operation in question result in physical damage or injuries to individuals; it need only produce a negative effect.
6. The Rule addresses a situation in which the relevant acts are underway. For instance, a State that allows cyber infrastructure on its territory to be used by a terrorist group to undertake an attack against another State

DID YOU KNOW?

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

In the aftermath of the Russia-Estonia cyber conflict of 2007, NATO members agreed for the need to create a centralized organization to train and educate personnel on the capabilities of cyber warfare. Centres of Excellence (COE) are designed to allow member states to pool their information, making the entire alliance more efficient in its processes and procedures. Strangely, despite being tied to NATO, they are not part of its command structure, and are not funded by NATO, they are instead sponsored by member states interested in participation. Estonia, one of the most internet-dependent nations of the alliance, first proposed a COE for cyber operations in 2005, believing such an effort represented a significant way to enhance the small nation's value to NATO. In 2008, Germany, Italy, Latvia, Lithuania, the Slovak Republic, and Spain agreed to serve as sponsoring nations. In the decade that followed, they were joined by the Czech Republic, France, Greece, Hungary, Poland, Turkey, the United Kingdom, and the United States. In 2013, the CCDCOE issued the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, effectively establishing NATO's position on the roles and responsibilities of cyber combatants in modern conflicts.

would be in violation of this Rule, as would a State that, upon notification by another State that this activity is being carried out, fails to take reasonably feasible measures to terminate the conduct.

7. The International Group of Experts could not agree whether situations in which the relevant acts are merely prospective are covered by this Rule. Some of the Experts took the position that States must take reasonable measures to prevent them. Others suggested that no duty of prevention exists, particularly not in the cyber context given the difficulty of mounting comprehensive and effective defences against all possible threats.
8. This Rule also applies with regard to acts contrary to international law launched from cyber infrastructure that is under the exclusive control of a government. It refers to situations where the infrastructure is located outside the respective State's territory, but that State nevertheless exercises exclusive control over it. Examples include a military installation in a foreign country subject to exclusive sending State control pursuant to a basing agreement, sovereign platforms on the high seas or in international airspace, or diplomatic premises.
9. This Rule applies if the relevant remedial cyber operations can be undertaken by State organs or by individuals under State control. The International Group of Experts also agreed that if a remedial action could only be provided by a private entity, such as a private internet service provider, the State would be obliged to use all means at its disposal to require that entity to take the action necessary to terminate the activity.
10. The Rule applies if the State has actual knowledge of the acts in question. A State will be regarded as having actual knowledge if, for example, State organs such as its intelligence agencies have detected a cyber attack originating from its territory or if the State has received credible information (perhaps from the victim State) that a cyber attack is underway from its territory.
11. The International Group of Experts could not achieve consensus as to whether this Rule also applies if the respective State has only constructive ("should have known") knowledge. In other words, it is unclear whether a State violates this Rule if it fails to use due care in policing cyber activities on its territory and is therefore unaware of the acts in question. Even if constructive knowledge suffices, the threshold of due care is uncertain in the cyber context because of such factors as the difficulty of attribution, the challenges of correlating separate sets of events as part of a coordinated and distributed attack on one or more targets, and the case with which deception can be mounted through cyber infrastructure.
12. Nor could the International Group of Experts achieve consensus as to whether this Rule applies to States through which cyber operations are routed. Some Experts took the position that to the extent that a State of transit knows of an offending operation and has the ability to put an end to it, the State must do so. These Experts took notice, however, of the unique routing processes of cyber transmissions. For instance, should

a transmission be blocked at one node of a network, it will usually be rerouted along a different transmission path, often through a different State. In such a case, these Experts agreed that the State of transit has no obligation to act, because doing so would have no meaningful effect on the outcome of the operation. Other Experts took the position that the Rule applied only to the territory of the State from which the operation is launched or to territory under its exclusive control. They either argued that the legal principle did not extend to other territory *in abstracto* or justified their view on the basis of the unique difficulties of applying the Rule in the cyber context.

13. If a State fails to take appropriate steps in accordance with this Rule, the victim State may be entitled to respond to that violation of international law by resorting to proportionate responses. These may include, where appropriate in the circumstances, countermeasures (Rule 9) or the use of force in self-defence (Rule 13).
14. With regard to such situations during an international armed conflict, see Rule 94.

. . .

Rule 20—Applicability of the law of armed conflict. Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict.

1. The law of armed conflict applies to cyber operations as it would to any other operations undertaken in the context of an armed conflict. Despite the novelty of cyber operations and the absence of specific rules within the law of armed conflict explicitly dealing with them, the International Group of Experts was unanimous in finding that the law of armed conflict applies to such activities in both international and non-international armed conflicts (Rules 22 and 23).
2. A condition precedent to the application of the law of armed conflict is the existence of an armed conflict. The term "armed conflict" was first used in a law of war codification in the 1949 Geneva Conventions, but has never been authoritatively defined as a matter of treaty law. It has today replaced the term "war" for law of armed conflict purposes. As used in this Manual, armed conflict refers to a situation involving hostilities, including those conducted using cyber means. The term takes on a different meaning for the purposes of characterizing international and non-international armed conflict. Rules 22 and 23 discuss the extent of hostilities required to reach those thresholds.
3. To illustrate, in 2007 Estonia was the target of persistent cyber operations. However, the law of armed conflict did not apply to those cyber operations because the situation did not rise to the level of an armed conflict. By contrast, the law of armed conflict governed the cyber operations that occurred during the international armed conflict between Georgia and Russia in 2008 because they were undertaken in furtherance of that conflict. The latter case illustrates that in a situation of on-going kinetic

hostilities amounting to an armed conflict, the applicable law of international or non-international armed conflict will govern cyber operations undertaken in relation to that conflict. The precise aspects of the law of armed conflict that apply depend on whether the conflict is international or non-international in character.

4. The term "cyber operations" includes, but is not limited to, "cyber attacks" (Rule 30). As used in this Manual, cyber attacks is a term of art referring to a specific category of cyber operations. Certain types of cyber operations, such as those affecting the delivery of humanitarian assistance (Rule 86) are governed by the law of armed conflict even when those operations do not rise to the level of an "attack."
5. The International Group of Experts adopted the phrase "in the context of an armed conflict" as a compromise formula with respect to the scope of the law of armed conflict. All members of the International Group of Experts agreed that there must be a nexus between the cyber activity and the armed conflict for the law of armed conflict to apply to the activity in question. However, they differed as to the nature of that nexus. According to one view, the law of armed conflict governs any cyber activity conducted by a party to an armed conflict against its opponent (note, in this regard, the discussion on attributability in the Commentary to Rule 22). According to the second view, the cyber activity must have been undertaken in furtherance of the hostilities, that is, in order to contribute to the originator's military effort. Consider a cyber operation conducted by State A's Ministry of Trade against a private corporation in enemy State B in order to acquire commercial secrets during an armed conflict. According to the first view, the law of armed conflict would govern that operation because it is being conducted by a party to the armed conflict against a corporation of the enemy State. Those Experts adopting the second view considered that the law of armed conflict does not apply because the link between the activity and the hostilities is insufficient.
6. The International Group of Experts noted that the precise parameters of the phrase 'in the context of' are less clear in a non-international armed conflict. This is because a State retains certain law enforcement obligations and rights with respect to its territory in which the hostilities are taking place, notwithstanding the armed conflict. To the extent that it is involved in purely law enforcement activities, domestic and human rights law, not the law of armed conflict, apply.
7. The law of armed conflict does not embrace activities of private individuals or entities that are unrelated to the armed conflict. Take, for example, the case of a private corporation that is engaged in theft of intellectual property to achieve a market advantage over a competitor in the enemy State. In principle, the law of armed conflict does not govern such activity.
8. The applicability of the law of armed conflict does not depend upon the qualification of the situation under *jus ad bellum* (Chapter 2). Pursuant to the principle of equal application of the law of armed conflict, even a

resort to armed force that is unlawful from the perspective of *jus ad bellum* is subject to the law of armed conflict.

9. It should be noted that the application of the law of armed conflict to cyber operations can prove problematic. It is often difficult to identify the existence of a cyber operation, its originator, its intended object of attack, and its precise effects. Still, these questions of fact do not prejudice the application of the law of armed conflict.
10. To the extent an express rule of the law of armed conflict does not regulate cyber activities, regard should be had to the Martens Clause, found in Hague Convention IV, the 1949 Geneva Conventions, and Additional Protocol I. The text in Hague Convention IV provides that:

    > Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience.

To the extent that cyber activities are conducted in the course of an armed conflict, the Martens Clause, which reflects customary international law, functions to ensure that such activities are not conducted in a legal vacuum. This point is without prejudice to the disputed question of the applicability of human rights law during armed conflict.

. . .

Rule 28—Mercenaries. Mercenaries involved in cyber operations do not enjoy combatant immunity or prisoner of war status.

1. Article 47(1) of Additional Protocol I reflects a customary international law rule that mercenaries, including those engaged in cyber operations, are unprivileged belligerents. As the notions of combatant status and belligerent immunity do not apply in non-international armed conflict, this Rule has no relevance to non-international armed conflict.
2. The most widely accepted definition of mercenary is found in Article 47(2) of Additional Protocol I. It sets forth six conditions that must be cumulatively fulfilled: special recruitment; direct participation in hostilities; desire for private gain as a primary motivation; neither a national of a party to the conflict nor a resident of territory controlled by a party; not a member of the armed forces of a party to the conflict; and not sent by another State on official duty as a member of its armed forces. For example, consider a private company located in State A that is engaged by State B to conduct cyber operations on its behalf in its armed conflict with State C. So long as the six criteria are fully met, its employees who conduct the cyber operations are mercenaries, and thus unprivileged belligerents.

The same would be true with regard to a "hacker for hire" who meets the criteria, even if operating alone and far from the battlefield.

3. It is clear that no person qualifying as a mercenary enjoys combatant status. This is especially important in light of the criminalization of mercenarism by many States.

. . .

Rule 30—Definition of cyber attack. A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.

1. For the purposes of the Manual, this definition applies equally to international and non-international armed conflict.
2. The notion of "attack" is a concept that serves as the basis for a number of specific limitations and prohibitions in the law of armed conflict. For instance, civilians and civilian objects may not be "attacked" (Rule 32). This Rule sets forth a definition that draws on that found in Article 49(1) of Additional Protocol I: "attacks means acts of violence against the adversary, whether in offence or defence." By this widely accepted definition, it is the use of violence against a target that distinguishes attacks from other military operations. Non-violent operations, such as psychological cyber operations or cyber espionage, do not qualify as attacks.
3. "Acts of violence" should not be understood as limited to activities that release kinetic force. This is well settled in the law of armed conflict. In this regard, note that chemical, biological, or radiological attacks do not usually have a kinetic effect on their designated target, but it is universally agreed that they constitute attacks as a matter of law. The crux of the notion lies in the effects that are caused. To be characterized as an act of violence, an action must result in the consequences set forth in this Rule, which are explained below. Restated, the consequences of an operation, not its nature, are what generally determine the scope of the term "attack"; "violence" must be considered in the sense of violent consequences and is not limited to violent acts. For instance, a cyber operation that alters the running of a SCADA system controlling an electrical grid and results in a fire qualifies. Since the consequences are destructive, the operation is an attack.
4. All members of the International Group of Experts agreed that the type of consequential harm set forth in this Rule qualifies an action as an attack, although, as discussed below, there are nuances to its application. The text of numerous Articles of Additional Protocol I, and the ICRC commentary thereto, supports this conclusion. For instance, Article 51(1) sets forth the general principle that the "civilian population and individual civilians shall enjoy general protection against *dangers* arising from military operations." Other Articles provide further support. The rules of proportionality speak of "*loss* of civilian life, *injury* to civilians, *damage* to

civilian objects, or a combination thereof." Those relating to protection of the environment refer to "widespread, long-term, and severe *damage*," and the protection of dams, dykes, and nuclear electrical generating stations is framed in terms of "severe *losses* among the civilian population." The Experts agreed that *de minimis* damage or destruction does not meet the threshold of harm required by this Rule.

5. The word "cause" in this Rule is not limited to effects on the targeted cyber system. Rather, it encompasses any reasonably foreseeable consequential damage, destruction, injury, or death. Cyber attacks seldom involve the release of direct physical force against the targeted cyber system; yet, they can result in great harm to individuals or objects. For example, the release of dam waters by manipulating a SCADA system could cause massive downstream destruction without damaging the system. Were this operation to be conducted using kinetic means, like bombing the dam, there is no question that it would be regarded as an attack. No rationale exists for arriving at a different conclusion in the cyber context.
6. Although the Rule is limited to operations against individuals or physical objects, the limitation should not be understood as excluding cyber operations against data (which are non-physical entities) from the ambit of the term attack. Whenever an attack on data results in the injury or death of individuals or damage or destruction of physical objects, those individuals or objects constitute the "object of attack" and the operation therefore qualifies as an attack. Further, as discussed below, an operation against data upon which the functionality of physical objects relies can sometimes constitute an attack.
7. The phrase "against the adversary" in Article 49(1) could cause confusion by suggesting that destructive operations must be directed at the enemy to qualify as attacks. The International Group of Experts agreed that such an interpretation would make little sense in light of, for instance, the prohibition on attacking civilians and civilian objects. The Experts agreed that it is not the status of an action's target that qualifies an act as an attack, but rather its consequences. Therefore, acts of violence, or those having violent effects, directed against civilians or civilian objects, or other protected persons or objects, are attacks.
8. While the notion of attack extends to injuries and death caused to individuals, it is, in light of the law of armed conflict's underlying humanitarian purposes, reasonable to extend the definition to serious illness and severe mental suffering, that are tantamount to injury. In particular, note that Article 51(2) of Additional Protocol I prohibits "acts or threats of violence the primary purpose of which is to spread terror among the civilian population." Since terror is a psychological condition resulting in mental suffering, inclusion of such suffering in this Rule is supportable through analogy.
9. With regard to digital cultural property, see the Commentary accompanying Rule 82.

10. Within the International Group of Experts, there was extensive discussion about whether interference by cyber means with the functionality of an object constitutes damage or destruction for the purposes of this Rule. Although some Experts were of the opinion that it does not, the majority of them were of the view that interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components. Consider a cyber operation that is directed against the computer-based control system of an electrical distribution grid. The operation causes the grid to cease operating. In order to restore distribution, either the control system or vital components thereof must be replaced. The cyber operation is an attack. Those experts taking this position were split over the issue of whether the "damage" requirement is met in situations where functionality can be restored by reinstalling the operating system.
11. A few Experts went so far as to suggest that interference with functionality that necessitates data restoration, while not requiring physical replacement of components or reinstallation of the operating system, qualifies as an attack. For these Experts, it is immaterial how an object is disabled; the object's loss of usability constitutes the requisite damage.
12. The International Group of Experts discussed the characterization of a cyber operation that does not cause the type of damage set forth above, but which results in large-scale adverse consequences, such as blocking email communications throughout the country (as distinct from damaging the system on which transmission relies). The majority of the Experts took the position that, although there might be logic in characterizing such activities as an attack, the law of armed conflict does not presently extend this far. A minority took the position that should an armed conflict involving such cyber operations break out, the international community would generally regard them as attack. All Experts agreed, however, that relevant provisions of the law of armed conflict that address situations other than attack, such as the prohibition on collective punishment (Rule 85), apply to these operations.
13. It should be noted that a cyber operation might not result in the requisite harm to the object of the operation, but cause foreseeable collateral damage at the level set forth in this Rule. Such an operation amounts to an attack to which the relevant law of armed conflict applies, particularly that regarding proportionality (Rule 51).
14. A cyber operation need not actually result in the intended destructive effect to qualify as an attack. During the negotiation of Additional Protocol I the issue of whether laying land mines constituted an attack arose. The "general feeling" of the negotiators was that "there is an attack whenever a person is directly endangered by a mine laid." By analogy, the introduction of malware or production-level defects that are either time-delayed or activate on the occurrence of a particular event is an attack when the intended consequences meet the requisite threshold of harm. This is so irrespective of whether they are activated. Some members took

the position that although there is no requirement that the cyber operation be successful, an attack only transpires once the malware is activated or the specified attack occurs.

15. An attack that is successfully intercepted and does not result in actual harm is still an attack under the law of armed conflict. Thus, a cyber operation that has been defeated by passive cyber defences such as firewalls, anti-virus software, and intrusion detection or prevention systems nevertheless still qualifies as an attack if, absent such defences, it would have been likely to cause the requisite consequences.
16. Cyber operations may be an integral part of a wider operation that constitutes an attack. As an example, a cyber operation may be used to disable defences at a target that is subsequently kinetically attacked. In such a case, the cyber operation is one component of an operation that qualifies as an attack, much as laser designation makes possible attacks using laser-guided bombs. The law of armed conflict on attacks applies fully to such cyber operations.
17. If an attack is conducted against civilians or civilian objects in the mistaken but reasonable belief that they constitute lawful targets, an attack has nonetheless occurred. However, if the attacker has fully complied with the requirement to verify the target (Rule 53), the attack will be lawful.
18. It may be the case that the target of a cyber attack does not realize it has been attacked. For instance, a cyber attack directed against civilian infrastructure may be designed to appear as if the ensuing damage resulted from simple mechanical malfunction. The fact that a cyber attack is not recognized as such has no bearing on whether it qualifies as an attack and is subject to the law of armed conflict thereon.
19. Care is required when identifying the originator of an attack. To illustrate, an individual may receive an email with an attachment containing malware. Execution of the malware, which occurs automatically upon opening, will cause the requisite level of harm. If that individual unwittingly forwards the email and it does cause such harm, he or she will not have conducted an attack; the email's originator will have done so. By contrast, if the intermediary forwards the email knowing it contains the malware, both individuals will have conducted an attack.

. . .

Rule 66—Cyber Espionage. (a) Cyber espionage and other forms of information gathering directed at an adversary during an armed conflict do not violate the law of armed conflict. (b) A member of the armed forces who has engaged in cyber espionage in enemy-controlled territory loses the right to be a prisoner of war and may be treated as a spy if captured before re-joining the armed forces to which he or she belongs.

1. The formulation of this Rule is based on customary international law, Articles 29 and 31 of the Hague Regulations, and Article 46 of Additional

Protocol I. (b) applies only in international armed conflict because the concept of espionage is limited to inter-State relations and because the notions of prisoner of war status and combatant immunity have no application in non-international armed conflicts.

2. For the purposes of this Manual, "cyber espionage" is defined narrowly as any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party. The act must occur in territory controlled by a party to the conflict. "Clandestinely" refers to activities undertaken secretly or secretively, as with a cyber espionage operation designed to conceal the identity of the persons involved or the fact that it has occurred. An act of cyber information collection is "under false pretences" when so conducted as to create the impression that the individual concerned is entitled to access the information in question. In the cyber domain, it often consists of an individual masquerading as a legitimate user by employing that user's permissions to access targeted systems and data.
3. Cyber espionage must be distinguished from computer network exploitation (CNE), which is a doctrinal, as distinct from an international law, concept. CNE often occurs from beyond enemy territory, using remote access operations. Cyber operators sometimes also use the term "cyber reconnaissance." The term refers to the use of cyberspace capabilities to obtain information about enemy activities, information resources, or system capabilities. CNE and cyber reconnaissance are not cyber espionage, when conducted from outside enemy-controlled territory.
4. Although there is no express prohibition on cyber espionage in the law of armed conflict (or international law more generally), it is subject to all prohibitions set forth in that body of law. For instance, cyber espionage can in some circumstances violate the prohibition on perfidy (Rule 60). Such conduct may also amount to "direct participation in hostilities" by any civilians involved, thereby rendering them subject to attack (Rule 35). Although cyber espionage, whether by civilians or members of the armed forces, does not violate international law, it may violate the domestic law of States that enjoy jurisdiction over the individual or the offence.
5. Article 29 of the Hague Regulations employs the term "zone of operations of a belligerent." Article 46(2) of Additional Protocol I expands the geographical scope of the concept to any territory controlled by enemy forces. State practice supports this extension as a matter of customary international law. Given the geographic limitations to territory controlled by the enemy, cyber espionage will most likely occur as a close access cyber operation, such as when a flash drive is used to gain access to a computer system.
6. Cyber information gathering that is performed from outside territory controlled by the adverse party to the conflict is not cyber espionage but, in certain circumstances, may be punishable under the domestic criminal

law of the State affected or of the neutral State from which the activity is undertaken. However, since no cyber espionage is involved, belligerent immunity would attach when appropriate (Rule 26).

7. The International Group of Experts agreed that the information in question must be gathered on behalf of a party to the conflict. For example, it is not cyber espionage for the purposes of this Rule for a corporation located in the territory of a party to the conflict to use cyber means to surreptitiously gather information about the commercial activities of a corporation in the territory of another party to the conflict.
8. The majority of the International Group of Experts took the position that the nature of the information gathered has no bearing on the characterization of the activity as cyber espionage. By contrast, the minority agreed with the AMW Manual position that the information involved must be of some military value.
9. Certain acts of cyber espionage involve more than mere information-gathering activities and can cause damage to computer systems. Therefore, acts whose primary purpose is cyber espionage may sometimes amount to a cyber attack, in which case the Rules as to cyber attack apply (Chapter 4).
10. With respect to (b), it is well accepted that spies who are captured in enemy-controlled territory do not enjoy combatant immunity or prisoner of war status. However, a spy who, after re-joining the army to which he belongs, is subsequently captured by the enemy, is treated as a prisoner of war, and incurs no responsibility for his previous acts of spying. This provision applies to cyber espionage. Accordingly, if a member of the armed forces who has engaged in cyber espionage in enemy-controlled territory succeeds in re-joining his own forces, he or she is no longer liable to prosecution for those cyber espionage activities.

SOURCE: Group of International Experts, North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2010), 26–29, 75–79, 103–104, 106–110, 192–195, https://issuu.com/nato_ccd_coe/docs/tallinnmanual

ANALYSIS

The *Tallinn Manual* explains in extreme detail precisely how and why the existing laws of armed conflict apply in the cyber domain. It draws key distinctions regarding the actors, actions, and intents of cyber operations and relies upon much of the same logic and precedent as the existing laws of armed conflict. By expecting States to be held accountable for their actions, and those of their designated agents, the Manual establishes the precedent that the cyber domain is not unique regarding responsible behavior. Its treatment of mercenaries and spies is also particularly noteworthy, as in both cases, it demonstrates that these actors, who are often ancillary

to a nation's primary efforts in conflict, may operate in the cyber domain but should expect no more protections there than in the physical world. Although the Manual did not bind NATO members to any specific action, as it was expressly the work of the International Group of Experts, it did effectively become the guiding document for NATO members operating in the cyber domain, and as such, it is a key document in the history of cyber warfare.

- ***Document 60:*** *A Strong Britain in an Age of Uncertainty: The National Security Strategy*
- ***When:*** October 2010
- ***Where:*** London, United Kingdom
- ***Significance:*** In 2010, the United Kingdom released a national security strategy. It came after British troops had faced nearly a decade of war in Afghanistan and seven years of conflict in Iraq. The document placed terrorism as the highest threat to national security, an understandable position given that Britain was preparing to host the 2012 Summer Olympic Games. However, the second-highest security threat to Britain, according to the Ministry of Defence, came from international cyberattacks.

DOCUMENT

Risks to Our Security
The Highest Priority Risks
2. Cyber Attack

3.27 Like terrorism, this is not simply a risk for the future. **Government, the private sector and citizens are under sustained cyber attack today, from both hostile states and criminals.** They are stealing our intellectual property, sensitive commercial and government information, and even our identities in order to defraud individuals, organisations and the Government.

3.28 But in future, unless we take action, this threat could become even worse. For this reason, cyber security has been assessed as one of the highest priority national security risks to the UK. Cyberspace is already woven in to the fabric of our society. It is integral to our economy and our security and access to the internet, the largest component of cyberspace, is already viewed by many as the "fourth utility," a right rather than a privilege. In less than 15 years, the number of global web users has exploded by more than a hundred-fold, from 16 million in 1995 to more than 1.7 billion today.

3.29 While cyberspace provides the UK with massive opportunities, the risks emanating from our growing dependence on it are huge. By 2015, there will be more interconnected devices on the planet than humans—everything from mobile phones, cars and fridges will be networked across homes, offices and classrooms across the globe. Activity in cyberspace will continue to evolve as a direct national security and economic threat, as it is refined as a means of espionage and crime, and continues to grow as a terrorist enabler, as well as a military weapon for use by states and possibly others. But **getting our cyber security posture right across the full spectrum of activities is also a great opportunity for the UK** to capitalise on our national economic and security **comparative advantages**.

3.30 The internet provides great benefits for UK's industry, government and general populace, but as our dependency on it increases so do the risks and threats we face online:

- Modern UK national infrastructure, government and business depends more and more on information and communications technology and particularly the internet
- Cyber-crime has been estimated to cost as much as **$1 trillion per year globally**, with untold human cost. Major British companies are increasingly anxious about the impact of cybercrime on their bottom line and the resilience of the networks upon which commerce relies
- The Olympics will be an attractive target for criminals and others seeking to defraud and potentially disrupt. Beijing experienced **12 million cyber attacks per day** during the 2008 games
- Attacks in cyberspace can have a potentially devastating real-world effect. Government, military, industrial and economic targets, including critical services, could feasibly be disrupted by a capable adversary. "Stuxnet," a computer worm discovered in June 2010, was seemingly designed to target industrial control equipment. Although no damage to the UK has been done as a result, it is an example of the realities of the dangers of our interconnected world
- Terrorists use cyberspace to organise, communicate and influence those vulnerable to radicalisation.

3.31 But the UK already has some areas of comparative advantage in cyber-security, which we can use not just to mitigate the risk, but also to gain economic and security opportunities.

SOURCE: United Kingdom Ministry of Defence, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (United Kingdom: Her Majesty's

DID YOU KNOW?

Air Gapping

Air gapping is a technique commonly used to provide enhanced computer network security. It serves to isolate a computer or a network from any connection to the larger internet. This is considered absolutely vital for any computer or network containing classified information—but it is not an absolute protection against unauthorized intrusions as most air-gapped machines are still vulnerable to local penetrations through flash drives and other removable media. The computer network running the Iranian uranium enrichment program was air-gapped, yet still fell victim to the Stuxnet virus when an unknown person inserted a compromised flash drive into a computer on the network, accidentally uploading the malware that quickly spread through the entire system. Thus, air-gapping, while helpful, is not the only measure necessary to keep a network safe from malicious actors.

Stationery Office, 2010), 29–30, https://webarchive.nationalarchives.gov.uk/20121018134855/http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf. Contains public sector information licensed under the Open Government Licence v3.0.

ANALYSIS

The British emphasis upon cyberattacks as a source of concern, particularly those conducted by other states, is unsurprising given the amount of damage such attacks had already caused in Britain. The national strategy makes the important (and accurate) prediction that such attacks would only increase in the future and that the sooner the government and military took action to create cybersecurity plans, the less painful the net effect of cyberattacks would be. It is important to note that the security strategy effectively places the responsibility for defending the entire nation, including private entities, under the government, and especially the military. In this regard, the British strategy is a significant departure from contemporary American documents, which made rudimentary calls for partnership between the public and private sectors but also made certain not to offer even the hint that the government might accept responsibility for the entire cyber defense mission.

- ***Document 61:*** *Cyber Warfare*
- ***When:*** October 29, 2010
- ***Where:*** Geneva, Switzerland
- ***Significance:*** In many ways, the International Committee of the Red Cross serves as the "referee" during open conflicts around the globe. It, and its partner organizations, have a unique status during warfare, maintained by a strict neutrality and a desire to mitigate the worst aspects of national conflicts. The Red Cross often serves as the "protecting power" for prisoners of war, which entails maintaining lines of communication between prisoners and their home governments, inspecting prisoner of war camps, and recording any abuses or atrocities committed by belligerents against prisoners. By offering perspectives on how newly developed cyber weapons might be governed by the existing laws of armed conflict, the Red Cross effectively provided a neutral explanation of the limits of belligerents in the cyber domain.

DOCUMENT

Lawyers and technical experts agree that the potential of computer network attacks is considerable, raising questions about the application of international humanitarian law and even the definition of "armed conflict" itself.

There is no specific mention of cyber warfare or computer network attacks in the Geneva Conventions or their Additional Protocols. But the principles and rules in these treaties governing the means and methods of warfare are not restricted to situations that existed at the time of their adoption. IHL clearly anticipated advances in weapons' technology and the development of new means and methods of waging war.

There can be no doubt, therefore, that international humanitarian law covers cyber warfare. In particular IW's potential to threaten and harm civilians and their means of survival during armed conflict brings it directly into the realm of IHL.

The idea of cyber warfare or computer network attack in armed conflict is very new. So much so that the discussion about its potential impact is often speculative. Cyber warfare has been defined as any hostile measures against an enemy designed "to discover, alter, destroy, disrupt or transfer data stored in a computer, manipulated by a computer or transmitted through a computer." Examples of hostile use include computer attacks on air traffic control systems, on oil pipeline flow systems and nuclear plants.

Under IHL such attacks must not be indiscriminate. They must distinguish between military targets and civilians and be proportionate and justified by military gain. In this respect, cyber warfare techniques are little different from other means of warfare.

The fact that a computer network attack during an armed conflict is not kinetic, physical or violent in itself, does not put it beyond the remit of IHL. As with other means and methods of warfare, computer network attacks against combatants and military objectives are legal as long as they are consistent with humanitarian law. However, computer network attacks open up new questions since they can be used, for example, against the enemy's production, distribution and banking systems, making the impact more difficult to judge.

The IHL principle that civilians should be protected and their livelihoods and the environment in which they live should not be targeted, provides basic guidance when faced with these new methods of warfare.

Cyber warfare adds a new level of complexity to armed conflict that may pose novel questions for IHL. As a result IHL's relevance needs to be reaffirmed as the principal body of law that can regulate such warfare. The norms in international humanitarian law covering such issues as the use of indiscriminate weapons, distinction between military targets and civilians, proportionality and perfidy, can and must be applied also to cyber warfare.

SOURCE: International Committee of the Red Cross, *Cyber Warfare*, October 29, 2010, https://www.icrc.org/en/document/cyber-warfare. Used by permission of the International Committee of the Red Cross.

ANALYSIS

As this short article makes clear, the Red Cross position is that cyber warfare is not inherently unique, nor is it exempt from the principles of international humanitarian law. Just as kinetic weapons must be used in a discriminate and proportionate fashion, without targeting civilian populations or their livelihoods, so must belligerents govern their use of cyber weapons. Essentially, the Red Cross is staking out the position that cyber warfare has little or no difference from other forms of conflict, so far as humanitarian law is concerned, even if the means by which its attacks are conducted differ from those of more traditional forms of warfare. As such, the Red Cross suggests that there is no inherent need to create new legal provisions for cyber warfare, as the existing framework should apply in the cyber domain.

- ***Document 62:*** *National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace*
- ***When:*** May 2012
- ***Where:*** Athens, Greece
- ***Significance:*** The European Union offers tremendous potential for collective action in the areas of economic, military, and diplomatic sources of national power. However, member states of the European Union have often struggled with many aspects of mutual defense, and the cyber domain is no exception. This document illustrates the variety of approaches different states have taken with regard to cybersecurity and then offers some conclusions and recommendations for collective action in the cyber domain.

DOCUMENT

Evolution of Cyber Strategies of EU Member States

The first national cyber security strategies began to appear during the first years of the previous decade. One of the first countries to recognise cyber security as a national strategic matter was the United States. In 2003 they published the National Strategy to Secure Cyberspace. It was a part of the overall National Strategy for Homeland Security, which was developed in response to the terrorist attacks on September 11th 2001.

Developed for similar reasons, action plans and strategies with limited focus began to spring up across Europe in the following years. In 2005, Germany adopted the "National Plan for Information Infrastructure Protection (NPSI)." The following year, Sweden developed a "Strategy to improve Internet security in Sweden."

Following the severe cyber-attack on Estonia in 2007, the country was the first EU Member State to publish a broad national cyber security strategy in 2008. Since then considerable work has been done in this area on a national level and in the last four years, ten EU Member States have published a national cyber security strategy. These are briefly summarised below. Across the EU there are also several Member States which are currently developing strategies—and some are very far in the process, close to publication. In addition, a few more EU Member States have unofficial or informal NCSS.

- ***Estonia*** (2008): Estonia emphasizes the necessity of a secure cyberspace in general and focuses on information systems. The recommended measures are all of a civil character and concentrate on regulation, education and cooperation.
- ***Finland*** (2008): The basis of the strategy is a view of cyber security as a data security issue and as a matter of economic importance that is closely related to the development of the Finnish information society.
- ***Slovakia*** (2008): Ensuring information security is viewed as being essential to the functioning and development of society. Therefore the purpose of the strategy is to develop a comprehensive framework. The strategic objectives of the strategy are mainly focused on prevention as well as readiness and sustainability.
- ***Czech Republic*** (2011): Essential objectives of the cyber security strategy include protection against threats which information and communication systems and technologies are exposed to, and mitigation of potential consequences in the event of an attack against ICTs. The strategy focuses mainly on unimpeded access to services, data integrity and confidentiality of the Czech Republic's cyberspace and is coordinated with other related strategies and concepts.
- ***France*** (2011): France focuses on the enablement of information systems to resist events in cyberspace which could compromise the availability, integrity or confidentiality of data. France stresses both technical means related to the security of information systems and the fight against cybercrime and the establishment of a cyber-defence.
- ***Germany*** (2011): Germany focuses on preventing and prosecuting cyber-attacks and also on the prevention of coincident IT failures, especially where critical infrastructures are concerned. The strategy sets the ground for the protection of critical information structures. It explores existing regulations to clarify whether, and if so, where additional powers are required to secure IT systems in Germany by means of providing basic security functions certified by the state and also supporting SMEs by setting up a new task force.
- ***Lithuania*** (2011): Lithuania aims to determine the objectives and tasks for the development of electronic information in order to ensure the confidentiality, integrity and accessibility of electronic information and services provided in cyberspace; safeguarding of electronic communication networks, information systems and critical information infrastructure against incidents and cyber-attacks; protection of personal data and privacy. The strategy also

defines the tasks, which when implemented would allow total security of cyberspace and entities operating in it.

- ***Luxembourg*** (2011): Recognising the pervasiveness of ICTs, the strategy states that it is a priority to prevent any adverse effects on health and public safety or on the economy. It also mentions the importance of ICTs for citizens, society and for economic growth. The strategy is based on five action lines. These can briefly be summarised as CIIP and incident response; modernizing the legal framework; national and international cooperation; education and awareness; and promoting standards.
- ***Netherlands*** (2011): The Netherlands aims towards safe and reliable ICTs and fears abuse and (large-scale) disruption—and at the same time acknowledges the need to protect the openness and freedom of the internet. The Netherlands include a definition of cyber security in the strategy: "Cyber security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information."
- ***UK*** (2011): The UK approach is concentrating on the national objectives linked to evolving cyber security: making the UK the major economy of innovation, investment and quality in the field of ICT and by this to be able to fully exploit the potential and benefits of cyberspace. The objective is to tackle the risks from cyberspace like cyber-attacks from criminals, terrorists and states in order to make it a safe space for citizens and businesses.

. . .

Conclusions and Recommendations

In an environment with constantly emerging and evolving cyber threats, EU Member States would greatly benefit from flexible and dynamic cyber security strategies to meet new, global threats. The cross-border nature of threats makes it essential to focus on strong international cooperation. Cooperation at pan-European level is necessary to effectively prepare, but also respond to cyberattacks. Comprehensive national cyber security strategies are the first step in this direction.

We make the following recommendations to the Member States:

In the short-term:

- Develop, re-evaluate and maintain a National Cyber Security Strategy as well as action plans within the framework of the strategy.
- Clearly state the scope and objectives of the strategy as well as the definition of cyber security used in the strategy.
- Ensure that input and concerns from across governmental departments, national regulatory authorities and other public bodies are heard and addressed.
- Ensure the input and engagement of industry, academia and citizen representatives.

- Collaborate with other Member States and with the European Commission to ensure that the cross-border and global nature of cyber security are addressed in a coherent fashion.
- Recognise that the constant development and evolution of cyberspace and cyber security issues means that the strategy will have to be a living document.
- Be aware that the above point does not just mean emerging threats and new risks, but also opportunities to improve and enhance the use of information and communication technologies for government, industry and citizens.
- Ensure that strategies recognise and take account of the work that has been done to date in improving the level of security of national and pan European CIIP, by avoiding duplication of effort and concentrating on new challenges.
- Support the EU Commission in the definition of the Internet Security Strategy.

In the long-term:

- Agree on a commonly accepted working definition of cyber security that is precise enough to support the definition of common goals across the EU.
- Ensure that the cyber security strategies of the EU and of its Member States do not conflict with the goals of the international community, but rather support the efforts to tackle cyber security challenges globally.

The public and the private sector should work closely together to implement these cyber security strategies. This should be done through sharing of information, deployment of good practices (e.g. on incident reporting and handling) and through national exercises and pan-European exercises.

To assist the Commission and the Member States in this important task ENISA is developing a Good Practice Guide. This will present good practices and recommendations on how to develop, implement and maintain a national cyber security strategy. The Good Practice Guide is intended to be a useful tool and practical advice for those, such as regulators and policy makers, responsible for and involved in cyber security strategies. The guide is being developed in collaboration with public and private stakeholders from across Europe with participation of a few international stakeholders to expand on the intermediate analysis and recommendations from ENISA as presented in this paper.

SOURCE: European Network and Information Security Agency, *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace* (Athens, Greece: European Network and Information Security Agency, 2012), 5–6, 12–13, https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

ANALYSIS

By demonstrating the incredible variety of cybersecurity strategies undertaken by member states, the European Network and Information Security Agency effectively

illustrated the enormity of its task to the full membership of the European Union. Trying to create mutually interoperable network systems is a monumental challenge, finding a way to protect them might be a truly impossible goal. Given the disparate national interests of member states, and the unwillingness or inability of some states to contribute meaningfully to the cyber defense mission, this task is likely to create vexing problems for the foreseeable future. Because computer networks are only as secure as their weakest links, any effort to unify European cyber defense begins with substantial handicaps, as there are some states that are incredibly vulnerable to external attack. Network connections to those states would have the effect of rendering the entire European Union open to the same cyberattacks, something that the most economically developed states are unlikely to allow without substantial evidence of enhanced security consciousness and capability from all member states.

- ***Document 63:*** *Cyberwarfare and International Humanitarian Law: The ICRC's Position*
- ***When:*** 2013
- ***Where:*** Geneva, Switzerland
- ***Significance:*** An expansion of the ICRC's original position regarding cyberwar, this article gives a much broader explanation of how the cyber domain is governed by existing humanitarian law, despite seeming on the surface to be an inherently new and different form of conflict. By continuing to revise and expand its position that cyber conflict is contained within the broader nature of warfare, the Red Cross continued to offer a neutral opinion that might inform the digital behavior of actors in the cyber domain.

DOCUMENT

Cyberwarfare and international humanitarian law: the ICRC's position
What limits does the law of war impose on cyber attacks?

Does cyber warfare have limits and rules? Are civilian computers, networks and cyber infrastructure protected against cyber attacks? A group of international legal and military experts says "yes" in the recently published Tallinn Manual[1], a process in which the ICRC took part as an observer. Laurent Gisel, legal adviser at the

[1] *Tallinn Manual on the International Law Applicable to Cyber Warfare*—prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2013.

ICRC, explains why the Tallinn Manual is an important step towards underscoring the relevance of international humanitarian law (IHL) in armed conflicts of every kind, with the aim of reducing human suffering.

Why is the ICRC concerned by cyber warfare?

The expression "cyber warfare" appears to have been used by different people to mean different things. The term is used here to refer to means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL. The ICRC is concerned about cyber warfare because of the vulnerability of cyber networks and the potential humanitarian cost of cyber attacks. When the computers or networks of a State are attacked, infiltrated or blocked, there may be a risk of civilians being deprived of basic essentials such as drinking water, medical care and electricity. If GPS systems are paralysed, there may be a risk of civilian casualties occurring—for example, through disruption to the flight operations of rescue helicopters that save lives. Dams, nuclear plants and aircraft control systems, because of their reliance on computers, are also vulnerable to cyber attack. Networks are so interconnected that it may be difficult to limit the effects of an attack against one part of the system without damaging others or disrupting the whole system. The well-being, health and even lives of hundreds of thousands of people could be affected. One of the ICRC's roles is to remind all parties to a conflict that constant care must be taken to spare civilians. Wars have rules and limits, which apply just as much to the use of cyber warfare as to the use of rifles, artillery and missiles.

A group of legal and military experts recently published a manual—known as the Tallinn Manual—stating that IHL applies to cyber warfare and setting out how the rules of IHL will play out in this area. Why is that important?

We welcome the fact that experts are thinking about the consequences of cyber warfare and the law applicable to it. The use of cyber operations in armed conflict can potentially have devastating humanitarian consequences. For the ICRC, it is crucial to identify ways of limiting the humanitarian cost of cyber operations and, in particular, to reaffirm the relevance of IHL to this new technology when used in armed conflict. This is precisely what the experts say in the Tallinn Manual. Means and methods of war evolve over time, and are clearly not the same as the ones available when the Geneva Conventions were drafted in 1949; but IHL continues to apply to all activities conducted by parties in the course of armed conflict, and must be respected. It cannot be ruled out, however, that there might be a need to develop the law further to ensure it provides sufficient protection to the civilian population, as cyber technologies evolve or their humanitarian impact is better understood. That will have to be determined by States.

While the Tallinn Manual is a non-binding document prepared by a group of experts, we certainly hope that it can usefully contribute to further discussion among States on these challenging issues, and that States and non-State armed groups will ensure that any use of cyber operations in armed conflict will be in accordance with their international obligations. There is currently much debate about how international law, including IHL, should be interpreted and how it should apply to State

and non-State activities occurring in cyberspace. The ICRC will continue to offer its expertise in IHL to address these challenges.

This does not mean that IHL applies to any cyber operation or to all those that are often called "cyber attacks" in common parlance: IHL does not regulate cyber operations that fall outside a situation of armed conflict. Business corporations and governments are as much concerned by cyber espionage, cyber crimes, and other malicious cyber activity as they are by cyber attacks that would fall under IHL. The technical means of protecting cyber infrastructure from espionage or from an attack might be similar, but the law governing these operations is not. One of the key issues is therefore to identify the circumstances in which cyber operations may be regarded as occurring in the course of armed conflict, or giving rise to armed conflict in and of themselves, such that IHL would apply.

So what does the Tallinn Manual say on the scope of application of IHL in cyberspace?

The Tallinn Manual offers interesting perspectives in this respect. For example, it upholds the classical dichotomy between international and non-international armed conflicts, and recognizes that cyber operations alone may constitute armed conflicts depending on the circumstances—notably on the destructive effects of such operations. In this regard, the manual defines a "cyber attack" under IHL as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." The crux of the matter, however, lies in the detail, namely what must be understood as "damage" in the digital world. After intense discussion, the majority of the experts agreed that beside physical damage, loss of functionality of an object may also constitute damage. The ICRC's view is that if an object is disabled, it is immaterial how this occurred, whether through kinetic means or a cyber operation. This issue is very important in practice, as, otherwise, a cyber operation aimed at making a civilian network dysfunctional would not be covered by the IHL prohibition on targeting directly civilian persons and objects.

What was the role of the ICRC in this process and are its positions reflected in the manual?

The ICRC contributed, as an observer, to the discussions of the experts who drafted the Tallinn Manual in order to ensure that it reflects as far as possible existing IHL and to uphold the protection this body of law affords to the victims of armed conflicts. The 95 rules set forth in the manual reflect text on which it was possible to achieve consensus among the experts. The ICRC generally agrees with the formulation of the rules; however, there may be exceptions. For example, the rule that recalls the prohibition of belligerent reprisals against a number of specially protected persons and objects does not include cultural property, contrary to the finding of the ICRC's study on customary IHL. The manual also provides useful commentaries to the rules, including the expression of diverging views among the experts. One example of such divergence concerns the obligation of parties to an armed conflict to take all feasible precautions to protect the civilian population and civilian objects

under their control against the effects of cyber attacks: while the manual's commentary argues that this rule's scope of application would be limited to international armed conflicts, the ICRC considers the obligation to apply in any type of armed conflict.

What are the main challenges raised by cyber warfare?

There is only one cyberspace, shared by military and civilian users, and everything is interconnected. The key challenges are to ensure that attacks are directed against military objectives only and that constant care is taken to spare the civilian population and civilian infrastructure. Furthermore, the expected incidental civilian losses and damage must not be excessive in relation to the concrete and direct military advantage anticipated by the cyber attack. If these conditions cannot be met, the attack must not be launched. The manual appropriately recalls in this regard that collateral damage consists of both direct and indirect effects, and that any anticipated indirect effect must be factored into the proportionality assessment during the planning and execution of an attack, a point highly relevant in cyberspace. These challenges underline the importance of States being extremely cautious when resorting to cyber attacks.

Are hackers a legitimate target in cyber warfare?

The term "hackers" encompasses so many people engaged in so many different activities that it cannot be said that hackers as such can be attacked. Most cyber operations are not linked to an armed conflict, so IHL does not even apply. Even in armed conflict, most hackers would be civilians who remain protected by IHL against direct attack—although they would remain subject to law enforcement and possible criminal prosecution depending on whether their activities violated other bodies of law. The situation is different if hackers take a direct part in hostilities by way of a cyber attack in support of one side in an armed conflict. In such a situation, the hackers cannot expect the enemy to remain idle; they lose their legal protection against direct attack during the execution of the cyber attack and the preparatory measures forming an integral part thereof.

Can cyber technology have positive uses in armed conflict?

When conducting military operations, States have an obligation to avoid or at least minimize incidental civilian casualties and damage to civilian infrastructure. Without underestimating the challenges, one cannot rule out the possibility that technological evolution might lead in the future to the development of cyber weapons that would, in specific circumstances, cause fewer casualties and less collateral damage than traditional weapons, to achieve the same military advantage. The ICRC will continue to monitor developments in this regard.

SOURCE: International Committee of the Red Cross, *Cyberwarfare and International Humanitarian Law: the ICRC's Position* (Geneva: International Committee of the Red Cross, 2013), 1–4, https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf. Used by permission of the International Committee of the Red Cross.

ANALYSIS

This particular article from the Red Cross offered a substantial amount of legitimacy to the *Tallinn Manual*, excerpts of which are included in Document 59 of this volume. As such, it effectively announced that the Red Cross had accepted NATO's view of the laws and ethics of cyber warfare—an important consideration given the other perspectives in the world. This is unsurprising, given the ICRC's foundation by western nations, but it is an important consideration when attempting to evaluate the limits of acceptable behavior in the cyber domain. Some of the reservations expressed by the ICRC are illustrative—despite being invited to the conference that drafted the Tallinn Manual, the ICRC was unable to gain consensus that cyberattacks of any kind must be limited to military targets, regardless of the type of conflict being fought. In that regard, the cyber domain again parallels the physical realm—the traditional laws of armed conflict, including the Geneva Conventions, are general accepted as applying to international conflicts—but their applications in small wars are much more in doubt. The same appears to be the case in cyber small wars, so long as they do not escalate to international status.

- ***Document 64:*** *Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*
- ***When:*** December 3, 2013
- ***Where:*** Vienna, Austria
- ***Significance:*** The Organization for Security and Co-operation in Europe (OSCE) is a 57-member organization founded in 1973 that maintains a comprehensive approach to European security. Each member is committed to improving the security situation in Europe by cooperating on political, military, economic, and environmental issues, with a special emphasis on the human aspects of security. Of particular note, both the United States and the Russian Federation are members of the OSCE.

DOCUMENT

975th Plenary Meeting

PC Journal No. 975, Agenda item 1

DECISION No. 1106 INITIAL SET OF OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in co-operation with relevant international organizations, hereinafter referred to as "security of and in the use of ICTs." They further decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

The OSCE participating States, recalling the OSCE role as a regional arrangement under Chapter VIII of the UN Charter, confirm that the CBMs being elaborated in the OSCE complement UN efforts to promote CBMs in the field of security of and in the use of ICTs. The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be consistent with: international law, including, inter alia, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms.

1. Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties.

2. Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs.

3. Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity.

4. Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable internet.

5. The participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard.

6. Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.

7. Participating States will voluntarily share information on their national organization; strategies; policies and programmes—including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.

8. Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States

will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.

9. In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary.

10. Participating States will voluntarily exchange views using OSCE platforms and mechanisms inter alia, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs.

11. Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include inter alia proposals from the Consolidated List circulated by the Chairmanship of the IWG under PC.DEL/682/12 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.

SOURCE: OSCE Permanent Council: Decision No.1106, *Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies* (PC Journal No. 975, Agenda item 1), 975th Plenary Meeting of 3 December 2013. https://www.osce.org/pc/109168

ANALYSIS

Unlike the NATO, which is primarily a military alliance, the OSCE is an organization dedicated to preventing security threats and crises by maintaining open dialogue among all participants. This document illustrates the understanding of OSCE member states that engaging one another in the cyber domain could theoretically spill over into kinetic conflict between member states. By calling upon all members to voluntarily share their views upon the acceptable uses of information and communication technologies, the OSCE effectively offered to serve as a mediating body for any potential disputes. Because the OSCE does not have the same high profile as the United Nations, it might offer a better venue for the United States and Russia to develop a common understanding of where the boundaries of acceptable behavior in the cyber domain should lie.

- ***Document 65:*** *Wales Summit Declaration*
- ***When:*** September 5, 2014
- ***Where:*** North Atlantic Council, Wales, United Kingdom
- ***Significance:*** In 2014, the Russian Federation began a campaign to annex Crimea from Ukraine. After orchestrating a plebiscite of Crimean citizens, many of ethnic Russian heritage, to demand separation from Ukrainian sovereignty and annexation by Russia, the Russian government began sending military forces to the region with the intent of seizing the area by force. The NATO member states vehemently protested the Russian actions, but had little plausible means to deny the Russian movements.

DOCUMENT

1. We, the Heads of State and Government of the member countries of the North Atlantic Alliance, have gathered in Wales at a pivotal moment in Euro-Atlantic security. Russia's aggressive actions against Ukraine have fundamentally challenged our vision of a Europe whole, free, and at peace. Growing instability in our southern neighbourhood, from the Middle East to North Africa, as well as transnational and multi-dimensional threats, are also challenging our security. These can all have long-term consequences for peace and security in the Euro-Atlantic region and stability across the globe.

2. Our Alliance remains an essential source of stability in this unpredictable world. Together as strong democracies, we are united in our commitment to the Washington Treaty and the purposes and principles of the Charter of the United Nations. Based on solidarity, Alliance cohesion, and the indivisibility of our security, NATO remains the transatlantic framework for strong collective defence and the essential forum for security consultations and decisions among Allies. The greatest responsibility of the Alliance is to protect and defend our territories and our populations against attack, as set out in Article 5 of the Washington Treaty. As stated in the Transatlantic Declaration that we issued today, we are committed to further strengthening the transatlantic bond and to providing the resources, capabilities, and political will required to ensure our Alliance remains ready to meet any challenge. We stand ready to act together and decisively to defend freedom and our shared values of individual liberty, human rights, democracy, and the rule of law.

3. Today we reaffirm our commitment to fulfil all three core tasks set out in our Strategic Concept: collective defence, crisis management, and cooperative security. Here in Wales, we have taken decisions to meet the challenges of today and

tomorrow. We are reaffirming our strong commitment to collective defence and to ensuring security and assurance for all Allies; we are adapting our operations, including in Afghanistan, in light of progress made and remaining challenges; and we are strengthening our partnerships with countries and organisations around the globe to better build security together.

. . .

72. As the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging. To face this evolving challenge, we have endorsed an Enhanced Cyber Defence Policy, contributing to the fulfillment of the Alliance's core tasks. The policy reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. It recalls that the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.

73. We are committed to developing further our national cyber defence capabilities, and we will enhance the cyber security of national networks upon which NATO depends for its core tasks, in order to help make the Alliance resilient and fully protected. Close bilateral and multinational cooperation plays a key role in enhancing the cyber defence capabilities of the Alliance. We will continue to integrate cyber defence into NATO operations and operational and contingency planning, and enhance information sharing and situational awareness among Allies. Strong partnerships play a key role in addressing cyber threats and risks. We will therefore continue to engage actively on cyber issues with relevant partner nations on a case-by-case basis and with other international organisations, including the EU, as agreed, and will intensify our cooperation with industry through a NATO Industry Cyber Partnership. Technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives. We will improve the level of NATO's cyber defence education, training, and exercise activities. We will develop the NATO cyber range capability, building, as a first step, on the Estonian cyber range capability, while taking into consideration the capabilities and requirements of the NATO CIS School and other NATO training and education bodies.

SOURCE: North Atlantic Council, *Wales Summit Declaration* (Wales, UK: North Atlantic Council, 2014), https://www.nato.int/cps/en/natohq/official_texts_112964.htm

ANALYSIS

Given that NATO was formed primarily to check aggression from the Soviet Union by creating a mutual defense pact, it is unsurprising that a resurgent and aggressive Russian state would provoke a strong NATO response. In addition to its moves in Crimea, Russia has intervened in the Syrian Civil War and continues its decades-long conflict in Chechnya. Russian cyberattacks have increased over the past decade and moved beyond criminal enterprises into large-scale information operations to disrupt electoral processes in the West. While NATO had little ability to intervene in Ukraine, and no legal responsibility to do so, there is no doubt that the member states that border Russia are looking with trepidation at events on the Black Sea. The Wales Summit Declaration served to present NATO's perspective upon Russian aggression in no uncertain terms, to include statements regarding Russian cyber malfeasance against member states, and to renew guarantees to one another regarding mutual defense and cooperation.

- ***Document 66:*** *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*
- ***When:*** November 2015
- ***Where:*** London, United Kingdom
- ***Significance:*** The United Kingdom is a nation in the midst of significant transition. Having rebuilt its economy after World War II and the end of the colonial era, the British government realizes the importance of the cyber domain for prosperity in the twenty-first century. Given Britain's central role in global financial transactions and trade, it is unsurprising that the national security strategy places equal emphasis upon security and prosperity.

DOCUMENT

Chapter 4—Protect Our People
Overview

4.1 National Security Objective 1 is to **protect our people**—at home, in our Overseas Territories and abroad, and to protect our territory, economic security, infrastructure and way of life.

4.2 This chapter sets out how the Government will use the full spectrum of our capabilities to do this. In particular, we will invest in our **Armed Forces** and **security and intelligence agencies**; deter potential adversaries, including with our **nuclear**

DID YOU KNOW?

The Dark Web

The Dark Web is the term given to a small group of websites with hidden internet protocol (IP) addresses. In order to access such websites, a user requires specialized tools and technical knowledge, but once the sites are reached, users have the ability to interact anonymously with one another and the operators of the sites. This enables all forms of illicit activity, including narcotic sales, prostitution, hackers for hire, and even contract murders. In 2002, the U.S. Naval Research Laboratory field-tested The Onion Router (TOR), a downloadable software kit that allowed Web surfing in a truly anonymous fashion. Although digital privacy activists hailed the development, unforeseen consequences included a massive rise in cybercrime as malefactors began using the same system to exchange child pornography, engage in recruitment for terror organizations, and trade contraband. Although the vast majority of Web users have never utilized the Dark Web, it accounts for a substantial amount of the illicit activities that pervade the modern internet.

deterrent; combat extremism and terrorism at home and overseas; put in place tough and innovative **cyber security** measures; strengthen our ability to disrupt **serious and organised crime**; and increase our **resilience** against threats and hazards.

4.3 This is an integrated, cross-government effort, at home and overseas. For example, our **domestic** work is led by the Home Office, but also involves a wide range of other government and law enforcement agencies. Our **security and intelligence agencies** work closely together, and with law enforcement, military, industry and international partners, to protect our national security. Our **diplomatic** work led by the Foreign and Commonwealth Office (FCO) builds effective, long-term partnerships overseas, which enable us better to disrupt threats to the UK and tackle them at source.

. . .

E. Cyber

4.103 British businesses and government, including the security and intelligence agencies, have made the UK a world leader in cyber security.

4.104 In 2011 we published the UK's first National Cyber Security Strategy. Since then we have invested £860 million in new technology and capabilities. We established the Centre for Cyber Assessment and the UK's Computer Emergency Response Team (CERT-UK). We have built a close partnership between government, the private sector and academia, sharing research, driving innovation and supporting our growing digital economy. We share our specialist knowledge with allies, and cyber defence is part of NATO's core task of collective defence, which could lead to an Article 5 response to a cyber attack threatening national security, stability and prosperity.

4.105 We will invest £1.9 billion over the next five years in protecting the UK from cyber attack and developing our sovereign capabilities in cyber space. In 2016 we will publish a second five-year National Cyber Security Strategy, and we will launch a further five-year National Cyber Security Programme. These will ensure that we have in place all the necessary components to defend the UK from cyber attack. These include capabilities that allow us to understand and tackle the most advanced threats, law enforcement capabilities to deal with cyber crime, support for businesses particularly in the UK's CNI, and the skills and innovation needed for the long term.

Detection, defence and response

4.106 The volume and complexity of cyber attacks against the UK are rising sharply, as are the costs to business. It is becoming easier to put together an advanced attack because of software readily available on the black market.

4.107 We will invest in capabilities to detect and analyse cyber threats, pre-empt attacks and track down those responsible. Primarily based in the Government Communications Headquarters (GCHQ), these capabilities will enable us to match the pace of technological change. We will continue to share knowledge with British industry and with allies.

4.108 We will develop a series of measures to actively defend ourselves against cyber attacks. These national capabilities, developed and operated by the private sector, will reinforce the UK's reputation for being one of the safest places in the world to do business.

4.109 We will improve our national ability to respond quickly and effectively to cyber attack. **We will create a new National Cyber Centre to lead this response.** Operating under GCHQ leadership, it will manage our future operational response to cyber incidents, ensuring that we can protect the UK against serious attacks and minimise their impact. We will pursue a robust policy of challenging those who attempt to use cyber capabilities to cause the UK harm.

4.110 We all have a role to play in protecting computers, networks and data. We will improve the way government protects its data by applying appropriately high standards of cyber security to government systems, introducing stronger defences for our systems and maintaining public confidence in our online government services. **We will build a new secure, cross-government network to improve joint working on sensitive cyber issues.**

4.111 We will help companies and the public to do more to protect their own data from cyber threats, providing specialist information to those who need it. This will include simplifying private sector access to government cyber security advice, and our new National Cyber Centre will form a single point of contact for companies seeking advice. Our approach to protecting CNI is described later in this chapter.

4.112 The Government will ensure that our Armed Forces have strong cyber defences, and that in the event of a significant cyber incident in the UK, they are ready to provide assistance. We will provide the Armed Forces with advanced offensive cyber capabilities, drawing on the National Offensive Cyber Programme which is run in partnership between the MOD and GCHQ. We will continue to help NATO and other allies to protect their networks using our intelligence and technical insights, and we will use our advanced capabilities to enable the success of coalition operations.

Cyber Crime

4.113 Since 2010, we have invested in new law enforcement capabilities, including establishing the National Cyber Crime Unit within the NCA. We have improved the skills of law enforcement officers and our understanding of cyber crime. **We will reinforce law enforcement's specialist capabilities**, making it more difficult for cyber criminals to operate from within the UK. **We will work with industry to strengthen our ability to disrupt cyber crime**, sharing more information on the threat.

4.114 Most of the cyber criminals threatening the UK are based overseas, often exploiting the anonymity of the internet or the absence of effective cyber law enforcement in their host countries. We will disrupt the activities of cyber criminals

overseas through prosecution and other means. **We will create a new intelligence unit dedicated to tackling the criminal use of the "dark web."**

International response

4.115 The UK has led the international debate about what responsible behaviour looks like and how international law applies. Through the London Cyber Process, we have challenged partners to do more to build an open, secure and resilient cyber space, and to work together to tackle criminality.

4.116 We will continue to build an international consensus around the acceptable use of cyber space, increasing the political risk for states which attack the UK or our allies. We will build the capacity of our partners to tackle the cyber threat at source, maximising the likelihood that cyber attacks will fail and be traced back to the point of origin.

SOURCE: United Kingdom Ministry of Defence, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom* (London, United Kingdom: Her Majesty's Stationery Office, 2015), 23, 40–42, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf. Contains public sector information licensed under the Open Government Licence v3.0.

ANALYSIS

The British government has a well-established reputation for leading efforts to create new elements of international law and seems poised to pursue the same approach in the cyber domain. It is in Britain's best interests to create a common understanding of acceptable norms in cyberspace and to ensure that peer competitors adhere to those norms. If a global consensus can be forged, a common effort to eliminate cybercrime will likely follow, with British cyber experts playing a key role in the effort. For decades, the British have placed a substantial amount of effort into creating and maintaining an independent deterrence capability separate from NATO and other international partnerships. This led to a British nuclear weapons program, and in the twenty-first century, it has led to a fairly aggressive cyber policy regarding any efforts to hack into government and military computer networks. The British government seems both willing and able to conduct counterattacks in cyberspace in response to international provocations, and this posture seems to have had a fairly strong deterrent effect against nations considering launching cyber espionage campaigns against British targets. Much like in the United States, the British government issues a national security strategy that is then followed by the subordinate strategic documents for organizations connected to strategic objectives. Thus, this national security strategy also announced the intention to create and propagate a specific cyber strategy that would address 2016 through 2021.

- ***Document 67:*** *National Cyber Security Strategy 2016–2021*
- ***When:*** 2016
- ***Where:*** London, United Kingdom
- ***Significance:*** In support of the 2015 national security strategy issued by the United Kingdom, in 2016, the Ministry of Defence prepared a national cyber strategy designed to govern cyber operations for the following five years. Much like the national security strategy, the cyber strategy places twin emphases on security and prosperity as its overarching goals.

DOCUMENT

1.1. The future of the UK's security and prosperity rests on digital foundations. The challenge of our generation is to build a flourishing digital society that is both resilient to cyber threats, and equipped with the knowledge and capabilities required to maximise opportunities and manage risks.

1.2. We are critically dependent on the internet. However, it is inherently insecure and there will always be attempts to exploit weaknesses to launch cyber attacks. This threat cannot be eliminated completely, but the risk can be greatly reduced to a level that allows society to continue to prosper, and benefit from the huge opportunities that digital technology brings.

1.3. The 2011 National Cyber Security Strategy, underpinned by the British Government's £860m National Cyber Security Programme, has delivered substantial improvements to UK cyber security. It achieved important outcomes by looking to the market to drive secure cyber behaviours. But this approach has not achieved the scale and pace of change required to stay ahead of the fast moving threat. We now need to go further.

1.4. Our vision for 2021 is that **the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.**

1.5. To realise this vision we will work to achieve the following objectives:

- DEFEND We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.
- DETER The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.

DID YOU KNOW?

GhostNet

GhostNet is the name assigned to an advanced persistent threat (APT) detected by cyber researchers in 2009. The APT sought to penetrate the computer networks of the Dalai Lama and Tibetan government-in-exile offices, primarily in India. The campaign began with a coordinated effort to gain access via spearphishing emails and social engineering. Once the participants in the APT managed to penetrate their target networks, they utilized malware to spread their points of access and began exfiltrating data out of the Tibetan networks, presumably to servers in the People's Republic of China. By spoofing email addresses and using infected files to spread malware through the target networks, the propagators of the APT managed to implant remote access trojan (RAT) software throughout the network. The RAT malware, in turn allowed the attackers to activate microphones and cameras on infected computers to engage in spying activity. The resulting discoveries were then used as a means to imprison Tibetans still living in China, and prevent expatriates from returning to areas under Chinese control.

- DEVELOP We have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

1.6. Underpinning these objectives, we will pursue **INTERNATIONAL ACTION** and exert our influence by investing in partnerships that shape the global evolution of cyberspace in a manner that advances our wider economic and security interests. We will deepen existing links with our closest international partners, recognising that this enhances our collective security. We will also develop relationships with new partners to build their levels of cyber security and protect UK interests overseas. We will do this both bilaterally and multilaterally, including through the EU, NATO and the UN. We will deliver clear messages about consequences to adversaries who threaten to harm our interests, or those of our allies, in cyberspace.

1.7. To achieve these outcomes over the next five years, the UK Government intends to intervene more actively and use increased investment, while continuing to support market forces to raise cyber security standards across the UK. The UK Government, in partnership with the Devolved Administrations of Scotland, Wales and Northern Ireland, will work with the private and public sectors to ensure that individuals, businesses and organisations adopt the behaviours required to stay safe on the internet. We will have measures in place to intervene (where necessary and within the scope of our powers) to drive improvements that are in the national interest, particularly in relation to the cyber security of our critical national infrastructure.

1.8. The UK Government will draw on its capabilities and those of industry to develop and apply active cyber defence measures to significantly enhance the levels of cyber security across UK networks. These measures include minimising the most common forms of phishing attacks, filtering known bad IP addresses, and actively blocking malicious online activity. Improvements in basic cyber security will raise the UK's resilience to the most commonly deployed cyber threats.

1.9. We have created a National Cyber Security Centre (NCSC) to be the authority on the UK's cyber security environment, sharing knowledge, addressing systemic vulnerabilties and providing leadership on key national cyber security issues.

1.10. We will ensure that our Armed Forces are resilient and have the strong cyber defences they need to secure and defend their networks and platforms, continuing to operate and retaining global freedom of manoeuvre despite cyber threats.

Our military Cyber Security Operations Centre will work closely with the NCSC and we will ensure that the Armed Forces can assist in the event of a significant national cyber attack.

1.11. We will have the means to respond to cyber attacks in the same way as we respond to any other attack, using whichever capability is most appropriate, including an offensive cyber capability.

1.12. We will use the authority and influence of the UK Government to invest in programmes to address the shortage of cyber security skills in the UK, from schools to universities and across the workforce.

1.13. We will launch two new cyber innovation centres to drive the development of cutting-edge cyber products and dynamic new cyber security companies. We will also allocate a proportion of the £165m Defence and Cyber Innovation Fund to support innovative procurement in defence and security.

1.14. We will invest a total of £1.9 billion over the next five years to transform significantly the UK's cyber security.

SOURCE: UK Ministry of Defence, *National Cyber Security Strategy 2016–2021* (London, UK: Ministry of Defence, 2016), 9–10, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. Contains public sector information licensed under the Open Government Licence v3.0.

ANALYSIS

The British cyber strategy rests upon three pillars: defense, deterrence, and developing further capabilities. British cyber defenses are both active and passive, and the overall direction of national cyber defense operations is led by a centralized agency, the National Cyber Security Centre. By creating such an institution, the British government eliminated duplication and confusion that arose from allowing different organizations to set their own policy regarding cyber defenses. The deterrent aspect of British cyber policy comes in large part from the explicit threat to engage in offensive cyber operations if they are deemed advantageous. Likewise, the British reserve the right to respond to cyberattacks in any fashion, whether in the cyber domain or through other mechanisms. British higher education produces a substantial number of extremely well-trained cyber professionals each year, creating a national reserve of cyber expertise that enhances the credibility of any implied threat to engage in cyber warfare.

- ***Document 68:*** *People's Republic of China National Cyberspace Security Strategy*
- ***When:*** December 27, 2016
- ***Where:*** Beijing, People's Republic of China

- ***Significance:*** Western states are not the only global powers that choose to develop and disseminate their broad strategic objectives. The People's Republic of China has also created strategy documents that offer guidelines for subordinate agencies that are operating in the cyber domain. The Chinese cyberspace strategy bears substantial resemblance to the U.S. cyber strategy but has some interesting points of departure.

DOCUMENT

The widespread use of information technology and the development of cyberspace have greatly promoted economic and social prosperity and progress, but also brought new security risks and challenges. Cyberspace security (hereinafter referred to as cybersecurity) is related to the common interests of mankind, to world peace and development, and to national security. Maintaining China's cybersecurity is an important measure to coordinate and promote the comprehensive construction of a well-off society, comprehensively deepen reforms, comprehensively ruling the country according to law, and comprehensively and strictly manage the party's strategic layout. It is to achieve the goal of "two hundred years" and realize the Chinese revival of the Chinese nation. An important guarantee. In order to implement the "Four Principles" of Chairman Xi Jinping's promotion of the reform of the global internet governance system and the "five-point proposal" for building a community of cyberspace destiny, clarify China's important position on the development and security of cyberspace, guide China's cybersecurity work, and maintain The state formulates this strategy in the interests of sovereignty, security, and development of cyberspace.

Opportunities and Challenges

(1) Major Opportunities

With the rapid development of the information revolution, the cyberspace composed of the internet, communication networks, computer systems, automation control systems, digital devices and their applications, services and data is transforming people's production and lifestyle, and profoundly affecting the history of human society. Development process.

New channels for information dissemination. The development of network technology has broken through the limitations of time and space, expanded the scope of communication, and innovated the means of communication, which triggered a fundamental change in the pattern of communication. The internet has become a new channel for people to obtain information, learn and communicate, and become a new carrier of human knowledge transmission.

A new space for production and life. In today's world, the depth of the network is integrated into people's learning, life, work and other aspects. Online education, entrepreneurship, medical care, shopping, and finance are becoming more and more popular. More and more people exchange ideas, achieve careers, and realize their dreams through the internet.

The new engine of economic development. The internet has increasingly become the leading force for innovation-driven development. Information technology has been widely used in various industries of the national economy, promoting the transformation and upgrading of traditional industries, and has spawned new technologies, new formats, new industries, and new models, and promoted economic restructuring and transformation of economic development patterns. It has injected new impetus into economic and social development.

A new carrier of cultural prosperity. The network promotes cultural exchanges and popularization of knowledge, releases the vitality of cultural development, promotes cultural innovation and creation, enriches people's spiritual and cultural life, and has become a new means of disseminating culture and a new means of providing public cultural services. Network culture has become an important part of cultural construction.

A new platform for social governance. The role of the network in promoting the modernization of the national governance system and governance capacity has become increasingly prominent. The application of e-government has become more in-depth, and government information has been publicly shared. It has promoted the scientific, democratic, and rule-based government decision-making, and has smoothed the channels for citizens to participate in social governance. An important way to protect citizens' right to know, participate, express and supervise.

A new link for exchanges and cooperation. The development of informatization and globalization has promoted the global flow of information, capital, technology, talents and other factors, and has enhanced the exchange and integration of different civilizations. The internet has turned the world into a global village, and the international community has increasingly become a community of destiny in you and me.

DID YOU KNOW?

Operation Titan Rain

Operation Titan Rain was the federal designation applied to a series of attacks against U.S. computer networks beginning in 2003. The attacks were classified as an advanced persistent threat (APT), and probably originated from the People's Republic of China, although full attribution for the attacks has never been made public. The planners of the campaign used a variety of malware and proxy servers to hide their identities, and were able to gain access to defense contractors in the United States, including Lockheed Martin, Sandia National Laboratories, and Redstone Arsenal, in addition to the National Aeronautics and Space Administration (NASA). The hackers also targeted the Defense Intelligence Agency and UK Ministry of Defense. The SANS Institute accused the Chinese military of sponsoring the attacks, although the PRC government denied any responsibility or involvement, and instead claimed that the attackers had merely used compromised Chinese computers to launch their attacks. Regardless of attribution, the Titan Rain attacks facilitated a massive data transfer, including a substantial amount of material related to the F-35 Lightning II Joint Strike Fighter, the newest air-superiority aircraft in the U.S. arsenal, which underwent several redesign efforts due to the cyber espionage campaign.

The new territory of national sovereignty. Cyberspace has become a new field of human activity that is as important as land, sea, sky and space. The expansion of national sovereignty extends to cyberspace, and cyberspace sovereignty has become an important part of national sovereignty. Respecting cyberspace sovereignty, maintaining cybersecurity, seeking common governance, and achieving win-win results are becoming the consensus of the international community.

(2) **Severe challenges**

The cyber security situation is becoming increasingly severe. The country's political, economic, cultural, social, and national defense security and citizens' legitimate rights and interests in cyberspace are facing serious risks and challenges.

Network penetration harms political security. Political stability is the basic prerequisite for national development and people's happiness. The use of the network to interfere in his internal affairs, attack the political system of other countries, incite social unrest, subvert the political power of other countries, and large-scale network monitoring, network theft and other activities seriously endanger the political security of the country and the security of user information.

Cyber attacks threaten economic security. Network and information systems have become the backbone of critical infrastructure and even the entire economic society. Attacks and destruction and major security incidents will lead to paralyzed infrastructures such as energy, transportation, communications, and finance, causing catastrophic consequences and seriously jeopardizing national economic security. And the public interest.

Harmful information on the internet erodes cultural security. Various ideological and cultural networks on the internet are in conflict and confrontation, and excellent traditional culture and mainstream values are facing impact. Internet rumors, decadent culture and obscenity, violence, superstition and other harmful information that violates the core values of socialism erodes the physical and mental health of young people, ruin the social atmosphere, mislead value orientation and endanger cultural security. Online morality is out of order, lack of integrity is frequent, and the degree of network civilization needs to be improved.

Cyber terror and illegal crimes undermine social security. Terrorism, separatism, extremism and other forces use the internet to incite, plan, organize and implement violent terrorist activities, directly threatening people's lives and property, and social order. Computer viruses, Trojans, etc. spread in the cyberspace. Internet fraud, hacker attacks, intellectual property infringement, and misuse of personal information are abundant. Some organizations deliberately steal user information, transaction data, location information, and corporate trade secrets, seriously damaging the country, corporate and personal interests, affecting social harmony and stability.

The international competition in cyberspace is on the rise. The international competition for competing for and controlling cyberspace strategic

resources, seizing the rule-making power and strategic commanding heights, and seeking strategic initiative is becoming increasingly fierce. Individual countries have strengthened their network deterrence strategies and intensified the cyberspace arms race, and world peace has been challenged by new challenges.

Cyberspace opportunities and challenges coexist, and opportunities outweigh challenges. We must adhere to active use, scientific development, management according to law, ensure security, resolutely safeguard network security, maximize the utilization potential of cyberspace, better benefit more than 1.3 billion Chinese people, benefit all mankind, and firmly safeguard world peace.

Second, the goal

Guided by the overall national security concept, we will implement the development concept of innovation, coordination, green, openness, and sharing, enhance risk awareness and crisis awareness, coordinate the two major domestic and international situations, and coordinate the development of two major events, actively defending and responding effectively. Promote cyberspace peace, security, openness, cooperation, orderly, safeguard national sovereignty, security, development interests, and achieve the strategic goal of building a network power.

Peace: Information technology abuse has been effectively curbed, and activities such as the cyberspace arms race that threaten international peace have been effectively controlled, and cyberspace conflicts have been effectively prevented.

Security: The network security risks are effectively controlled, the national network security assurance system is sound and complete, the core technical equipment is safe and controllable, and the network and information systems are stable and reliable. Network security talents meet the needs, and the society's cyber security awareness, basic protection skills, and confidence in using the network have increased dramatically.

Openness: Information technology standards, policies and markets are open and transparent, product circulation and information dissemination are smoother, and the digital divide is increasingly bridging. Regardless of size, strength, or wealth, countries around the world, especially developing countries, can share development opportunities, share development results, and participate fairly in cyberspace governance.

Cooperation: All countries in the world have closer cooperation in the fields of technology exchange, combating cyber terrorism and cybercrime. The multilateral, democratic and transparent international internet governance system is sound and perfect, and the cyberspace destiny community with cooperation and win-win as the core has gradually formed.

Orderly: The public's right to know, participation, expression, and supervision in the cyberspace are fully protected, and the privacy of cyberspace is effectively protected and human rights are fully respected. The domestic and international legal systems and standards of cyberspace have been

gradually established. The cyberspace has been effectively governed according to law. The network environment is honest, civilized and healthy. The free flow of information and the maintenance of national security and public interests are organically unified.

SOURCE: National Internet Information Office, People's Republic of China, *National Cyberspace Security Strategy* (Beijing, PRC: National Internet Information Office, 2016), translated by Google Translate, http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

ANALYSIS

It is illuminating that the Chinese government has chosen to portray its cyber objectives as being in the interest of all humankind—it is either an incredibly ethnocentric viewpoint or a deliberate attempt to convey the argument that the Chinese government is above the petty interests of its primary competitors in the cyber arena. Naturally, the first objective of the Chinese cyber strategy is to maintain the security of its own networks and to allow its government and military to have freedom of action through the cyber domain. However, given the past behavior of the People's Liberation Army and its long-term cyber espionage campaigns against global power rivals, it is disingenuous to suggest that the Chinese cyber strategy will be one of openness, peace, and harmony going forward. Rather, it is entirely possible that the Chinese government has recognized its own vulnerability to cyber attack and exploitation—some estimates suggest that over 90 percent of Chinese computers are running pirated versions of Microsoft Windows software, making them ineligible for security updates and incredibly open to even the most unsophisticated of cyberattacks. Perhaps the Chinese government has effectively decided that the best way to protect itself from external attack is to create a new era of global cyber harmony.

- ***Document 69:*** *Developments in the Field of Information and Communications Technology in the Context of International Security*
- ***When:*** October 29, 2018
- ***Where:*** Russian Delegation, United Nations, New York City, United States
- ***Significance:*** This Russian proposal was presented to the United Nations less than two weeks after a proposal by the United States (see Document 56 in this volume). The competing proposals had the potential to set the international framework for deciding the laws and ethics of behavior in the cyber domain, and each

represented the vital interests of its proposing government. The Russian proposal places the onus of infrastructure protection upon the defender, suggesting that the victim has a certain degree of responsibility for being vulnerable in the first place.

DOCUMENT

Developments in the field of information and telecommunications in the context of international security

1. Welcomes the following set of international rules, norms and principles of responsible behaviour of States, enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 20133 and 20152 adopted by consensus and recommended in resolution 71/28 entitled "Developments in the field of information and telecommunications in the context of international security," adopted by the General Assembly on 5 December 2016:

1.1. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

1.2. States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Accusations of organizing and implementing wrongful acts brought against States should be substantiated. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

1.3. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-State actors to commit such acts.

1.4. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

1.5. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 of 5 July 2012 and 26/13 of 26 June 2014 on the promotion, protection and enjoyment of human rights on the internet, as well

as General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

1.6. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

1.7. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

1.8. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

1.9. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.

1.10. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

1.11. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies for such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

1.12. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

1.13. States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behaviour in information space with regard to their potential role;

2. Calls upon Member States to promote further, at multilateral levels, the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information;

3. Considers that the purpose of such measures could be served through further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

4. Invites all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts on

Developments in the Field of Information and Telecommunications in the Context of International Security,1 to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;
(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;
(c) The content of the concepts mentioned in paragraph 3 above;
(d) Possible measures that could be taken by the international community to strengthen information security at the global level;

5. Decides to convene, beginning in 2019, with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent, an open-ended working group acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States listed in paragraph 1 above, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building and the concepts referred to in paragraph 3 above, and to submit a report on the results of the study to the General Assembly at its seventy-fifth session, and to provide the possibility of holding, from within voluntary contributions, intersessional consultative meetings with the interested parties, namely business, non-governmental organizations and academia, to share views on the issues within the group's mandate;

6. Also decides that the open-ended working group shall hold its organizational session in June 2019 in order to agree on the organizational arrangements connected with the group;

7. Further decides to include in the provisional agenda of its seventy-fourth session the item entitled "Developments in the field of information and telecommunications in the context of international security."

SOURCE: Russian Federation Delegation to the United Nations, *Developments in the Field of Information and Communications Technology in the Context of International Security*, October 29, 2018, 3–5, https://undocs.org/A/C.1/73/L.27/Rev.1

ANALYSIS

Perhaps the most noteworthy departure between the Russian and U.S. proposals concerns the responsibilities of states when international cyberattacks are launched from their soil—the Russian proposal takes a much weaker stance on the issue

perhaps because of the number of cyberattacks launched from Russia on a daily basis. Russia tends to be very committed to protecting its own citizens from any outside interference, to include a refusal to consider most extradition requests, particularly for cyber activity. While the Russian proposal includes a call for sharing information, it ultimately leaves each nation responsible for punishing its own citizens, if necessary, rather than allowing them to be held accountable by other nations or any international body. This reflects the typical Russian government approach to cyberattacks, which is that they will not be punished, as long as they do not target Russian citizens or systems.

5

SPEECHES, TESTIMONY, AND TRANSCRIPTS

- ***Document 70:*** *President Barack Obama, "Remarks on Securing the Nation's Cyber Infrastructure"*
- ***When:*** May 29, 2009
- ***Where:*** Washington, D.C.
- ***Significance:*** President Barack Obama's administration entered office with a better understanding of the capabilities and limits of the cyber domain than any of its predecessors. During the election campaign, his team had harnessed the enormous potential of the internet to raise unprecedented sums of money and to maintain almost constant contact with devoted supporters of the campaign. Upon assuming office, President Obama directed the formation of a commission to study the threats that cyberattacks might present to the nation's infrastructure. Less than five months after assuming office, he offered a major policy change regarding cyber defense and national security.

DOCUMENT

It's long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: This world—cyberspace—is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives.

It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history.

So cyberspace is real. And so are the risks that come with it.

It's the great irony of our Information Age—the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox—seen and unseen—is something that we experience every day.

It's about the privacy and the economic security of American families. We rely on the internet to pay our bills, to bank, to shop, to file our taxes. But we've had to learn a whole new vocabulary just to stay ahead of the cyber criminals who would do us harm—spyware and malware and spoofing and phishing and botnets. Millions of Americans have been victimized, their privacy violated, their identities stolen, their lives upended, and their wallets emptied. According to one survey, in the past two years alone cyber crime has cost Americans more than $8 billion.

I know how it feels to have privacy violated because it has happened to me and the people around me. It's no secret that my presidential campaign harnessed the internet and technology to transform our politics. What isn't widely known is that during the general election hackers managed to penetrate our computer systems. To all of you who donated to our campaign, I want you to all rest assured, our fundraising website was untouched. (Laughter.) So your confidential personal and financial information was protected.

But between August and October, hackers gained access to emails and a range of campaign files, from policy position papers to travel plans. And we worked closely with the CIA—with the FBI and the Secret Service and hired security consultants to restore the security of our systems. It was a powerful reminder: In this Information Age, one of your greatest strengths—in our case, our ability to communicate to a wide range of supporters through the internet—could also be one of your greatest vulnerabilities.

This is a matter, as well, of America's economic competitiveness. The small businesswoman in St. Louis, the bond trader in the New York Stock Exchange, the workers at a global shipping company in Memphis, the young entrepreneur in Silicon Valley—they all need the networks to make the next payroll, the next trade, the next delivery, the next great breakthrough. E-commerce alone last year accounted for some $132 billion in retail sales.

But every day we see waves of cyber thieves trolling for sensitive information—the disgruntled employee on the inside, the lone hacker a thousand miles away, organized crime, the industrial spy and, increasingly, foreign intelligence services. In one brazen act last year, thieves used stolen credit card information to steal millions of dollars from 130 ATM machines in 49 cities around the world—and they did it in just 30 minutes. A single employee of an American company was convicted of stealing intellectual property reportedly worth $400 million. It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion.

In short, America's economic prosperity in the 21st century will depend on cybersecurity.

And this is also a matter of public safety and national security. We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control. Yet we know that cyber intruders have probed our electrical grid and that in other countries cyber attacks have plunged entire cities into darkness.

Our technological advantage is a key to America's military dominance. But our defense and military networks are under constant attack. Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyber attack on our country—attacks that are harder to detect and harder to defend against. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer—a weapon of mass disruption.

In one of the most serious cyber incidents to date against our military networks, several thousand computers were infected last year by malicious software—malware. And while no sensitive information was compromised, our troops and defense personnel had to give up those external memory devices—thumb drives—changing the way they used their computers every day.

And last year we had a glimpse of the future face of war. As Russian tanks rolled into Georgia, cyber attacks crippled Georgian government websites. The terrorists that sowed so much death and destruction in Mumbai relied not only on guns and grenades but also on GPS and phones using voice-over-the-internet.

For all these reasons, it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation.

It's also clear that we're not as prepared as we should be, as a government or as a country. In recent years, some progress has been made at the federal level. But just as we failed in the past to invest in our physical infrastructure—our roads, our bridges and rails—we've failed to invest in the security of our digital infrastructure.

No single official oversees cybersecurity policy across the federal government, and no single agency has the responsibility or authority to match the scope and scale of the challenge. Indeed, when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should—with each other or with the private sector. We saw this in the disorganized response to Conficker, the internet "worm" that in recent months has infected millions of computers around the world.

. . .

From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.

. . .

First, working in partnership with the communities represented here today, we will develop a new comprehensive strategy to secure America's information and communications networks. To ensure a coordinated approach across government, my Cybersecurity Coordinator will work closely with my Chief Technology Officer, Aneesh Chopra, and my Chief Information Officer, Vivek Kundra. To ensure accountability in federal agencies, cybersecurity will be designated as one of my key management priorities. Clear milestones and performances metrics will measure progress. And as we develop our strategy, we will be open and transparent, which is why you'll find today's report and a wealth of related information on our Web site, www.whitehouse.gov.

Second, we will work with all the key players—including state and local governments and the private sector—to ensure an organized and unified response to future cyber incidents. Given the enormous damage that can be caused by even a single cyber attack, ad hoc responses will not do. Nor is it sufficient to simply strengthen our defenses after incidents or attacks occur. Just as we do for natural disasters, we have to have plans and resources in place beforehand—sharing information, issuing warnings and ensuring a coordinated response.

Third, we will strengthen the public/private partnerships that are critical to this endeavor. The vast majority of our critical information infrastructure in the United States is owned and operated by the private sector. So let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity.

Fourth, we will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time. And that's why my administration is making major investments in our information infrastructure: laying broadband lines to every corner of America; building a smart electric grid to deliver energy more efficiently; pursuing a next generation of air traffic control systems; and moving to electronic health records, with privacy protections, to reduce costs and save lives.

And finally, we will begin a national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms, and to build a digital workforce for the 21st century. And that's why we're making a new commitment to education in math and science, and historic investments in science and research and development. Because it's not enough for our children and students to master today's technologies—social networking and e-mailing and texting and blogging—we need them to pioneer the technologies that will allow us to work effectively through these new media and allow us to prosper in the future. So these are the things we will do.

Let me also be clear about what we will not do. Our pursuit of cybersecurity will not—I repeat, will not include—monitoring private sector networks or internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans. Indeed, I remain firmly committed to net neutrality so we can keep the internet as it should be—open and free.

SOURCE: Barack Obama, *Remarks on Securing the Nation's Cyber Infrastructure*, White House transcripts (Washington, D.C., May 29, 2009), https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

ANALYSIS

Although President Obama's predecessors had been briefed about the potential capabilities brought about by the development of the cyber domain, they did not show an inherent understanding of the vast potential that cyberattacks might represent. The same cannot be said of Obama—he seemed to possess an almost visceral grasp of how cyber networks might be leveraged in the future and wanted to take steps to protect them as he would any other critical infrastructure. By publicly announcing the importance of protecting the nation's cyber assets, he clearly illustrated the importance of such networks to the economic and social vitality of the nation. This speech served to unify the disparate efforts being conducted to secure the nation's cyber assets, and signaled that a much greater centralization process could be expected over the course of his administration.

- ***Document 71:*** *William J. Lynn, III, "Remarks at the Defense Information Technology Acquisition Summit"*
- ***When:*** November 12, 2009
- ***Where:*** Washington, D.C.

- ***Significance:*** William J. Lynn, III, served as the deputy secretary of defense under President Obama. In 2009, he offered his perspective on the challenges faced by the enormous military bureaucracy regarding the acquisition, maintenance, and security of information technology.

DOCUMENT

IT acquisition is a challenge for the department for two primary reasons. First, traditional weapons systems develop mature technology in classified settings. With IT, development happens in the commercial marketplace. Mature technology is then imported into DOD systems, often with little further modification. Weapons systems depend upon stable requirements, but with IT, technology changes faster than the requirements process can keep up. It changes faster than the budget process and it changes faster than the acquisition milestone process. For all these reasons the normal acquisition process does not work for information technology.

On average it takes 81 months in DOD from when a program is first funded to when it becomes operational. If we take into account the continued growth of computing power, this means that systems are being delivered four to five generations behind state-of-the-art. By comparison, the iPhone was developed in less time than it would take DOD to budget for an IT program, and there are now 100,000 apps that enable users to customize the platform to their own needs.

The second problem with the current acquisition process is that it often fails to take into account end-user preferences. Our soldiers are digital natives. Information technology is a natural part of everything they do. Many of our enemies are digital natives as well. Unless we build systems for tech-savvy soldiers, we will continue to limit ourselves in the fight against tech-savvy enemies.

So what approach should we take to IT acquisition? A new approach to IT acquisition is taking shape inside the department as we speak. We recognize that information technology has never fit the classic acquisition model. The inherent modularity of IT, together with its rapid commercial innovation, means that the nature and lifecycle of IT platforms differs significantly from other weapons systems. Similarly, the government's role in maturing them is different as well. With most IT being developed commercially, our primary role is to design system architecture and to test vendor components.

Future IT systems will be continually reinvented as they age, allowing old platforms to be used for new missions. Our approach to acquisition must be mindful of this kind of thinking. We need to encourage the use of commercial technology. We need to emphasize open design protocols that make systems easy to modify, and we need to adopt service-oriented architectures that will allow vendors to be unable to monopolize systems with proprietary technology.

This approach to IT acquisition is already working inside the department. The Navy is applying it to its combat systems on submarines. With the exception of

transducers and water-cooled racks, all of the hardware and 60 percent of the software is commercial. With an open architecture, new capabilities can be inserted each time a sub returns to base. A program that began with one submarine has now expanded to them all, proving that service-oriented architectures can work.

A more nimble IT acquisition process is even more important with the transition away from supplemental appropriations bills which had allowed us to deliver crucial warfighting technologies outside the usual budget acquisition processes. As we return to funding wartime programs through the base budget, we need to build greater responsiveness in our standing processes. We need to redirect IT systems from an 81-month march to obsolescence and put them on a path to meet warfighters' evolving needs.

Although IT enables tremendous gains, it's also a double-edged sword. There's no exaggerating our military dependence on information networks. Command and control of our forces, intelligence and logistics, the weapons and technologies we field all depend on computer systems and networks. Our networks therefore make a tempting target—all 15,000 of them. This includes 7 million computers, laptops, servers and other devices.

This is not an emerging threat; this is not some future contingency. The cyber threat is here today; it's here now. There are more than 100 intelligence organizations trying to hack into U.S. systems even today. Foreign governments are developing offensive cyber capabilities. Russia and China already have the capacity to disrupt elements of U.S. information infrastructure. And the cyber threat does not end with states. Organized criminal groups and individual hackers are building global networks of compromised computers, botnets and zombies, and renting them to the highest bidder, in essence becoming 21st century cyber mercenaries. And terrorist groups are active on thousands of websites. Al Qaeda and others have expressed a desire to unleash coordinated cyber attacks on the United States.

So our defense networks are already under attack. They are probed thousands of times each day; they are scanned millions of times each day, and the frequency and the sophistication of those attacks are increasing exponentially. It's an unprecedented challenge to our national security. By virtue of its source, its speed and its scope, it marks a new development in the history of war. In the 18th and 19th centuries, ships crossed the oceans in days. In World War II, aircraft could cross the oceans in hours. In the Cold War, missiles could do it in minutes. Today we face cyber attacks that can be mounted in milliseconds. The speed has profound implications for how we mount a defense. If attacked in milliseconds, we can't take days, weeks or months to respond. We need to respond at network speed, before attacks compromise ongoing operations or the lives of our troops.

Fortunately, to this point cyber attacks on our military networks have not cost any lives, but they are costing an increasing amount of money, and the threat is there. In one recent six-month period, the department spent more than $100 million simply defending its networks. For all these reasons, the President has called the cyber threat one of the most serious economic and national security challenges we face as a nation.

So what is DOD doing about it? Our troops and the American people need to understand that DOD has built strong, layered and robust cyber-defenses. Over the

years we've taken a number of critical steps. DOD has formally recognized cyberspace for what it is: a domain similar to land, sea, air, and space. Unlike the others, though, cyberspace is a man-made domain, but still it is a domain that we depend upon and we need to protect. Just as we need freedom of navigation on the seas, we need freedom of movement online. Just as we protect the front gates of our military bases, we must protect the back doors of our systems and networks that adversaries seek to exploit.

With your help we are taking further steps to make our networks safe. Our efforts fall into three general areas: culture, capabilities, and command. At DOD we are trying to build a culture of responsibility towards the use of information technology. It takes 90,000 personnel to administer, monitor and defend the 15,000 networks, but most are not formally certified in information assurance, so we're expanding our training and certification to build a truly world-class cyber workforce. And with 3 million employees, improving cyber security training and accountability has to be a priority. The same is true for our defense partners who need to protect sensitive information on their own classified networks. To help them achieve this mission, we share information on the latest threats and vulnerabilities. Defense contractors report incidents more quickly, and today we respond and recover faster as we did with the Conficker worm.

Second, we are developing a doctrine to cover how we protect cyberspace as a domain, how our forces will be designed and how they will be trained to protect and defend our networks. The ongoing Quadrennial Defense Review is assessing our current capabilities and will make recommendations on doctrine for the future.

Mounting an effective cyber defense also takes new capabilities. We subject weapons systems to extensive evaluations. We test the skills of our troops on training ranges, but we have no such equivalent in cyber security. DARPA, which helped invent the internet decades ago, is leading our effort to build a national cyber range—in effect a model of the internet. This will allow us to engage in real-world simulations so we can develop, test and field new leap-ahead capabilities for cyber security. Many of you are involved in this effort. As we build new capabilities, we can't retreat behind a fortress of firewalls. Today's cyber threats are organic and are constantly evolving. Our cyber defenses must do the same. We can't afford a digital version of the Maginot Line. A better model is maneuver warfare, where new tactics and technologies allow nimble forces to out-maneuver foes.

The third area where we're taking action is command. Secretary Gates approved a new Cyber Command as a sub-unified command of the Strategic Command—STRATCOM. It will lead day-to-day defense and protection of all DOD networks. But CYBERCOM is not intended to be the militarization of cyberspace. It will be responsible for DOD's networks—the dot-mil world. Responsibility for federal civilian networks—dot-gov—stays with the Department of Homeland Security, and that's exactly how it should be.

To coordinate our national response to the cyber threat, the president has created a new White House office and will shortly be naming a White House cyber security coordinator to lead it.

So we're making progress, but we still have a long way to go. How we proceed will depend on how we answer some key questions—questions that I hope you'll address in today's conference. These include, how can we deter and prevent cyber attacks?

Deterrence is predicated generally on knowing the adversary, but in cyberspace it's often the case that we have great difficulty in identifying the adversary, so does the deterrent model apply? Or how does it apply in those kinds of circumstances?

Beyond DOD, how do we organize the government as a whole? Again, DHS is the lead for federal civilian networks, and DOD is proud to be coordinating with DHS and providing some expertise. DOD has employees that are part of the DHS-led Computer Emergency Response Team, and DHS employees help DOD respond to intrusions into our networks. We participate in each other's exercises and share the latest technologies.

Beyond government, how do we partner with industry? Neither the government nor the private sector can do this alone. The government needs industry, which owns and operates most of our nation's information infrastructure. The private sector needs government to establish coherent, effective laws and regulations. Public-private partnerships are still hard to forge in this world. It comes down to trust. Industry needs to trust government to protect proprietary information; government needs to trust industry to protect sensitive details of threats and vulnerabilities.

Beyond the United States, how do we cooperate internationally? Many cyber attacks on U.S. networks originate overseas. Botnet attacks involve computers all over the world. This raises complex issues of national sovereignty and international law. How do we defend ourselves in this global environment? When exactly is a cyber attack an act of war? We need to confront these questions. We need to confront them as a partnership between industry and government.

But we've only just begun. We've just begun to consider these questions. It's not easy working across so many sectors. It can be frustrating and at times exhausting. So I'd leave you with this simple observation: It's only 1928. By that I mean, we've just marked the 100th anniversary of military aviation, which began in 1908; 2009, however, is only the 20th anniversary of the World Wide Web. In other words, in terms of cyber security, we're at the 1928 point. We're still in the era of biplanes and dirigibles. We're still at the dawn of the Information Age. We still have decades of change and challenges ahead of us, decades of innovations we haven't yet imagined. There will be setbacks and failures along the way, but if history is any guide, this too is a challenge we can solve together; this too is an opportunity to meet our share of responsibility to protect the security of our people, to ensure the prosperity of our economies, and to uphold and preserve civil liberties. That's the spirit in which I join you today, that's the spirit the DOD will bring to this challenge, and that's the spirit our nation will need now and in the years to come.

SOURCE: William J. Lynn, III, *Remarks at the Defense Information Technology Acquisition Summit*, November 12, 2009, https://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1399

ANALYSIS

Lynn's remarks in 2009 demonstrated that while the Department of Defense (DOD) might have grasped the dangers of operating in the cyber domain, it had done little to fix its own bureaucracy, which hindered the development, acquisition,

and employment of effective information technology systems. As a result, the department found itself inherently on the defensive, facing almost continual cyberattacks while using an aging and vulnerable information network system. Although Lynn was able to report some success in the acquisition and employment of commercial off-the-shelf products, the problem of keeping pace with technological developments continues to plague the DOD, and the level of cyberattacks launched against the DOD continues to rise each year.

- ***Document 72:*** *Hillary Clinton, "Remarks on Internet Freedom"*
- ***When:*** January 21, 2010
- ***Where:*** Washington, D.C.
- ***Significance:*** Secretary of State Hillary Clinton spoke to a gathering of internet freedom activists, U.S. political leaders, and international representatives at a gathering in Washington, D.C. in early 2010. By calling for greater freedom of information flow across the internet, Clinton's remarks were interpreted by some totalitarian leaders as an effort to undermine their rule. Given her role as the U.S. secretary of state, it is unsurprising that many such leaders perceived this speech as evidence of an imminent cyberattack upon their regimes.

DOCUMENT

The spread of information networks is forming a new nervous system for our planet. When something happens in Haiti or Hunan, the rest of us learn about it in real time—from real people. And we can respond in real time as well. Americans eager to help in the aftermath of a disaster and the girl trapped in the supermarket are connected in ways that were not even imagined a year ago, even a generation ago. That same principle applies to almost all of humanity today. As we sit here, any of you—or maybe more likely, any of our children—can take out the tools that many carry every day and transmit this discussion to billions across the world.

Now, in many respects, information has never been so free. There are more ways to spread more ideas to more people than at any moment in history. And even in authoritarian countries, information networks are helping people discover new facts and making governments more accountable.

During his visit to China in November, for example, President Obama held a town hall meeting with an online component to highlight the importance of the internet. In response to a question that was sent in over the internet, he defended

the right of people to freely access information, and said that the more freely information flows, the stronger societies become. He spoke about how access to information helps citizens hold their own governments accountable, generates new ideas, encourages creativity and entrepreneurship. The United States belief in that ground truth is what brings me here today.

Because amid this unprecedented surge in connectivity, we must also recognize that these technologies are not an unmitigated blessing. These tools are also being exploited to undermine human progress and political rights. Just as steel can be used to build hospitals or machine guns, or nuclear power can either energize a city or destroy it, modern information networks and the technologies they support can be harnessed for good or for ill. The same networks that help organize movements for freedom also enable al-Qaida to spew hatred and incite violence against the innocent. And technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights.

In the last year, we've seen a spike in threats to the free flow of information. China, Tunisia, and Uzbekistan have stepped up their censorship of the internet. In Vietnam, access to popular social networking sites has suddenly disappeared. And last Friday in Egypt, 30 bloggers and activists were detained. One member of this group, Bassem Samir, who is thankfully no longer in prison, is with us today. So while it is clear that the spread of these technologies is transforming our world, it is still unclear how that transformation will affect the human rights welfare of the world's population.

On their own, new technologies do not take sides in the struggle for freedom and progress, but the United States does. We stand for a single internet where all of humanity has equal access to knowledge and ideas. And we recognize that the world's information infrastructure will become what we and others make of it. Now this challenge may be new, but our responsibility to help ensure the free exchange of ideas goes back to the birth of our republic.

There are many other networks in the world. Some aid in the movement of people or resources, and some facilitate exchanges between individuals with the same work or interests. But the internet is a network that magnifies the power and potential of all others. And that's why we believe it's critical that its users are assured certain basic freedoms. Freedom of expression is first among them. This freedom is no longer defined solely by whether citizens can go into the town square and criticize their government without fear of retribution. Blogs, emails, social networks, and text messages have opened up new forums for exchanging ideas, and created new targets for censorship. As I speak to you today, government censors somewhere are working furiously to erase my words from the records of history. But history has already condemned these tactics.

Some countries have erected electronic barriers that prevent their people from accessing portions of the world's networks. They've expunged words, names, and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent political speech. These actions contravene the Universal Declaration of Human Rights, which tells us that all people have the right "to seek, receive and impart information and ideas through any media and regardless of

frontiers." With the spread of these restrictive practices, a new information curtain is descending across much of the world. And beyond this partition, viral videos and blog posts are becoming the samizdat of our day.

As in the dictatorships of the past, governments are targeting independent thinkers who use these tools. In the demonstrations that followed Iran's presidential elections, grainy cell phone footage of a young woman's bloody murder provided a digital indictment of the government's brutality. We've seen reports that when Iranians living overseas posted online criticism of their nation's leaders, their family members in Iran were singled out for retribution. And despite an intense campaign of government intimidation, brave citizen journalists in Iran continue using technology to show the world and their fellow citizens what is happening inside their country. In speaking out on behalf of their own human rights, the Iranian people have inspired the world. And their courage is redefining how technology is used to spread truth and expose injustice.

Some nations, however, have co-opted the internet as a tool to target and silence people of faith. Last year, for example, in Saudi Arabia, a man spent months in prison for blogging about Christianity. And a Harvard study found that the Saudi Government blocked many web pages about Hinduism, Judaism, Christianity, and even Islam. Countries including Vietnam and China employed similar tactics to restrict access to religious information.

Now, just as these technologies must not be used to punish peaceful political speech, they also must not be used to persecute or silence religious minorities. Now, prayers will always travel on higher networks. But connection technologies like the internet and social networking sites should enhance individuals' ability to worship as they see fit, come together with people of their own faith, and learn more about the beliefs of others. We must work to advance the freedom of worship online just as we do in other areas of life.

A connection to global information networks is like an on-ramp to modernity. In the early years of these technologies, many believed they would divide the world between haves and have-nots. But that hasn't happened. There are 4 billion cell phones in use today. Many of them are in the hands of market vendors, rickshaw drivers, and others who've historically lacked access to education and opportunity. Information networks have become a great leveler, and we should use them together to help lift people out of poverty and give them freedom from want.

Now, we have every reason to be hopeful about what people can accomplish when they leverage communication networks and connection technologies to achieve progress. But make no mistake—some are and will continue to use global information networks for darker purposes. Violent extremists, criminal cartels, sexual predators, and authoritarian governments all seek to exploit these global networks. Just as terrorists have taken advantage of the openness of our societies to carry out their plots, violent extremists use the internet to radicalize and intimidate. As we work to advance freedoms, we must also work against those who use communication networks as tools of disruption and fear.

Governments and citizens must have confidence that the networks at the core of their national security and economic prosperity are safe and resilient. Now this is about more than petty hackers who deface websites. Our ability to bank online, use

electronic commerce, and safeguard billions of dollars in intellectual property are all at stake if we cannot rely on the security of our information networks.

States, terrorists, and those who would act as their proxies must know that the United States will protect our networks. Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation. In an internet-connected world, an attack on one nation's networks can be an attack on all. And by reinforcing that message, we can create norms of behavior among states and encourage respect for the global networked commons.

SOURCE: Hillary Clinton, *Remarks on Internet Freedom*, January 21, 2010, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

ANALYSIS

Ironically, despite her calls for greater internet freedom and the importance of allowing users of the internet to communicate freely with one another, Secretary Clinton showed little personal understanding of the inherent dangers and challenges of cybersecurity. She was later investigated for setting up a private, poorly secured network server in her home, and conducting government business through personal email systems, including the transmission of a number of classified documents on an unsecured system. These attacks dogged her during the 2016 presidential election campaign and almost certainly contributed to her defeat by President Donald Trump.

- ***Document 73:*** *Statement for the Record of Seán P. McGurk before the U.S. Senate Homeland Security and Governmental Affairs Committee*
- ***When:*** November 17, 2010
- ***Where:*** Washington, D.C.
- ***Significance:*** In 2010, Seán P. McGurk served as the acting director of the National Cybersecurity and Communications Integration Center (NCCIC) in the Department of Homeland Security (DHS). In his statement to the Senate Homeland Security and Governmental Affairs Committee, he outlined the DHS responsibilities regarding securing cyberspace in the United States. He also offered his perspective on the formation of computer emergency response teams (CERTs) and how they might be utilized in future cyber crises.

DOCUMENT

Overview of DHS Cybersecurity Responsibilities

DHS [Department of Homeland Security] is responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. DHS serves as the principal federal agency to lead, integrate, and coordinate implementation of efforts among federal departments and agencies, state and local governments, and the private sector to protect domestic critical infrastructure and key resources.

DHS takes threats to our private sector critical cyber infrastructure as seriously as we take threats to our conventional, physical infrastructure because our society and our economy depend on these networks and systems to operate effectively. A successful, large-scale cyber attack could have cascading effects across many sectors and around the world, which is among the reasons why President Obama identified our digital infrastructure as a national strategic asset.

In line with the President's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, DHS has developed a long-range vision of cybersecurity for the nation's homeland security enterprise. This effort resulted in the elevation of cybersecurity to one of the Department's five priority missions as articulated in the Quadrennial Homeland Security Review (QHSR), an overarching framework for the Department that defines our key priorities and goals and outlines a strategy for achieving them. Within the cybersecurity mission area, the QHSR details two overarching goals: (1) help create a safe, secure and resilient cyber environment; and (2) promote cybersecurity knowledge and innovation.

We are moving forward on this mission and working collaboratively with our public and private sector partners to assess and mitigate cyber risk and prepare for, prevent, and respond to cyber incidents. At the Office of Cybersecurity and Communications (CS&C), we are working to enable and establish a "system-of-systems" approach encompassing the people, processes, and technologies needed to create a front line of defense and grow the nation's capacity to respond to new and emerging threats:

1. First, we continue to enhance the EINSTEIN system's capabilities as a critical tool in protecting our federal executive branch civilian departments and agencies.
2. Second, we are finalizing the National Cyber Incident Response Plan (NCIRP) in collaboration with the private sector and other key stakeholders. The NCIRP provides a framework for effective incident response capabilities and coordination to ensure that all cybersecurity partners—including federal agencies, state and local governments, the private sector and international partners—are prepared to participate in a coordinated and managed response to a cyber incident.
3. Third, and the focus of my testimony today, is our efforts to increase the security of automated control systems that operate elements of our national critical infrastructure. Working with owners and operators of the nation's critical infrastructure and cyber networks, we will continue

to conduct vulnerability assessments, develop training, and educate the control systems community on cyber risks and mitigation solutions.

. . .

Coordination and Integration

The ICS-CERT coordinates control systems-related security incidents and information sharing with federal, state, and local agencies and organizations, as well as private sector constituents including vendors, owners and operators, and international and private sector computer emergency response teams.

In addition, the ICS-CERT leverages relationships with many working groups—including the Industrial Control Systems Joint Working Group and the Federal Control Systems Security Working Group—to increase and improve information sharing with critical infrastructure asset owners and operators and vendor community. It is through these relationships that private sector partners and vendors have called on the ICS-CERT during control systems emergencies and events.

In 2007, the CSSP studied several scenarios to evaluate the impacts of a successful cyber attack on critical control systems infrastructure in several critical infrastructure sectors, including energy and transportation. The studies used hypothetical, but credible, cyber attack scenarios that employed common hacking methods and knowledge of control systems. Consequences of the attacks ranged from multiple-day shutdowns of facilities without death or injury, to extensive system damages, casualties, and billions in economic loss. The scenario development took advantage of open source literature, inhouse and industry cyber experts, CSSP research and documentation, and engineering analysis to assess the feasibility of a cyber attack and derive the outcomes with assessed damage. Additional scenario development and analysis was conducted for cyber attacks on a nuclear power generation plant, an electricity-generating station, and a large industrial facility. This analysis also yielded estimated consequences resulting in significant economic impact, major disruption to services, injuries and potential loss of life.

Stuxnet

While scenario analysis plays an important part of understanding and reducing risk to critical infrastructure, a real-world threat emerged earlier this year that significantly changed the landscape of targeted cyber attacks. Malicious code, dubbed Stuxnet, was detected in July 2010. DHS analysis concluded that this highly complex computer worm was the first of its kind, written to specifically target mission-critical control systems running a specific combination of software and hardware. What makes Stuxnet unique is that it uses a variety of previously seen individual cyber attack techniques, tactics, and procedures, automates them, and hides its presence so that the operator and the system have no reason to suspect that any malicious activity is occurring. The concern for the future of Stuxnet is that the underlying code could be adapted to target a broader range of control systems in any number of critical infrastructure sectors.

The ICS-CERT immediately began to analyze the code and coordinate actions with critical infrastructure asset owners and operators, federal partners, and Information Sharing and Analysis Centers.

Our analysis quickly uncovered that this sophisticated malware has the ability to gain access to, steal detailed proprietary information from, and manipulate the systems that operate mission-critical processes within the nation's infrastructure. The malware is highly complex and contains over 4,000 functions, comparable to the amount of code in some commercial software applications.

Leveraging the unique capabilities and partnership with the Idaho National Laboratory, ICS-CERT was able to conduct sophisticated analysis on Stuxnet. ICS-CERT has documented that the malware was written to look specifically for computers running the Siemens WinCC Human Machine Interface (HMI). It then copies components into the associated Structured Query Language (SQL) database and checks to see if the HMI is connected to certain Siemens Simatic Programmable Logic Controller (PLC) models. If it finds the specific model of PLC, Stuxnet then checks for specific program elements in the PLCs and, if found, attempts to install rogue ladder logic into the PLC program.

ICS-CERT analysis indicates that the logic is only changed when these specific conditions are met. This selective infection criterion, along with the analysis of the logic injected by Stuxnet, indicates that a specific process was likely targeted. However, while we do not know which process was the intended target—it is important to note that the combination of Windows operating software and Siemens hardware can be used in control systems across critical infrastructure sectors—from automobile assembly lines to mixing baby formula to processing chemicals.

Furthermore, ICS-CERT concluded that Stuxnet was professionally created using carefully planned development concepts. The malware implements state-of-the-art techniques and capabilities for infecting a system, preventing detection (to maintain its presence), exfiltrating data, and inhibiting analysis once the code is detected. In other words, this code can automatically enter a system, steal the formula for the product you are manufacturing, alter the ingredients being mixed in your product, and indicate to the operator and your anti-virus software that everything is functioning as expected.

To combat this threat, the ICS-CERT has been actively analyzing and reporting on Stuxnet since it was first detected in July. To date, the ICS-CERT has briefed dozens of government and industry organizations and released multiple advisories and updates to the industrial control systems community describing steps for detecting an infection and mitigating the threat. As always, we attempt to balance the need for public information sharing while limiting the information that malicious actors may exploit.

Looking ahead, the Department is concerned that attackers could use the publicly available information about the code to develop variants targeted at broader installations of programmable equipment in control systems. The ICS-CERT will continue to work with the industrial control systems community to investigate these and other threats through malicious code and digital media analysis, on-site incident response activities, and information sharing and partnerships. The salient lesson of Stuxnet, and other emerging threats, is that the CSSP mission and coordination between DHS and the control systems community are vital to our efforts to protect the nation's critical infrastructure.

SOURCE: Seán P. McGurk, *Statement for the Record before the U.S. Senate Homeland Security and Governmental Affairs Committee*, November 17, 2010, 1–3, 9–13, https://www.hsgac.senate.gov/imo/media/doc/TestimonyMcGurk20101117REVISED.pdf

ANALYSIS

Since its creation, the DHS has struggled to clarify its roles and responsibilities relative to other federal agencies. In particular, the cybersecurity mission, which has been addressed by DHS, the DOD, the Department of Justice, and the intelligence agencies, has proven a difficult responsibility to assign to any single entity. McGurk's discussion of computer emergency response teams (CERTs) is illustrative because it demonstrates an ability to form cooperative teams to respond to any cyber crisis, but to do so, it also requires the various agencies to be continually reacting to those crises rather than being proactive in preventing them. CERTs are a valuable mechanism to bring the resources and capabilities of a wide variety of actors together in order to solve a specific problem, but they might not represent the most effective or efficient means of securing the nation's cyberspace.

- ***Document 74:*** *Leon Panetta, "Remarks on Cybersecurity"*
- ***When:*** October 11, 2012
- ***Where:*** New York City, NY
- ***Significance:*** Secretary of Defense Leon Panetta held the key position in President Barack Obama's cabinet when it came to cybersecurity. He oversaw the centralization of the DOD's various agencies connected to cyber operations, as well as the consolidation of those functions into U.S. Cyber Command, one of the largest organizations in the DOD. In this speech, delivered to the Business Executives for National Security, Panetta adopted an optimistic tone regarding the future of cyber operations but also warned of the possibility of devastating surprise cyberattacks if the United States failed to prepare for such operations.

DOCUMENT

Cyberspace has fundamentally transformed the global economy. It's transformed our way of life, providing two billion people across the world with instant access to

information to communication, to business opportunities. Cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities also come new perils and new dangers. The internet is open. It's highly accessible, as it should be. But that also presents a new terrain for warfare. It is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens. I know that when people think of cybersecurity today, they worry about hackers and criminals who prowl the internet, steal people's identities, steal sensitive business information, steal even national security secrets. Those threats are read and they exist today. But the even greater danger—the danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation.

Let me give you some examples of the kinds of attacks that we have already experienced. In recent weeks, as many of you know, some large U.S. financial institutions were hit by so-called Distributed Denial of Service attacks. These attacks delayed or disrupted services on customer websites. While this kind of tactic isn't new, the scale and speed with which it happened was unprecedented. But even more alarming is an attack that happened two months ago when a very sophisticated virus called Shamoon infected computers in the Saudi Arabian State Oil Company Aramco. Shamoon included a routine called a "wiper," coded to self-execute. This routine replaced crucial systems files with an image of a burning U.S. flab. But it also put additional garbage data that overwrote all the real data on the machine. More than 30,000 computers that it infected were rendered useless and had to be replaced. It virtually destroyed 30,000 computers. Then just days after this incident, there was a similar attack on RasGas of Qatar, a major energy company in the region. All told, the Shamoon virus was probably the most destructive attack that the private sector has seen to date.

These attacks mark a significant escalation of the cyber threat, and they have renewed concerns about still more destructive scenarios that could unfold. For example, we know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity, and water plants and those that guide transportation throughout this country. We know of specific instances where intruders have successfully gained access to these control systems. We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction and even loss of life.

An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches. They could, for example, derail passenger trains or even more dangerous, derail trains loaded with lethal chemicals. They could contaminate the water supply in major cities or shutdown the power grid across large parts of the country. The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a cyber Pearl Harbor, an attack that would cause physical

destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.

The Department of Defense, in large part through the capabilities of the National Security Agency, NSA, has developed the world's most sophisticated system to detect cyber intruders and attackers. We are acting aggressively to get ahead of this problem, putting in place measures to stop cyber attacks dead in their tracks. We are doing this as part of a broad whole of government effort to confront cyber threats.

The Department of Defense also has a role. It is a supporting role but it is an essential role. And tonight, I want to explain what that means. But first let me make clear what it does not mean. It does not mean that the Department of Defense will monitor citizens' personal computers. We're not interested in personal communications or in e-mails or in providing the day to day security of private and commercial networks. That is not our goal. That is not our job. That is not our mission. Our mission is to defend the nation. We defend. We deter, and if called upon, we take decisive action to protect our citizens. In the past, we have done so through operations on land and at sea, in the skies and in space. In this century, the United States military must help defend the nation in cyberspace as well. If a foreign adversary attacked U.S. soil, the American people have every right to expect their national defense forces to respond. If a crippling cyber attack were launched against our nation, the American people must be protected. And if the Commander in Chief orders a response, the Defense Department must be ready to obey that order and to act.

To ensure that we fulfill our role to defend the nation in cyberspace, the department is focusing upon three main tracks. One, developing new capabilities. Two, putting in place the policies and organizations we need to execute our mission. And three, building much more effective cooperation with industry and our international partners.

First, developing new capabilities. DoD is investing more than $3 billion annually in cybersecurity because we have to retain that cutting edge capability in the field. Following our new defense strategy, the department is continuing to increase key investments in cybersecurity even in an era of fiscal restraint. Our most important investment is in skilled cyber warriors needed to conduct operations in cyberspace. Just as DoD developed the world's finest counterterrorism force over the past decade, we need to build and maintain the finest cyber force and operations. We're recruiting, we're training, the best and the brightest in order to stay ahead of other nations. It's no secret that Russia and China have advanced cyber capabilities. Iran has also undertaken a concerted effort to use cyberspace to its advantage. Moreover, DoD is already in an intense daily struggle against thousands of cyber actors who probe the Defense Department's networks, millions of times a day. Throughout the innovative efforts of our cyber operators, we've been trying to enhance the department's cyber defense programs. These systems rely on sensors, they rely on software to hunt down the malicious codes before it harms our systems. We actively share our own experience defending our systems with those running the nation's critical private sector networks. In addition to defending the department's networks, we also help deter attacks. Our cyber adversaries will be far less likely to hit us if they know that

we will be able to link to the attack or that their effort will fail against our strong defenses. The department has made significant advances in solving a problem that makes deterring cyber adversaries more complex, the difficulty of identifying the origins of that attack. Over the last two years, DoD has made significant investments in forensics to address this problem of attribution and we're seeing the returns on that investment. Potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.

But we won't succeed in preventing a cyber attack through improved defenses alone. If we detect an imminent threat that will cause significant, physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us to defend this nation when directed by the president. For these kinds of scenarios, the department has developed the capability to conduct effective operations to counter threats to our national interests in cyberspace. Let me be clear that we will only do so to defend our nation, to defend our interests, to defend our allies and we will only do so in a manner that is consistent with the policy principles and legal frameworks that the department follows for other domains including the law of armed conflict.

Which brings me to the second area of focus, policies and organization. Responding to the cyber threat requires the right policies and organizations across the federal government. For the past year, the Department of Defense has been working very closely with other agencies to understand where are the lines of responsibility when it comes to cyber defense. Where do we draw those lines? And how do those responsibilities get executed? As part of that effort, the department is now finalizing the most comprehensive change to our rules of engagement in cyberspace in seven years. The new rules will make clear that the department has a responsibility, not only to defend DoD's networks, but also to be prepared to defend the nation and our national interests against an attack in or through cyberspace. These new rules make the department more agile and provide us with the ability to confront major threats quickly.

Three years ago, the department took a major step forward by establishing the United States Cyber Command, under the leadership of General Keith Alexander, a four-star officer who also serves as the director of the National Security Agency. Cyber Command has matured into what I believe is a world-class organization. It has the capacity to conduct a full range of missions inside cyberspace. The threat picture could be quickly shared with DoD's geographic and functional combatant commanders, with DHS, with FBI and with other agencies in government. After all, we need to see an attack coming in order to defend against that attack. And we're looking at ways to strengthen Cyber command as well. We must ensure that it has the resources, that it has the authorities, that it has the capabilities required to perform this growing mission. And it must also be able to react quickly to events unfolding in cyberspace and help fully integrate cyber into all of the department's plans and activities.

And finally, the third area is to build stronger partnerships. As I've made clear, securing cyberspace is not the sole responsibility of the United States military or even the sole responsibility of the United States government. The private sector,

government, military, our allies—all share the same global infrastructure and we all share the responsibility to protect it. Therefore, we are deepening cooperation with our closest allies with the goal of sharing threat information, maximizing shared capabilities and determining malicious activities. The president, the vice president, Secretary of State and I have made cyber a major topic of discussion in nearly all of our bilateral meetings with foreign counterparts. I recently met with our Chinese military counterparts just a few weeks ago. As I mentioned earlier, China is rapidly growing its cyber capabilities. In my visit to Beijing, I underscored the need to increase communication and transparency with each other so that we could avoid a misunderstanding or a miscalculation in cyberspace. This is in the interest of the United States, but it's also in the interest of China.

Ultimately, no one has a greater interest in cybersecurity than the businesses that depend on a safe, secure and resilient global, digital infrastructure. Particularly those who operate the critical networks that we must help defend. To defend those networks more effectively, we must share information between the government and the private sector about threats in cyberspace. We've made real progress in sharing information with the private sector. But very frankly, we need Congress to act to ensure that this sharing is timely and comprehensive.

Companies should be able to share specific threat information with the government, without the prospect of lawsuits hanging over their head. And a key principle must be to protect the fundamental liberties and privacy in cyberspace that we are all duty bound to uphold. Information sharing alone is not sufficient. We've got to work with the business community to develop baseline standards for our most critical private-sector infrastructure, our power plants, our water treatment facilities, our gas pipelines. This would help ensure that companies take proactive measures to secure themselves against sophisticated threats, but also take common sense steps against basic threats. Although awareness is growing, the reality is that too few companies have invested in even basic cybersecurity. The fact is that to fully provide the necessary protection in our democracy, cybersecurity legislation must be passed by the Congress. Without it, we are and we will be vulnerable.

SOURCE: Leon Panetta, *Remarks on Cybersecurity to the Business Executives for National Security* (New York City, October 11, 2012), https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136

ANALYSIS

Panetta, in speaking to business executives, sought to build partnerships in the cyber domain, recognizing that the federal government has neither the legal right nor the capacity to protect every computer network in the United States. By creating an information-sharing expectation, he made it far more likely that the major corporations in the nation, particularly those operating in the national security sphere, would be open to cooperation on cyber defenses. It was also an extremely effective rhetorical device to suggest the possibility of a cyber 9/11 attack, and then present the example of the attacks upon Saudi Aramco, which caused millions of dollars in

damages and lost revenues. Given the location of the speech (New York City) and the economic motivations of many of the audience members, the examples he chose proved terrifying and easily understood.

- ***Document 75:*** *Robert S. Mueller, III, "Remarks before the RSA Cyber Security Conference"*
- ***When:*** February 28, 2013
- ***Where:*** San Francisco, CA
- ***Significance:*** Robert Mueller served as the director of the Federal Bureau of Investigation (FBI) from 2001 until 2013. He took office just a week before the September 11 terror attacks, and remained in his position beyond the first term of President Obama's administration. Over his time in office, the U.S. government faced substantial challenges in determining which agencies should take leadership in the cyber domain, both in defensive and offensive operations. The situation was complicated by the creation of the DHS, which brought together a number of federal agencies but did not include the FBI.

DOCUMENT

Lanes in the Road

Let me begin by addressing a recurring question: What are the lanes in the road for federal agencies that handle cyber security? Michael Daniel of the White House has just spoken generally on this topic, but I would like to be more specific.

What is the allocation of responsibilities among DHS, NSA, and the FBI? I do know there has been some confusion as to the roles of these three agencies.

In recent meetings between Janet Napolitano of DHS, Keith Alexander of NSA, and the Bureau, as well as other leaders in our respective agencies, we have sought to ensure we are all on the same page with regard to our particular roles.

The FBI's role—operating domestically—is to anticipate, investigate, attribute, and disrupt cyber intrusions affecting the United States.

Likewise, NSA's role is to gather intelligence on foreign cyber threats and to protect national security systems.

DHS's role is to protect our critical infrastructure and our networks . . . to coordinate mitigation and recovery from major cyber intrusions . . . and to disseminate threat information across various sectors.

One question often posed is that of who exactly is in charge of addressing any particular intrusion. While the answer depends in part on the scope and the nature

of the intrusion, the FBI often will be the first responder because of our nationwide coverage. But the investigative team, at a minimum, should include the expertise of both DHS and NSA.

Our agencies operate under separate authorities and have different roles to play. Yet we also understand that we must work together on every substantial intrusion and share information among the three of us. In other words, notification of an intrusion to one agency should be—and will be—notification to all.

The Role of the Private Sector

Defining these lanes in the road is an important step.

Yet the private sector plays a critical role in cyber security. In this respect, I am reminded of the comparable challenge we faced in the wake of the September 11 attacks.

Improved collaboration and information sharing among federal agencies such as the CIA, NSA, DHS, and the FBI has been vital to our collective success against terrorism over the past decade. But equally critical to our success has been the integration of our state and local law enforcement counterparts through the establishment of Joint Terrorism Task Forces.

I do believe—and I have said in the past—that in the future, the cyber threat will equal or even eclipse the terrorist threat. But the alignment of actors critical to defeating the cyber threat includes a different array of partners.

Today, the private sector is the essential partner if we are to succeed in defeating the cyber threat.

On the one hand, the private sector is a primary victim of cyber intrusions—and your networks contain the evidence of countless such attacks.

On the other hand, you are key to defeating this threat. You possess the information, the expertise, and the knowledge to be an integral partner in this new world. You also build the components of cyber security—the hardware, the software, and the networks—and you drive future technology. Without you, we cannot combine innovation and security.

Removing Obstacles

Yet as I mentioned before, there are a number of hurdles to strengthening the partnership between the public and private enclaves. And I want to mention three here.

First: There is a perception among many that the FBI cares only about prosecuting those responsible for intrusions. That is simply not true.

We learned as a result of the attacks of September 11 that our mission was to use our skills and resources to identify terrorist threats and to find ways of disrupting those threats. Prosecution is but one such avenue. We must be willing to use whatever legal means are available and appropriate—civil, criminal, or other means—to disrupt a particular threat—whether it be a terrorist threat or a cyber threat.

Under this approach, we recognize that at the beginning, any cyber investigation into a substantial intrusion is a search for intelligence that will enable us to define and attribute the particular threat. This has been the mindset at the heart of every terrorism investigation since September 11—and it must be true of every case in the cyber arena as well.

A second obstacle to strong cooperation and information sharing is that we have two separate legal regimes for collecting information about threats. First is the criminal justice regime, which looks to bring individuals to justice. Second is the national security regime, which seeks to identify and to thwart both domestic and external threats. These two regimes have separate statutory frameworks.

Since the attacks of September 11, we have been able, for the most part, to reconcile—and indeed, leverage—these two regimes with respect to counterterrorism. And by leverage, I mean using the strength of the criminal justice process to generate intelligence as a result of obtaining the cooperation of defendants.

The conflicts between these two regimes—which largely have been resolved in the counterterrorism arena—must also be addressed in the cyber arena.

Resolving these conflicts depends upon identifying particular factual scenarios and then applying a specific legal analysis that seeks to make full use of our capabilities under one—or, indeed, both—of these regimes.

Improved Understanding

A third obstacle we face is a lack of mutual understanding of basic concepts.

In the cyber arena, terminology has run amok. And by that I mean, who among you knows the meaning of all of the following: NCCIC . . . NTOC . . . ISMA . . . ASIS . . . BACSS . . . not to mention our own NCIJTF? I could go on and on.

There are so many affected participants at so many levels, each with their own jargon, that it is often difficult to comprehend what is being said. That is so without even considering the proliferation of acronyms in the government and elsewhere.

Collectively, we must strive to clarify our common language in this area and adopt a glossary that seeks to simplify the concepts being articulated.

We must overcome these several obstacles by building bridges between the federal government and the private sector. We in the FBI have undertaken a number of initiatives to build such bridges to better protect our critical infrastructure and to share threat information.

One is the Domestic Security Alliance Council, which includes chief security officers from more than 200 companies, representing every critical infrastructure and business sector.

Another is InfraGard, which has grown from a single chapter in 1996 to 88 chapters today. InfraGard has nearly 55,000 members nationwide, representing government, the private sector, academia, and law enforcement.

And just last week, the Bureau held the first session of our National Cyber Executive Institute, a three-day seminar to train leading industry executives on cyber threat awareness and information sharing.

True Collaboration

But as noteworthy as these outreach programs may be, we must do more. We need to shift to a model of true collaboration. A model of working side-by-side, as a matter of course . . . rather than just outreach from one to the other.

We must build structured partnerships within our respective enclaves—both in government and in the private sector. We then must develop channels for

sharing information and intelligence more quickly and effectively between these two enclaves.

Unfortunately, there is no quick fix to this problem. From the perspective of the private sector, disclosing information to the government raises the specter of privacy issues and lawsuits, loss of competitive edge, and bad publicity.

From the perspective of the government, sharing information with the private sector is inhibited by statutes protecting certain classes of information—such as grand jury testimony or classified information—as well as the threat of disclosure of sources and methods.

When I say there is no quick fix, I mean there is no one protocol that will solve each of these problems. But it is essential that we address the various strands of this Gordian knot to allow the exchange of information.

The National Cyber Investigative Joint Task Force, or NCIJTF—one of those unfortunate acronyms I referenced earlier—is one example of an effective partnership in the federal enclave. It comprises 19 separate agencies and serves as a national focal point for cyber threat information.

A wholly private entity, on the other hand, is the National Cyber Forensics and Training Alliance—a proven model for sharing private sector intelligence in collaboration with law enforcement. Located in Pittsburgh and with access to more than 700 subject matter experts, the Alliance includes more than 80 industry partners from many sectors—including financial services, telecommunications, retail, and manufacturing. It works together with federal and international partners to provide real-time threat intelligence every day.

Another such initiative, known as the Enduring Security Framework, includes top leaders from the private sector and the federal government. This partnership shows that the solution to cyber security lies not only with information sharing, but also with joint problem solving.

The framework addresses discrete threats such as DDoS attacks, malware, and emerging vulnerabilities in both software and hardware, such as one finds in mobile devices. It analyzes not only current threats, but also those we can anticipate down the road. In this way, we can resolve potential issues before the damage is done—before your company becomes a victim.

These entities are steps in the right direction. But we must build on these initiatives to expand the channels of information sharing and collaboration.

Consider a unique DDoS attack, for example. We can move faster and more efficiently if we have an experienced team in place—one with experts from both the private sector and government—experts who have worked together and who are focused on issues affecting specific sectors.

The sooner we have teams in place to dissect these issues, the sooner we can develop long-term strategies to resolve and—indeed—anticipate them.

In seeking a concrete way forward on any of these issues, we need your input and your expertise.

We do not merely want our private sector partners to report one-off intrusions after the fact—although such reporting is important. We want to work with you to identify anomalies or other signs that will help us forecast a coming attack, or that highlight a vulnerability to an attack.

For our part, the Bureau and our government partners must do more to provide you with better information in real time.

We must put into place the mechanism for sharing intelligence concerning vulnerabilities without necessarily disclosing the classified context of these vulnerabilities. The president's recent executive order concerning cyber security mandates important steps in this direction.

Likewise, we do not need to know each and every detail about your intellectual property, your trade secrets, your proprietary information, your clients, or even your customers. We need information about threats and attacks so that we can work with you to address them.

Only by establishing channels to share information swiftly will we be capable of warning one another of pending attacks. We must put into place the mechanisms—both public and private—to meet those threats and to identify and deter similar events in the future.

And we must fuse private sector information with information from the intelligence community to produce a complete picture of cyber threats—one that benefits all of us. For only by having a common picture can we effectively disrupt those threats.

The People Behind the Keyboards

One last thought that I ask you to keep in mind: We must remember that behind every intrusion there is an individual—not a computer, but a criminal—responsible for that intrusion. We must remember that cyber security is not just defending the ones and the zeros.

For two decades, cyber security has focused principally on reducing vulnerabilities—through more complex firewalls, dual-factor authentication, aggressive password policies, and the like.

While these are worthwhile efforts, they cannot fully eliminate our vulnerabilities. We must identify and deter the persons behind those computer keyboards. And once we identify them—be they state actors, organized criminal groups, or 18-year-old hackers—we must devise a response that is effective, not just against that specific attack, but for all similar illegal activity.

We often think of cyber investigations as unique in nature. And yes, they do require a certain expertise. But our success in resolving cyber investigations rests on investigative techniques we have used in cases throughout the FBI's history—physical surveillance, forensics, cooperating witnesses, sources, and court-ordered wire intercepts.

Let me share an example of how this works.

The combination of technical skills and traditional investigative techniques recently led the FBI to the hacker known as "Sabu"—one of the co-founders of the hacktivist group LulzSec.

This case began when our Los Angeles Division collected numerous IP addresses used to hack into the database of a TV game show. Meanwhile, our New York Field Office used a combination of investigative techniques, including human sources, search warrants, and surveillance, to identify and locate the man known as Sabu—who had failed to anonymize his IP address during this intrusion.

We went to arrest him, and we gave him a choice: Go to jail now, or cooperate.

Sabu agreed to cooperate, and he became a source, continuing to use his online identity. His cooperation helped us build cases that led to the arrest of six other hackers linked to groups such as Anonymous and LulzSec. It also allowed us to identify hundreds of security vulnerabilities—which helped us to stop future attacks and limit harm from prior intrusions.

. . .

Defeating today's complex cyber threats requires us to continually evolve and adapt.

We need to abandon the belief that better defenses alone will be sufficient. And we need to stop thinking we can defeat this threat by acting on our own.

Instead of just building better defenses, we must build better relationships. And we must overcome the obstacles that prevent us from sharing information and, most importantly, collaborating.

If we do these things—and if we bring to these tasks the sense of urgency that this threat demands—I am confident that we can and will defeat cyber threats, now and in the years to come.

SOURCE: Robert S. Mueller, III, *Remarks before the RSA Cyber Security Conference* (San Francisco, CA, February 28, 2013), https://archives.fbi.gov/archives/news/speeches/working-together-to-defeat-cyber-threats

ANALYSIS

Mueller's remarks clarify many of the inherent challenges that faced different federal agencies when attempting to sort out authorities and responsibilities in the cyber domain. Without clear guidance from either the legislature or the executive branch, each agency's leader effectively decided for their entire organization how involved they should be in the cyber domain. The result was a chaotic mess of overlapping boundaries and expectations, and a shockingly vulnerable U.S. cyber infrastructure. Although each of the agencies had the best interests of the U.S. public in mind, the variations in procedures, capabilities, and resources meant that many efforts were duplicative, while key networks were occasionally effectively left unprotected. The result was a string of very embarrassing and damaging cyber espionage campaigns against virtually every federal agency of note, with no single agency or individual held responsible for the failure to protect the nation's secrets. Ironically, from 2017 through 2019, Mueller headed an investigative team that examined the possibility of collusion between the Donald Trump election campaign and the Russian government, with special emphasis upon Russian uses of cyberspace to promote Vladimir Putin's agenda.

- ***Document 76:*** *Statement of General Keith B. Alexander before the Senate Committee on Armed Services*
- ***When:*** March 12, 2013
- ***Where:*** Washington, D.C.

- ***Significance:*** General Keith Alexander served as the commander of U.S. Cyber Command (USCYBERCOM) and the National Security Agency (NSA). In this capacity, he essentially linked the military and intelligence organizations most devoted to cyber activities under a single leader. This allowed a much more effective and efficient approach to cyber defense, and, if necessary, cyber offense. In this testimony, Alexander sought to demonstrate the rising dangers of cyberattacks upon unprotected systems.

DOCUMENT

The Strategic Landscape

U.S. Cyber Command operates in a dynamic and contested environment that literally changes its characteristics each time someone powers on a networked device. Geographic boundaries are perhaps less evident in cyberspace, but every server, fiber-optic line, cell tower, thumb drive, router, and laptop is owned by someone and resides in some physical locale. In this way cyberspace resembles the land domain—it is all owned, and it can be reshaped. Most networked devices, for example, are in private hands, and their owners can deny or facilitate others' cyber operations by how they manage and maintain their networks and devices. Cyberspace as an operating environment also has aspects unique to it. Events in cyberspace can seem to happen instantaneously. Data can appear to reside in multiple locations. There is a great deal of anonymity, and strongly encrypted data are virtually unreadable. In cyberspace, moreover, sweeping effects can be precipitated by states, enterprises, and individuals, with the added nuance that such cyber actors can be very difficult to identify. The cyber landscape also changes rapidly with the connection of new devices and bandwidth, and with the spread of strong encryption and mobile devices. Despite the unique characteristics of cyberspace, states still matter because they can affect much of the physical infrastructure within their borders. Convergence is our watchword; our communications, computers, and networks are merging into one digital environment as our political, economic, and social realms are being re-shaped by the rush of innovation.

In this environment that is both orderly and chaotic, beneficial and perilous, we at USCYBERCOM have to focus on actors who possess the capability—and possibly the intent—to harm our nation's interests in cyberspace or to use cyber means to inflict harm on us in other ways. Unfortunately, the roster of actors of concern to us is growing longer and growing also in terms of the variety and sophistication of the ways they can affect our operations and security.

State actors continue to top our list of concerns. We feel confident that foreign leaders believe that a devastating attack on the critical infrastructure and population of the United States by cyber means would be correctly traced back to its source and elicit a prompt and proportionate response. Nonetheless, it is possible that some

future regime or cyber actor could misjudge the impact and the certainty of our resolve.

We have some confidence in our ability to deter major state-on-state attacks in cyberspace but we are not deterring the seemingly low-level harassment of private and public sites, property, and data. As former Secretary of Defense Panetta explained to an audience in New York last October, states and extremist groups are behaving recklessly and aggressively in the cyber environment. Such attacks have been destructive to both data and property. The Secretary mentioned, for example, the remote assaults last summer on Saudi Aramco and RasGas, which together rendered inoperable—and effectively destroyed the data on—more than 30,000 computers. We have also seen repressive regimes, desperate to hold on to power in the face of popular resistance, resort to all manner of cyber harassment on both their opponents and their own citizens caught in the crossfire. Offensive cyber programs and capabilities are growing, evolving, and spreading before our eyes; we believe it is only a matter of time before the sort of sophisticated tools developed by well-funded state actors find their way to non-state groups or even individuals. The United States has already become a target. Networks and websites owned by Americans and located here have endured intentional, state-sponsored attacks, and some have incurred damage and disruption because they happened to be along the route to another state's overseas targets.

Let me draw your attention to another very serious threat to U.S. interests. The systematic cyber exploitation of American companies, enterprises, and their intellectual property continued unabated over the last year. Many incidents were perpetrated by organized cybercriminals. Identity and data theft are now big business, netting their practitioners large profits and giving rise to an on-line sub-culture of markets for stolen data and cyber tools for stealing more. Much cyber exploitation activity, however, is state-sponsored. Foreign government-directed cyber collection personnel, tools, and organizations are targeting the data of American and western businesses, institutions, and citizens. They are particularly targeting our telecommunications, information technology, financial, security, and energy sectors. They are exploiting these targets on a scale amounting to the greatest unwilling transfer of wealth in history. States and cybercriminals do not leave empty bank vaults and file drawers behind after they break-in—they usually copy what they find and leave the original data intact—but the damage they are doing to America's economic competitiveness and innovation edge is profound, translating into missed opportunities for U.S. companies and the potential for lost American jobs. Cyber-enabled theft jeopardizes our economic growth. We at USCYBERCOM work closely with our interagency partners to address these threats.

We must also watch potential threats from terrorists and hacktivists in cyberspace. The Intelligence Community and others have long warned that worldwide terrorist organizations like al Qaeda and its affiliates have the intent to harm the United States via cyber means. We agree with this judgment, while noting that, so far, their capability to do so has not matched their intent. This is not to downplay the problem of terrorist use of the internet. Al Qaeda and other violent extremist groups are on the Web proselytizing, fundraising, and inspiring imitators. We should not ignore the effectiveness with which groups like al Qaeda and its affiliates

radicalize ever larger numbers of people each year—on more continents. The Federal Bureau of Investigation and other agencies cite instances in which would-be terrorists found motivation and moral support for suicide attacks at jihadist websites and chat rooms. This is an especially serious and growing problem in areas of hostilities where our troops and personnel are deployed. Another threat that is not growing as fast as we might have feared, on the other hand, is that of hacktivists with a cause or a grievance that leads them to target U.S. government and military networks. Our vulnerabilities to this sort of disruption remain, but 2012 saw fewer such incidents than 2011.

Looking Ahead: The Command's Priorities

I have established several priorities for U.S. Cyber Command in dealing with these risks and threats. We are actively working to guard the Department of Defense's networks and information and helping to defend the nation. Key to countering these threats is learning how to grow our capabilities in this challenging domain. We have no alternative but to do so because every world event, crisis, and trend now has a cyber-aspect to it, and decisions we make in cyberspace will routinely affect our physical or conventional activities and capabilities as well. USCYBERCOM is building cyber capabilities into our planning, doctrine, and thinking now—while we as a nation have time to do so in a deliberate manner. We do not want to wait for a crisis and then have to respond with hasty and ad hoc solutions that could do more harm than good.

When I say we are normalizing cyber operations, I mean we are making them a more reliable and predictable capability to be employed by our senior decisionmakers and Combatant Commanders. Normalizing cyber requires improving our tactics, techniques, and procedures, as well as our policies and organizations. It also means building cyber capabilities into doctrine, plans, and training – and building that system in such a way that our Combatant Commanders can think, plan, and integrate cyber capabilities as they would capabilities in the air, land and sea domains.

In keeping with the Department of Defense's Strategy for Operating in Cyberspace, U.S. Cyber Command and NSA are together assisting the Department in building: 1) a defensible architecture; 2) global situational awareness and a common operating picture; 3) a concept for operating in cyberspace; 4) trained and ready cyber forces; and 5) capacity to take action when authorized. Indeed, we are finding that our progress in each of these five areas benefits our efforts in the rest. We are also finding the converse—that inertia in one area can result in slower progress in others. I shall discuss each of these priorities in turn.

Defensible Architecture: The Department of Defense (DoD) owns seven million networked devices and thousands of enclaves. Cyber Command works around the clock with its Service cyber components, with NSA, and with DISA to monitor the functioning of DoD networks, including the physical infrastructure, the configurations and protocols of the components linked by that infrastructure, and the volume and characteristics of the data flow. This is a dynamic defense, and it consistently provides better security than the former patch-and-firewall paradigm. Patches and firewalls are still necessary—I wish everyone kept theirs up-to-date—but they are an insufficient

defense for DoD networks. Dynamic defenses have brought about noticeable improvements in the overall security of DoD information environment. We know for a fact that our adversaries have to work harder to find ways into our sensitive but unclassified networks. Unfortunately, adversaries are willing to expend that effort, and DoD's architecture in its present state is not defensible over the long run. We in the Department and the Command are crafting a solution. The Department's bridge to the future is called the DoD Joint Information Environment (JIE), comprising a shared infrastructure, enterprise services, and a single security architecture to improve mission effectiveness, increase security, and realize information technology (IT) efficiencies. The JIE will be the base from which we can operate in the knowledge that our data are safe from adversaries. Senior officers from USCYBERCOM and NSA sit on JIE councils and working groups, playing a leading role with the office of the DoD's Chief Information Officer, Joint Staff J6, and other agencies in guiding the Department's implementation of the JIE. NSA, as the Security Adviser to the JIE, is defining the security dimension of that architecture, and has shown how we can pool big data and still preserve strong security. We have even shared the source code publicly so public and private architectures can benefit from it. DoD is benefitting from that knowledge and from our growing understanding of the totality of measures, procedures, and tools required to assure the health and security of even the biggest networks and databases.

Increased Operational Awareness: Enhanced intelligence and situational awareness in our networks will help us know what is happening in the cyberspace domain. This effort can be likened to a cyber version of the tactical air picture of friendly, neutral, and aggressor aircraft that a Combined Air Operations Center in a Combatant Command typically maintains. We are now issuing a weekly Cyber Operating Directive (CyOD) across the DoD cyber enterprise for just this purpose, so that all friendlies understand what is happening in cyberspace. Our improving knowledge of what is normal in cyberspace is crucial to grasping what is not normal. We at USCYBERCOM are also helping DoD increase our global situational awareness through our growing collaboration with federal government mission partners like the Department of Homeland Security (DHS), the FBI, and other departments and agencies, as well as with private industry and with other countries. That collaboration in turn allows us to better understand what is happening across the cyber domain, which enhances our situational awareness, not only for the activities of organizations based at Fort Meade but also across the U.S. government. I am happy to report that at least one of our foreign partners has volunteered to invest in this and enter its own network traffic data to contribute to a common picture.

Operating Concepts: Our operating concept calls for us to utilize our situational awareness to recognize when an adversary is attacking, to block malicious traffic that threatens our networks and data, and then to maneuver in cyberspace to block and deter new threats. I am pleased to report that in December, the Department endorsed the force presentation model we need to implement this new operating concept. We are establishing cyber mission teams in line with the principles of task organizing for the joint force. The Services are building these teams to present to U.S. Cyber Command or to support Service and other Combatant Command missions. The teams are analogous to battalions in the Army and Marine Corps—or

squadrons in the Navy and Air Force. In short, they will soon be capable of operating on their own, with a range of operational and intelligence skill sets, as well as a mix of military and civilian personnel. They will also have appropriate authorities under order from the Secretary of Defense and from my capacity as the Director of NSA. Teams are now being constructed to perform all three of the missions given to U.S. Cyber Command. We will have 1) a Cyber National Mission Force and teams to help defend the nation against national-level threats; 2) a Cyber Combat Mission Force with teams that will be assigned to the operational control of individual Combatant Commanders to support their objectives (pending resolution of the cyber command and control model by the Joint Staff); and 3) a Cyber Protection Force and teams to help operate and defend DoD information environment.

Trained and Ready Forces: Each of these cyber mission teams is being trained to common and strict operating standards so that they can be on-line without putting at risk our own military, diplomatic, or intelligence interests. Doing this will give not only U.S. Cyber Command's planners, but more significantly our national leaders and Combatant Commanders, a certain predictability in cyber capabilities and capacity. Key to building out the Cyber Mission Force articulated in our Force Planning Model is having the training system in place to train each of the cyber warriors we need, in the skill sets we require and at the quality mandated by the cyber mission. We have that training system in place for the operators, and now we need to build the accompanying Command and Staff academic support packages and programs to ensure our officers and planners know how to effectively plan for and employ cyber capabilities for our nation. As a result of this operator and staff training system, decisionmakers who require increments of cyber skills to include in their plans will know how to ask for forces to fill this requirement, and planners will know how to work cyber effects into their organizations' plans. To build the skills of the force—as well as to test the ways in which its teams can be employed—U.S. Cyber Command has sponsored not only an expanding range of training courses but also two important exercises, CYBER FLAG and CYBER GUARD. The latter assembled 500 participants last summer including a hundred from the National Guards of twelve states. They exercised state and national-level responses in a virtual environment, learning each other's comparative strengths and concerns should an adversary attack our critical infrastructure in cyberspace. CYBER FLAG is our annual exercise at Nellis Air Force Base in Nevada and we conduct it with our inter-agency and international partners. Our most recent running of CYBER FLAG introduced new capabilities to enable dynamic and interactive force-on-force maneuvers at net-speed, while incorporating actions by conventional forces as well at Nellis' nearby training area.

Capacity to Take Action: Successful operations in cyberspace depend on collaboration between defenders and operators. Those who secure and defend must synchronize with those who operate, and their collaboration must be informed by up-to-date intelligence. I see greater understanding of the importance of this synergy across the Department and the government. The President recently clarified the responsibilities for various organizations and capabilities operating in cyberspace, revising the procedures we employ for ensuring that we act in a coordinated and mutually-supporting manner. As part of this progress, the Department of Defense and U.S. Cyber Command are being integrated in the machinery for National Event

responses so that a cyber incident of national significance can elicit a fast and effective response to include pre-designated authorities and self-defense actions where necessary and appropriate. USCYBERCOM is also working with the Joint Staff and the Combatant Commands to capture their cyber requirements and to implement and refine interim guidance on the command and control of cyber forces in-theater, ensuring our cyber forces provide direct and effective support to commanders' missions while also helping U.S. Cyber Command in its national level missions. In addition, we are integrating our efforts and plans with Combatant Command operational plans and we want to ensure that this collaboration continues at all the Commands. Finally, most cyber operations are coalition and interagency efforts, almost by definition. We gain valuable insight from the great work of other partners like the Departments of Justice and Homeland Security, such as in their work against distributed denial of service attacks against American companies, which in turn helps DoD finetune defenses for the DoD information environment. We also benefit from sharing with the services and agencies of key partners and allies. We welcome the interagency collaboration and evolving frameworks under which these efforts are proceeding, especially such revisions that would make it easier for the U.S. Government and the private sector to share threat data, as the administration previously emphasized. In addition, new standing rules of engagement for cyber currently under development will comply with and support recently issued policy directives on U.S. cyber operations.

Building for the Future

We have made strides in all of our focus areas, though what gratifies me the most is seeing that we are learning how they all fit together. We are building quickly and building well, but we are still concerned that the cyber threats to our nation are growing even faster. From the technological, legal, and operational standpoints we are learning not only what is possible to accomplish but also what is wise to attempt. Our plans for U.S. Cyber Command over the foreseeable future—which admittedly is not a very distant horizon—should be understood in this context.

In a speech last fall, then-Secretary Panetta emphasized the Department's need to adjust our forces as we transition away from a decade of war. He explained that a wise adjustment makes cuts without hollowing out the force, while also investing in ways that prepare us to meet future needs. We will do that, he said, by increasing our investments in areas including space and cyber. It is fair to ask how we plan to use such new resources while others are trimming back. Our new operating concept to normalize cyber capabilities is just the sort of overarching theme to unite the whole institutional push. We need to foster a common approach to force development and force presentation—up to and including the Service component and joint headquarters—given the intrinsically joint nature of this domain.

Let me emphasize that this is not a matter of resources alone—it is a matter of earning trust. We will continue to do our work in full support and defense of the civil liberties and privacy rights enshrined in the U.S. Constitution. We do not see a tradeoff between security and liberty. We can and must promote both simultaneously because each enhances the other. U.S. Cyber Command takes this responsibility very seriously. Indeed, we see this commitment in our day-by-day successes. We

in the Department of Defense and DHS, with DOJ and industry, for instance, have shown that together we can share threat information, to include malware signatures, while still providing robust protection for privacy and civil liberties.

Building the Department's defensible cyber architecture will let us guard our weapons systems and military command and control as well as our intelligence networks. We hope to take the savings in personnel and resources gained by moving to the JIE and have the Services repurpose at least some of them to hunt for adversaries in our DoD networks and even to perform full-spectrum operations. Although doing so will require a large investment of people, resources, and time, in the long run it will be cheaper to train Service personnel than to hire contractors. Moving to the JIE will make sharing and analytics easier while also boosting security. I know this sounds paradoxical but it is nonetheless true, as NSA has demonstrated in its Cloud capability. If we know what is happening on our networks, and who is working in them and what they are doing, then we can more quickly and efficiently see and stop unauthorized activities. We can also limit the harm from them and more rapidly remedy problems, whether in recovering from an incident or in preventing one in the first place. This is our ultimate objective for operations on our Department of Defense information architecture.

As we grow capacity, we are building cyber mission teams now , with the majority supporting the Combatant Commands and the remainder going to USCYBERCOM to support national missions. When we have built this high-quality, certified, and standardized force, we will be able to present cyber forces with known capability sets to our Combatant Commanders—forces they can train with, plan for, plan on, and employ like forces and units any other military domain. This gets at the essence of normalizing cyber capabilities for the Department of Defense. Furthermore, we want to increase the education of our future leaders by fully integrating cyber in our existing war college curricula. This will further the assimilation of cyber into the operational arena for every domain. Ultimately we could see a war college for cyber to further the professional military education of future leaders in this domain.

SOURCE: Keith B. Alexander, *Statement before the Senate Committee on Armed Services* (Washington, D.C., 2013), 2–9, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-091.pdf

ANALYSIS

One of the great challenges for USCYBERCOM is the need to provide protection for U.S. computer networks that are not directly under the control of the federal government and the U.S. military, while also maintaining respect for privacy laws and the individual rights of citizens. At times, Alexander had to be frustrated by the inherent difficulties of operating within an open, democratic, capitalist society while attempting to parry the cyber offensives of autocratic regimes. Yet, he managed to not only achieve the key elements of his mission but also expand the government-private partnerships within cyberspace, while also educating legislative leaders about the unique challenges of operating in the cyber domain.

- ***Document 77:*** *Keith Alexander, "Remarks at AFCEA International Cyber Symposium"*
- ***When:*** June 28, 2013
- ***Where:*** Baltimore, MD
- ***Significance:*** General Keith Alexander was the first commander of USCYBERCOM, named to the position after the creation of the unified command in 2010. He had already served as the director of the NSA since 2005. At the time of this speech, Edward Snowden had just revealed an enormous amount of classified information, leaking it through WikiLeaks, ostensibly after a crisis of conscience regarding surveillance programs conducted by the NSA and other intelligence agencies.

DOCUMENT

Before I go into my cyber discussion, I thought it was important for me to address some of the media leaks that are going on, and I think it's important that you hear from me some of this. I want to make six key points.

First, our responsibility, my main responsibility is defense of this country. These programs are part of that effort. In 2001, after 9/11, it was determined by the 9/11 Commission that the intelligence community could not connect the dots, foreign and domestic. We set about as a community to figure out how could we connect those dots. What programs do we need? And how do we do this under a legal framework? And we set up these two programs, 215, Section 215 for the business records FISA, and 702, as two of the capabilities look at a methodology to help us connect those dots. These capabilities were approved by the administration—thank you—Congress and the FISA court. With these exceptional authorities came equally exceptional oversight by all three branches of the government. These programs are focused with distinct purposes and oversight mechanisms. We understand and support the need to ensure we protect both civil liberties and national security. It's not one or the other. It must be both. That's why we take oversight of these programs very seriously.

A report issued by the Senate Select Intelligence Committee in June 2012, in support of the reauthorization of the 2008 amendments to FISA, emphasized that the government implements this authority in a responsible manner. And I quote: "Through four year of oversight, the committee has not identified a single case in which a government official engaged in willful effort to circumvent or violate the law—not one case in four years."

I'd like to just give you some insights on the business record FISA first and use an analogy using a lockbox. Under the business record FISA, or Section 215, we take

the metadata from the service providers and place it into a virtual lockbox. The only way NSA can go into that lockbox is if we have what is called reasonable, articulable suspicion of a selector that is related to terrorism. In all of 2012, we approved less than 300 selectors – such as telephone numbers – to initiate queries into that virtual lockbox. There has to be a foreign nexus, an association with al-Qaida or other specified terrorist organizations.

Operation High Rise is a great case in point. Now I won't give this as good as the deputy director of the FBI, Sean Joyce, did in our open hearing before the House last week, but I think it's important just to discuss this one, and then the others you can look at that open testimony and see what Sean actually said.

But just to review for you, Op High Rise: NSA was tracking terrorists in Pakistan. We used FAA 702 to get their email. We compelled that service provider to get us that email under a court order, that FAA 702. With that, armed with that information, we found that they were—this guy in Pakistan, an al-Qaida terrorist, was talking to a guy on email we believed to be in Colorado. We gave that to the FBI. That's our job: helping to connect the dots. In that, there was a telephone number that the FBI came up and said, hey, this is Najibullah Zazi, and we are concerned about this. We then used the business record FISA to go look in that virtual lockbox. We took that number, we got reasonable, articulable suspicion and we looked in that lockbox, and we found that Zazi was talking to a guy in New York who had connections to other terrorist elements for another operation on the second plot and others on a third plot. That information, along with information—the Customs and Border Patrol, CIA and our entire community brings together helped FBI stop that plot. We got that information in early September 2009 for an attack that was supposed to take place in mid-September. It would have been the biggest al-Qaida attack on American soil since 9/11. We were privileged and honored to be a part of disrupting that plot. FAA 702 was the initial tip. That's how important these programs are.

My third point: These programs have helped us connect the dots, as I've just used in Op High Rise, but our allies have benefited, too. On 21 June, last week, last Friday, we provided 54 cases to several congressional committees in which these programs contributed to our understanding, and in many cases, helped enable the disruption of terrorist plots in the U.S. and in over 20 countries throughout the world. It is important to note we are part of a larger government that includes our great partners at FBI, CIA, DHS, the Defense Department, as well as many others. We also partner with our allies in combatting terrorism. Here are some statistics of those 54 events.

Of the 54, 42 involved disruptive plots—disrupted plots. Twelve involved cases of material support to terrorism. Fifty of the 54 cases led to arrests or detentions. Our allies benefited, too. Twenty-five of these events occurred in Europe, 11 in Asia and five in Africa. Thirteen events had a homeland nexus. In 12 of those events, Section 215 contributed to our overall understanding and help to the FBI—twelve of the 13. That's only with a business record FISA can play. In 53 out of 54 events, Section 702 data played a role, and in many of these cases, provided the initial tip that helped unravel the threat stream. A significant portion, almost half of our counterterror reporting, comes from Section 702.

Fourth, these programs operate under a rigorous oversight framework from all three branches of our government. FISA provides that in order to target the content of a U.S. persons communications anywhere in the world, NSA and the rest of our government requires a finding of probable cause under a specific court order. This translates into significant information on—these capabilities translate into significant information on ongoing terrorist activities with no willful violations of our law.

Fifty-four terrorist activities disrupted; zero willful violations. When you think about how our government operates and what we've done to bring all three branches together, I think that's something to be proud of. We have defended the nation 54 times, and our allies, and we have ensured the protection of our civil liberties and privacy in oversight by all three forms of our—all three branches of our government. I think that's what the nation expects our government to do, disrupt terrorist activities, defend our civil liberties and privacy.

Most nations around the world are capable and do collect signals intelligence, just like we do. And their governments use lawful intercept efforts that require and compel companies to provide the requested information. I think our nation is among the best at protecting our privacy and civil liberties.

And I'll just give you an aside: When President Obama came into office, I met with him in the first few weeks on these programs. And he wanted to make sure that they were essential for defending the nation and that we could, with these, still protect our civil liberties and privacy, and he pushed us in that. Along with Congress, we came up with additional measures and for NSA, we built out of those meetings our directorate of compliance to make another step in ensuring we're doing this exactly right.

Sixth, my sixth point—I'm getting through this, bear with me—public discussion of NSA's tradecraft or the tools that support its operation provides insights that our adversaries, to include terrorists, can and do use to hide their activities. Those who wish us harm now know how we counter their actions.

These leaks have caused significant and irreversible damage to our nation's security. Historically, every time a capability is revealed, we lose our ability to track those targets. What is going on in these leaks is unconscionable, in my opinion, and it hurts our nation and our allies and it's flat wrong.

There are lawful and legitimate mechanisms to raise concerns about these programs. NSA, DOD and DNI all have whistle-blower programs and investigator generals who are in a position to do this. An individual acting nobly would have chosen one of those as a course of action to reveal his concerns.

I worry that there will be more leaks and that they will attempt to further sensationalize this issue. I'd ask you to remember that context matters, that these authorities are carefully debated and considered across three branches of government and that we only employ these capabilities that we believe are both useful and necessary.

As you may have read in the media, NSA previously had an email metadata program analogous to the telephony program that has been the subject of some of this recent discussion. This program was conducted under a different provision of the Patriot Act. As has already been noted by senior officials in public comments

recently, this program was terminated in 2011, because it didn't have the operational impact that we needed. That was a choice that came from us, from NSA; we started that debate and said, this did not have the value to stop the terrorist attacks that we need. We went forward to the administration and Congress and with all their support, shut that program down because it wasn't meeting what we needed and we thought we could better protect civil liberties and privacy by doing away with it, and all that data was purged at that time.

So what does that come to? A conclusion: First, the damage is real. I believe the irresponsible release of classified information about these programs will have a long-term detrimental impact on the intelligence community's ability to detect future attacks. These leaks have inflamed and sensationalized for ignoble purposes the work the intelligent (sic) community does lawfully under strict oversight and compliance.

If you want to know who's acting nobly, look at the folks at NSA, FBI, CIA and the Defense Department that defend our nation every day and do it legally and protect our civil liberties and privacy. They take an oath to our Constitution to uphold and defend that Constitution. And they take that oath seriously and they do a great job. They're the heroes that our nation should be looking at. They're the ones that are taking care of us and they're the ones protecting our civil liberties and privacy.

So that's all I wanted to say on the leaks.

SOURCE: Keith Alexander, *Remarks at the AFCEA International Cyber Symposium*, (Baltimore, MD, June 28, 2013), https://www.nsa.gov/news-features/speeches-testimonies/Article/1620137/remarks-by-gen-keith-alexander-commander-us-cyber-command-uscybercom-director-n/

ANALYSIS

Alexander's frustration regarding the leaks is palpable in this speech. Of course, he was in a position to understand the most likely long-term outcomes from the leaks, something that probably was not true for Edward Snowden. General Alexander's desire to clarify the programs being undertaken by the NSA, and their successes in disrupting terror plots against the United States and its allies, is certainly understandable. However, the Snowden leaks suggested that the surveillance and data collections systems were not quite so well-protected and controlled as Alexander might believe. The systems were certainly ripe for abuse, even if they had been effective in defeating specific plots—Snowden's ability to access the underlying data is simply one case in point. Although Alexander was correct to note that the Snowden leaks undermined the NSA's ability to conduct many of its missions, particularly in the fashion it had employed before the leaks, the leaks also conveyed to the public the level of government surveillance that was not only possible but actually being conducted at all times. While the NSA might have remained under careful control regarding the release of information, there was no guarantee that those capabilities would not be turned to more nefarious uses in the future.

- ***Document 78:*** *Michael Rogers, "Testimony before the U.S. House Intelligence Committee"*
- ***When:*** November 20, 2014
- ***Where:*** Washington, D.C.
- ***Significance:*** In 2014, Admiral Michael Rogers assumed command of USCYBERCOM and also became the director of the NSA. His testimony before the House Intelligence Committee allowed him to offer thoughts on the current state of cyber affairs particularly as pertained to long-term cyber espionage efforts against the United States and its private entities.

DOCUMENT

ADMIRAL MICHAEL ROGERS: I would start out by highlighting I don't think there should be anybody's mind that the cyber challenges we're talking about are not theoretical. This is something real that is impacting our nation and those of our allies and friends every day. And it is doing it in a meaningful way that is literally costing us hundreds of billions of dollars, that is leading to a reduced sense of security and that has the potential to lead to truly significant, almost catastrophic failures if we don't take action.

It also highlights to all of us, I think, that there is no one single group or party—party in the sense of whether it be government, whether it be the private sector—the challenges here are so broad that the idea that one sector or one individual organization is going to solve this, I just don't think is realistic. It is going to take a true partnership between the private sector, the government and academia to address the challenges we have.

I think the work that you have done on the legislative side is critically important, because we need a legal framework that enables us to rapidly share information, machine to machine and at machine speed, between the private sector and the government, and do it in a way that provides liability protection for the corporate sector, as well as ensuring that the very valid concerns about privacy and civil liberties are addressed.

I think we can do that. I think you've done that. The challenge clearly is achieving the political will and the political consensus to pass that. I leave that up to you fine women and women. What I'll try to focus on is, so, what do I think within the realm of responsibility of U.S. Cyber Command and the National Security Agency? What do we need to be doing?

In my hat as the National Security Agency—I'll talk about that first—primary roles for us, to ensure that we are generating insights that aid the public sector as well as government—the private sector as well as government, in terms of what's the

cyberthreat out there. What's coming at us? How can we give timely advance information that help us be in a position to respond and defeat those efforts getting into our systems, whether that be on the private side or in the government?

In addition, NSA has a primary role in ensuring its information assurance expertise is available to help both the government and the private sector in defending its systems and generating the standards and approaches to how you defend capability and ensuring that our expertise is available to help.

From the U.S. Cyber Command perspective, three primary missions for us: Number one, to defend our department's network. So I find myself, as many people do, just as the private sector does, just as many other elements in the government responsible for defending the cyber infrastructure of a large global organization.

We're taking a series of steps in the department to do that. It never goes as fast as you would like, but I'm very comfortable about the rate of progress and the plan we have to do that.

The other thing we're trying to do at U.S. Cyber Command is we're tasked with generating the cyber mission force, if you will, the men and women who are going to be addressing the department's cyber need, from the defensive to the offensive; and then, lastly, to be prepared, if directed by the president and the secretary of defense, to provide DOD capability to defend critical U.S. infrastructure.

As I think many of you are aware, the U.S. government has designated 16 segments within the private sector as being of critical significance to the nation's security. Think water. Think power. Think aviation, financial - 16. U.S. Cyber Command is tasked to be prepared to provide DOD capability to defend that infrastructure.

We continue to move along in that journey. We're about halfway through, the department has, between fiscal year '13 and fiscal year '16. So we have about four years to generate that capability, if you will. We're about halfway through that journey in time. We're about 40 percent in terms of actual generation of the force to date. Again, it's progressing well. We continue to learn insightful lessons as we continue through this.

I always remind people this will be an iterative journey, and where we are right now is not necessarily where we're going to end up. We're all trying to learn here. And cyber is an environment, a mission set, that continues to change.

. . .

REPRESENTATIVE MIKE CONAWAY (R-TX): Thank you, Admiral.

Your last comments—that was actually the question I had written down to ask you about, and that is your efforts at recruiting and retaining the folks that you need to defend as well as attack, assuming they get the orders to do that.

Given that this skill set in the kind of colloquial wisdom doesn't look like a, you know, clean-cut, short-haired, wearing, you know, a white Navy uniform kind of person, how do you fold in the kind of—or find the folks with the mindset to be able to do these kinds of specific technical things and also have the mindset to be a good sailor as an example, or soldier?

ADM. ROGERS: Thank you, sir.

So I'd make a couple of comments. First, the workforce will be composed of both military and civilian. So one of the comments I make to people is that gives us the opportunity to have a pretty broad swath of individuals. If you come out to the

National Security Agency today, you will see people with long ponytails, T-shirts, jeans; very casual, different approach to doing things, as opposed to what the military force looks like.

I think that's one of the advantages of a military and a civilian component to the workforce. We can get a broad range of capabilities and backgrounds. They don't all have to be the same. They don't all have to meet a military requirement, so to speak, in terms of physical fitness, standards of uniform and other things.

I'll tell you, when I started working in cyber in the department 10-plus years ago, my number one concern was how are we going to be able to recruit and retain the men and women that we need to execute this mission within the constraints we have within the department?

Ten-plus years into this now, and now, as the commander of United States Cyber Command, I would tell you I have been pleasantly surprised by our ability to do that, both in the uniformed element of the workforce and in the civilian element of the workforce.

. . .

REPRESENTATIVE JIM HIMES (D-CT): We heard last week from General Cartwright that more needs to be done to set international norms, something analogous to the laws of war, with respect to cyber. I'm wondering if you could take a few minutes to give us some sense, as somebody who's in the day-to-day mix here, about what some of the key principles might be for those international norms.

I'm obviously worried that in the absence of such agreements or norms, it may take a catastrophe and a retaliation to a catastrophe to force people to the table. So I wonder, could you give us a sense both what you think those norms would look like and, secondly, how we could help catalyze that agreement around the world?

ADM. ROGERS: Well, firstly, I would strongly concur with General Cartwright's comments. We have got, I believe, to develop a set of norms or principles for behaviors in this space, because, absent that kind of thing, being totally on the defensive is a very losing strategy to me. It will cost a significant amount of money. It leads to a much decreased probability of mission success. That's just not a good outcome for us in the long run.

And as you yourself referenced, and Representative Rogers did in his opening statement, there doesn't seem to be a sense of risk among nation-states, groups and individuals in the behaviors we see in cyber, that you can just do literally almost anything you want and there isn't a price to pay for it. That's not a good place, I would argue, for us as a nation, and I would argue, more broadly, for us internationally to be in.

So what we're trying to—and I'm not the primary in this, but what we're trying to make an argument, if you will, collectively is we need to develop a set of norms and behaviors that we can fundamentally agree with as a starting point for how we're going to behave and act within this environment. I've seen an initial set of points that the White House has developed and, in fact, has shared—have been raised in a couple of United Nation forums. We've talked about things like treat certs as hospitals, every nation-state should have its computer emergency capabilities left alone, every nation-state—that would be destabilizing—you want every nation to have the ability to respond to cyber emergencies. You don't want to take that capability away.

So what we're trying to—and I'm not the primary in this, but what we're trying to make an argument, if you will, collectively is we need to develop a set of norms and behaviors that we can fundamentally agree with as a starting point for how we're going to behave and act within this environment. I've seen an initial set of points that the White House has developed and, in fact, has shared—have been raised in a couple of United Nation forums. We've talked about things like treat certs as hospitals, every nation-state should have its computer emergency capabilities left alone, every nation-state—that would be destabilizing—you want every nation to have the ability to respond to cyber emergencies. You don't want to take that capability away.

There's discussion about do we want to put in standards about critical infrastructure for a nation-state. If you're—if you're going to go down that road, then that's a step beyond these norms and behaviors. Therefore, you're opening yourself up to potential repercussions. So the idea of critical infrastructure, some discussion about nation-state application against the commercial sector is a way to steal intellectual property for nation-state gain, you know, that—we have always argued that that is not within the U.S. vision. We don't do that. We have always argued that's not appropriate for the role of a nation-state. I think that would be among them.

Going after, as I said, infrastructure. If you looked at going after things that could lead to loss of life, if you looked at going after things that could lead to loss of control, you know, as outside the norms of behavior, that those are the kinds of things we're having discussions about, what—how do we build the framework if you will.

REP. HIMES: Do you, as you sort of look at the discussion internationally happening here, do you have any confidence that this debate or this discussion is going to advance? And in particular, are we going to be able to draw in bad actors like China and Iran? Or is it going to, in fact, take some demonstration of capability against them to get them to the table?

ADM. ROGERS: I don't know, is the short answer. I'm hoping it's not the latter. Clearly, there's ongoing dialogue.

You know, the other complicator in this is I often will hear people use the kind of nuclear analogy in terms of how we were able to develop over time to develop the concepts of deterrence, norms and behaviors. I try to remind people to remember the challenge of the nuclear analogy is when we started most of that work back in the 1950s and the 1960s, you had a capability—in this case, nuclear weapons—that were controlled purely by nation-states, no individuals or groups, by a very small number of nation-states—you know, two really, to start with initially when we had these initial discussions.

That's very different from the cyber dynamic, where we're not only going to be dealing with nation-states, but we're going to be dealing with groups, with individuals, when we're dealing with a capability that is relatively inexpensive and so easy to acquire, very unlike the nuclear kind of model. That makes this really problematic.

SOURCE: Michael Rogers, *Testimony before the House Intelligence Committee*, November 20, 2014, https://www.nsa.gov/news-features/speeches-testimonies/Article/1620360/hearing-of-the-house-select-intelligence-committee-subject-cybersecurity-threat/

ANALYSIS

This testimony offers some fascinating insights from Admiral Rogers. His discussion of the composition of the cyber forces of the United States, incorporating military and civilian personnel, was designed to reduce the power of the common trope that hackers are unfit for military service because they refuse to present a "clean-cut" appearance, follow military discipline, and adhere to standards of behavior. Rogers correctly notes that both USCYBERCOM and the NSA have a wide variety of personnel, who are selected on the basis of their unique skills rather than their appearances. Rogers also did much to dissuade Congressional representatives from relying heavily upon comparisons to the nuclear deterrence model—by providing a basic education in how cyber conflicts differ from other domains, Rogers did much to illustrate the underlying challenges he faced as the nation's top cyber expert.

- ***Document 79:*** *Barack Obama, "Remarks at the National Cybersecurity Communications Integration Center"*
- ***When:*** January 13, 2015
- ***Where:*** National Cybersecurity Communications Integration Center, Arlington, VA
- ***Significance:*** President Obama seemed to have a better intuitive grasp of the dangers of cyber warfare than most of his contemporary political peers. He devoted a substantial amount of his public speeches to the issue, to include addressing cyber intrusions in state of the union addresses, and he also announced a number of initiatives to enhance the nation's cybersecurity. In 2013, he spoke to the professionals tasked by coordinating the nation's cyber defenses.

DOCUMENT

Shortly after I took office, I declared that cyber threats pose an enormous challenge for our country. It's one of the most serious economic and national security challenges we face as a nation. Foreign governments, criminals and hackers probe America's computer networks every single day. We saw that again with the attack at Sony, which actually destroyed data and computer hardware that is going to be very costly for that company to clean up. Just yesterday, we saw the hack of a military Twitter account and You Tube channel. No military operations were impacted.

So far, it appears that no classified information was released. But the investigation is ongoing, and it's a reminder that cyber threats are an urgent and growing danger.

Moreover, much of our critical infrastructure—our financial systems, power grids, pipelines, health care systems—run on networks connected to the internet. So this is a matter of public safety and of public health. And most of this infrastructure is owned and operated by the private sector. So neither government, nor the private sector can defend the nation alone. It's going to have to be a shared mission—government and industry working hand in hand, as partners.

And that's why I've said that protecting our digital infrastructure is a national security priority and a national economic priority. Over the past six years, we've pursued a comprehensive strategy, boosting our defenses in government, sharing more information with the private sector to help them defend themselves, working with industry through what we call the Cybersecurity Framework not just to respond to threats and recover from attacks but to prevent and disrupt them in the first place.

And that's where these good folks come in. We are currently at the National Cybersecurity Communications Integration Center—also known as NCCIC. I just got a tour and a briefing. I want to thank everybody here, not just from DHS but from across government and the private sector, because, again, this is a shared responsibility.

This center is one of the critical lines of America's cyber defenses. These men and women work around the clock, 24/7, monitoring threats, issuing warnings, sharing information with the private sector, and keeping Americans safe. So, as a nation, we owe them thanks, and as a nation, we are making progress. We're more prepared to defend against cyber attacks. But every day, our adversaries are getting more sophisticated and more determined, and more plentiful. So every day, we've got to keep upping our game at the same time. We've got to stay ahead of those who are trying to do us harm.

The problem is that government and the private sector are still not always working as closely together as we should. Sometimes it's still too hard for government to share threat information with companies. Sometimes it's still too hard for companies to share information about cyber threats with the government. There are legal issues involved and liability issues. Sometimes, companies are reluctant to reveal their vulnerabilities or admit publicly that they have been hacked. At the same time, the American people have a legitimate interest in making sure that government is not potentially abusing information that it's received from the private sector.

So all of us—government and industry—are going to have to keep doing better. The new legislation and proposals I put forward yesterday will help, especially for a strong, single national standard for notifying Americans when their information has been breached. Today, I want to announce some additional steps.

First, we're proposing new cybersecurity legislation to promote the greater information sharing we need between government and the private sector. This builds and improves upon legislation that we've put forward in the past. It reflects years of extensive discussions with industry. It includes liability protections for companies that share information on cyber threats. It includes essential safeguards to ensure that government protects privacy and civil liberties even as we're doing our job of safeguarding America's critical information networks.

I raised this issue again and the need for this legislation with congressional leaders this morning, including Speaker Boehner and Leader McConnell, and we all agree that this is a threat that has to be addressed, and I am confident that we should be able to craft bipartisan legislation soon to put these systems in place. We're going to keep on working with Congress to get this done. And in the meantime, we're going to do everything we can with our existing authorities to make sure industry gets the information it needs to better defend itself.

Second, we're proposing to update the authorities that law enforcement uses to go after cyber criminals. We want to be able to better prosecute those who are involved in cyber attacks, those who are involved in the sale of cyber weapons like botnets and spyware. We want to ensure that we're able to prosecute insiders who steal corporate secrets or individuals' private information. And we want to expand the authority of courts to shut down botnets and other malware. The bottom line, we want cyber criminals to feel the full force of American justice, because they are doing as much damage, if not more, these days as folks who are involved in more conventional crime.

Finally, and since this is a challenge that we can only meet together, I'm announcing that next month we'll convene a White House summit on cybersecurity and consumer protection. It's a White House summit where we're not going to do it at the White House; we're going to go to Stanford University. And it's going to bring everybody together—industry, tech companies, law enforcement, consumer and privacy advocates, law professors who are specialists in the field, as well as students—to make sure that we work through these issues in a public, transparent fashion.

Because they're hard and they're complicated issues. But if we keep on working on them together, and focus on concrete and pragmatic steps that we can take to boost our cybersecurity and our privacy, I'm confident that both our privacy will be more secure and our information, our networks, public health, public safety will be more secure. We're going to keep on at this as a government, but we're also going to be working with the private sector to detect, prevent, defend, deter against attacks, and to recover quickly from any disruptions or damage. And as long as I'm President, protecting America's digital infrastructure is going to remain a top national security priority.

SOURCE: Barack Obama, *Remarks at the National Cybersecurity Communications Integration Center* (Arlington, VA, January 13, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent

ANALYSIS

In addition to the struggle associated with convincing political leaders from Congress to take the issue of cybersecurity seriously, President Obama also found that it was extremely difficult to convince private companies and individuals to put their trust in federal agencies and agree to far-reaching partnerships for cybersecurity. In part, this was due to excesses committed by federal agencies during his administration, in particular, the revelations about NSA surveillance of private

communications within the United States soured many individuals upon the idea that the federal government should be trusted with access to even more private information. In part, this was no doubt due to a failure to understand the problem for the leaders of many private companies, or a desire to shift the entire burden of cyber protection onto the federal government, or a fear that proprietary information might be shared with competitors. In any event, despite Obama's best efforts, the public–private cyber defense partnership never materialized to the level he hoped to achieve, as laid out in this speech.

- ***Document 80:*** *Advance Policy Questions for the Honorable Ashton Carter*
- ***When:*** February 4, 2015
- ***Where:*** Washington, D.C.
- ***Significance:*** Prior to a vote in the United States Senate regarding the confirmation of a cabinet-level official, Senators are able to provide questions for a nominee to answer regarding their perspectives on issues relevant to the duties of the office they seek to hold. Ashton Carter was sent a list of hundreds of questions prior to his formal confirmation hearings, and asked to provide thorough answers to each. Several of the questions pertained to cyber issues, and demonstrated that at least a few Senators were considering the cyber problems facing the nation.

DOCUMENT

Cyber Deterrence

247. Do you believe we are deterring and dissuading our adversaries in cyberspace?

An effective deterrence strategy requires a range of cyber policies and capabilities to affect a state or non-state actors' behavior. In addition to continuing efforts to improve U.S. cyber defenses and cybersecurity capabilities, the United States should continue to respond to cyber-attacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law. The U.S. government should continue to combine its cyber and non-cyber capabilities into a comprehensive cyber deterrence strategy. If confirmed, I will do all that I can to contribute to the development and execution of that effort.

248. Do you agree that, consistent with Section 941 of the FY14 National Defense Authorization Act, there is a need for an integrated policy to deter adversaries in cyberspace and that the President should promptly provide that policy to Congress as specified in law?

Deterrence cannot be achieved through cyberspace alone, but requires a multi-faceted effort across the totality of the U.S. government's instruments of national power, including network defense measures, economic actions, law enforcement actions, defense posture and response capabilities, intelligence, declaratory policy, and the overall resiliency of U.S. networks and systems. If confirmed, I will ensure that DoD is in full compliance with its reporting requirements to this Committee and to the Congress as a whole.

249. What steps do you believe the Department should take to reduce the frequency and severity of cyber intrusions from the Chinese government?

This is a serious problem and the Department should continue to take strong actions to address China's use of cyber theft to steal U.S. companies' confidential business information and proprietary technology. I am aware that the Administration has raised this as an issue of concern with the highest levels of China's government. If China does not take meaningful action to curb this behavior, it will undermine the economic relationship that benefits both our nations. Such activity undercuts the trust necessary to do business in a globally connected economy. Further, military involvement in such theft raises additional concerns that misunderstandings about China's intentions could result in unintended escalation between our countries. The U.S. Government should continue to use all instruments of national power, including diplomatic, informational, military, and economic, to prevent and respond to these intrusions.

250. What agencies should the Department coordinate with in tracking and eliminating cyber threats?

I believe a whole-of-government approach is required to address the cyber threats we face now and will increasingly face in the future. The Department of Defense must continue to work closely with the Department of Homeland Security, the Department of Justice (specifically FBI), and the Intelligence Community, as well as with other Federal partners, to identify, mitigate, and defend against cyber threats.

. . .

Act of War in Cyber

253. What do you believe would constitute an act of war in cyberspace?

Cyber-attacks can affect our critical infrastructure, the national economy, and military operations. I believe that what is termed an act of war should follow the same practice as in other domains, because it is the seriousness, not the means, of an attack that matters most. Whether a particular attack is considered an "act of war," in or out of cyberspace, requires a determination on a case-by-case and fact-specific basis. Malicious cyber activities could result in death, injury or significant destruction, and any such activities would be regarded with the utmost concern and could well be considered "acts of war." An attack does not need to be deemed an "act of war" to require a response.

254. Does North Korea's attack on the Sony Corporation of America—a costly destructive attack on a U.S. company—rise to the level of an act of war? If not, why not?

To my knowledge, the damage caused by this cyber-attack consisted of the deletion of data, the destruction of some Sony network infrastructure, and the unauthorized disclosure of personal information. While serious and deserving of a response, this does not seem to me to rise to the level of an "act of war."

China's Aggressive Theft of U.S. Intellectual Property

A recent report by the National Counterintelligence Executive confirmed the widespread belief that China is engaged in a massive campaign to steal technology, other forms of intellectual property, and business and trade information from the United States through cyberspace. The previous Commander of U.S. Cyber Command has referred to this as the greatest transfer of wealth in history and, along with others, believes this is a serious national security issue.

255. Do you believe that China's aggressive and massive theft of technology in cyberspace is a threat to national security and economic prosperity?

Yes. The theft of intellectual property through cyber means is a clear threat to the economic prosperity from which the nation derives its national security. Our competitive economic advantage and our military technological advantage rest on the innovations of a highly knowledge based U.S. industry. Any nation-state that engages in the theft of our intellectual property through cyber means jeopardizes both our national security and economic prosperity.

The Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 authorized the President to impose sanctions, pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.), on persons determined to knowingly request, engage in, support, facilitate, or benefit from economic or industrial espionage in cyberspace against United States persons.

256. What are your views on the potential impact of this legislation?

Addressing cyber threats requires a whole of government approach, which coordinates and integrates all the instruments of national power. Cyber legislation is an important part of this effort. If confirmed, I look forward to working closely with Congress on appropriate legislation to address a broad array of cybersecurity issues.

257. What additional steps do you believe are needed to deter China from such activities in the future?

We need to continue to use all the instruments of national power to deter this kind of behavior, including diplomatic, financial, network defense, law enforcement, and counterintelligence. I concur in the Administration's approach of raising this as an issue of concern at the highest levels of the Chinese government. I also support the State Department's efforts to work with like-minded countries to make China's leadership increasingly aware that elements of their government and military are on the wrong side of an emerging norm of responsible behavior in cyberspace. If confirmed, I will work closely with the Department's interagency partners to explore what additional whole-of-government approaches might help deter this unacceptable behavior.

DOD's Role in Defending the Nation from Cyber Attack

258. What is your understanding of the role of the Department of Defense in defending the Nation from an attack in cyberspace? In what ways is this role distinct from those of the homeland security and law enforcement communities?

The Defense Department is responsible for defending the Nation from all attacks, including those that occur in cyberspace. DoD is also responsible for defending its own networks against cyber-attacks. DoD plans, coordinates, and conducts cyber operations to ensure the 73 reliable operation of and to defend DoD systems and infrastructure. If directed, DoD can conduct cyber operations to defend the Nation, defend military networks, and support military operations in all domains. If required, DoD may provide support to the private sector and State and local governments.

The Defense Department also works closely with the Department of Homeland Security (DHS) and the Department of Justice (DoJ) in their missions. DHS is the lead agency for protecting, mitigating, and recovering from domestic cyber incidents. DoJ investigates, attributes, disrupts, and prosecutes cybercrimes that fall outside of military jurisdiction and provides domestic response to national security incidents.

Next Challenges in Growing Operational Cyber Capabilities

The Department of Defense, in a significant milestone in the maturation of the cyber warfare mission, is successfully organizing and training personnel for units to conduct military operations in cyberspace.

259. What challenges does the Department face in developing the command and control, operational planning, mapping and situational awareness, battle damage assessment, tools and weapons, and infrastructure capabilities necessary to conduct large-scale operations in cyberspace?

I understand that DoD is in its third year of building a Cyber Mission Force. This force is intended to defend DoD networks, defend the Nation from cyberattack, and provide full-spectrum cyberspace options for the Combatant Commands. I am aware of several challenges that should be addressed to ensure the Department can conduct military operations in cyberspace, among them effective command and control, and meeting the challenge of effectively incorporating National Guard teams.

SOURCE: Ashton Carter and members of the U.S. Senate Committee on Armed Services, *Advance Policy Questions for the Honorable Ashton Carter*, February 4, 2015, 69–73, https://www.armed-services.senate.gov/imo/media/doc/Carter_APQs_02-04-15.pdf

ANALYSIS

Carter clearly advocated for federal agencies to cooperate in order to present a united front regarding cyberattacks from international sources. Not surprisingly, the DOD tends to consider such incursions from a military perspective and focuses almost entirely upon the actions of hostile nations. However, the DOD is not a law enforcement agency—and so long as the violations in question are criminal in nature, Carter seems content to provide support to the FBI or the DHS as the lead

agency to handle defending private and government computer networks. He also has a much narrower definition of how a cyberattack might rise to the level of an act of war than many other experts might utilize. By defining most cyberattacks, even ones that cause substantial damage, as something other than acts of war, he is effectively shifting responsibility for responding to those attacks away from the DOD and, by implication, probably transferring it to the nation's intelligence agencies.

- ***Document 81:*** *Lisa O. Monaco, "Strengthening Our Nation's Cyber Defenses"*
- ***When:*** February 10, 2015
- ***Where:*** Wilson Center, Washington, D.C.
- ***Significance:*** Lisa O. Monaco served as the assistant to the president for Homeland Security and Counterterrorism. In that role, she delivered daily briefings to President Barack Obama on the pressing terrorism issues threatening American interests around the world. In this speech, she reflected current policy and thinking about the use of cyber assets for a variety of attacks, including terrorism.

DOCUMENT

We are at a transformational moment in the evolution of the cyber threat. The actions we take today—and those we fail to take—will determine whether cyberspace remains a great national asset or increasingly becomes a strategic liability. An economic and national security strength, or a source of vulnerability.

So today, I want to talk about the threat we face and the Administration's approach to countering it, drawing on counterterrorism lessons learned from the last decade of war.

Let me start with the facts. According to a recent U.S. Government assessment, cyber threats to our national and economic security are increasing in their frequency, scale, sophistication, and severity of impact. The range of cyber threat actors, methods of attack, targeted systems, and victims are expanding at an unprecedented clip.

The pace of cyber intrusions has also ticked up substantially—annual reports of data breaches have increased roughly five-fold since 2009. And the seriousness of those breaches is also rising, causing significant economic damage.

No one, it seems, is immune—from healthcare companies and universities to the tech industry, critical infrastructure, and entertainment sector. Just last week, Anthem, one of the nation's largest health insurance providers, announced that hackers had breached a database containing the personal information of 80 million customers and employees. Inside the U.S. government, we know that state and non-state actors, terrorists, hackers, and criminals are probing our networks every day—seeking to steal, spy, manipulate, and destroy data.

At the state level, threats come from nations with highly sophisticated cyber programs, including China and Russia, and nations with less technical capacity but greater disruptive intent, like Iran and North Korea. Several nations regularly conduct cyber economic espionage for the commercial gain of their companies. And politically motivated attacks are a growing reality, as we saw with North Korea's attack on South Korean banks and media outlets last year.

As for non-state actors, threats are increasingly originating from profit-motivated criminals—so-called hackers for hire—those who steal your information and sell it to the highest bidder online. Transnational criminals use cyber as a vector for profit. There are the ideologically motivated hackers or terrorists. You have groups like Anonymous that thrive on creating disruptions on company's websites and leaking personal information online. You have groups like the so-called Syrian Electronic Army, which conducts cyber attacks in support of the brutal regime in Syria.

And then there is ISIL, which has harnessed social media for a propaganda machine that's radicalizing and recruiting young people to their hateful message around the world.

Most concerning, perhaps, is the increasingly destructive and malicious nature of cyber attacks, as we saw with Sony Pictures Entertainment last fall. This attack stole large amounts of data and rendered inoperable thousands of Sony's computers and servers. It was a game changer because it wasn't about profit—it was about a dictator trying to impose censorship and prevent the exercise of free expression. At bottom, it was about coercion, which the United States believes is unacceptable, and which is why we took the extraordinary step of publicly identifying North Korea as responsible for the attack and responded swiftly, imposing additional sanctions on Kim Jong-Un's regime.

In short, the threat is becoming more diverse, more sophisticated, and more dangerous.

And I worry that malicious attacks like the one on Sony Pictures will increasingly become the norm unless we adapt quickly and take a comprehensive approach, just as we have in other contexts. Which brings me to the counterterrorism model.

Now, to be sure, there are many differences that make it difficult to apply lessons learned from the counterterrorism experience to cyber. For one, the private sector plays a more central role in spotting and responding to cyber incidents than they do in the counterterrorism realm, where the government largely takes the lead.

Having observed our Nation's response to terrorism post 9/11 from three different perches in the U.S. government—at the FBI, as Assistant Attorney General for National Security at the Department of Justice, and now at the White House—I can tell you there are structural, organizational, and cultural shifts that were made in our government in the counterterrorism realm that also apply to cyber. We need to develop the same muscle memory in the government response to cyber threats as we have for terrorist incidents.

Structurally, since 9/11 our government has done the hard work of breaking down walls in our counterterrorism agencies and bringing people together to share information so that we get the best possible assessment of the threat. Whenever possible, we're bringing partners together to share information and extend our operational reach. This model has made our counterterrorism mission against an evolving enemy more effective and sustainable.

Like counterterrorism, meeting cyber threats requires a whole-of-government approach that uses all the appropriate tools available to us—including our global diplomacy, our economic clout, our intelligence resources, our law enforcement expertise, our competitive technological edge, and, when necessary, our military capability. Those who would harm us should know that they can be found and will be held to account.

In the cyber context, we need to share threat information more broadly and coordinate our actions so that we're all working to achieve the same goal—and we have to do so consistent with our fundamental values and in a manner that includes appropriate protections for privacy and civil liberties. We need to sync up our intelligence with our operations and respond quickly to threats against our citizens, our companies, and our Nation.

Make no mistake. Over the last few years, we have developed new and better ways to collaborate across all levels of government and with our partners in the private sector—including at the operational hubs in our government charged with monitoring threats, issuing warnings, sharing information, and protecting America's critical infrastructure.

At the White House, we've taken steps to improve our policy response. Last summer, following a rising number of breaches and intrusions to public and private networks, we created the Cyber Response Group, or CRG—modeled on the highly effective and long-standing Counterterrorism Security Group. The CRG convenes the interagency and pools knowledge about ongoing threats and attacks and coordinates all elements of our government's response at the highest levels.

Despite this progress, it has become clear that we can do more as a government to quickly consolidate, analyze, and provide assessments on fast-moving threats or attacks. As President Obama said during the State of the Union last month, we will make "sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism."

So today, I'm pleased to announce that we will establish a new Cyber Threat Intelligence Integration Center, or CTIIC, under the auspices of the Director of National Intelligence. Currently, no single government entity is responsible for producing coordinated cyber threat assessments, ensuring that information is shared rapidly among existing Cyber Centers and other elements within the government, and supporting the work of operators and policy makers with timely intelligence about the latest cyber threats and threat actors. The CTIIC is intended to fill these gaps.

. . .

Moving forward, as our lives become more and more dependent on the internet, and the amount of territory we have to defend keeps expanding, our strategy will focus on four key elements.

First, we need to improve our defenses—employing better basic preventative cybersecurity, like the steps outlined in the Cybersecurity Framework announced last year, would enable every organization to manage cyber risk more effectively. But even just employing basic cyber hygiene could stop a large percentage of the intrusions we face, so we've got to start by getting the basics rights.

Second, we need to improve our ability to disrupt, respond to, and recover from cyber threats. That means using the full strength of the United States

government—not just our cyber tools—to raise the costs for bad actors and deter malicious actions.

Third, we need to enhance international cooperation, including between our law enforcement agencies, so that when criminals anywhere in the world target innocent users online, we can hold them accountable—just as we do when people commit crimes in the physical world.

And fourth, we need to make cyberspace intrinsically more secure—replacing passwords with more secure technologies, building more resilient networks, and enhancing consumer protections online, to start with.

President Obama will continue to do everything within his authority to harden our cyber defenses, but executive actions alone will not be enough. We need durable, long-term solutions, codified in law that bolster the Nation's cyber defenses. This is not, and should not, be a partisan issue. The future security of the United States depends on a strong, bipartisan consensus that responds to a growing national security concern. Everyone shares responsibility here, including the Congress.

In December, Congress passed important bills to modernize how the government protects its systems and to clarify the government's authorities to carry out its cyber missions. Today, we need the Congress to build on that progress by passing the package of cybersecurity measures that President Obama announced last month that encourage greater information sharing, set a national standard for companies to report data breaches, and provide law enforcement with updated tools to combat cybercrime. And we look to Congress to pass a budget with critical funding for cybersecurity, including for DHS. The Administration is ready to work with Congress to pass these measures as quickly as possible.

Cybersecurity is and will remain a defining challenge of the 21st century. With more than three billion internet users around the world and as many as ten billion internet-connected devices, there's no putting this genie back in the bottle. We have to get this right. Our prosperity and security depend upon the internet being secure against threats; reliable in our ability to access information; open to all who seek to harness the opportunities of the internet age; and interoperable to ensure the free flow of information across networks and nations.

But we are at a crossroads, and the clock is ticking. The choices we make today will define the threat environment we face tomorrow.

All of us have a responsibility to act—to take preventative measures to defend our systems; to build greater resilience into our networks to bounce back from attacks; to break down silos and improve information sharing and the integration and analysis of threats; to pass cybersecurity legislation; and to ensure we take a comprehensive, whole-of-government approach to respond to cyber attacks, just as we do in other contexts.

These are hard and complicated issues. But I'm confident that working together—government, industry, advocacy groups, the public, and Congress—our networks will be safer, our privacy protected, and our future more secure. I look forward to tackling these threats with all of you.

SOURCE: Lisa O. Monaco, *Strengthening our Nation's Cyber Defenses*, Speech at the Wilson Center (Washington, D.C., February 10, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/11/remarks-prepared-delivery-assistant-president-homeland-security-and-coun

ANALYSIS

President Obama's focus upon improving the nation's cyber defenses was an important step toward protecting against a catastrophic failure, and Lisa Monaco's role as his special adviser on such issues put her in an excellent position to understand the nature of the problem, the magnitude of the risks, and the consequences of failure. However, no presidential administration has unfettered power, and to truly address many of the inherent risks faced by the nation from attacks conducted through cyberspace, the president desperately needed cooperation from the legislature, as well as international bodies. Unfortunately, the U.S. Congressional leadership seemed more interested in scoring political points against the administration than in actually confronting the issues at hand, and getting Congressional leaders to take the issue of cyber defenses seriously proved all but impossible. Many of the Obama administration's officials made public addresses related to cyber, and these may have served to put some degree of public pressure upon Congressional leadership—but they were insufficient to trigger the massive reforms in cyber authorities necessary to truly revitalize the nation's cyber defenses. Monaco's speech does an excellent job of laying out the dangers confronting the federal government and private entities, but was less effective at stimulating major changes in the cyber readiness of the nation.

- ***Document 82:*** *James Clapper, Testimony before the U.S. Senate Committee on Armed Services*
- ***When:*** February 26, 2015
- ***Where:*** Washington, D.C.
- ***Significance:*** James Clapper served as the director of National Intelligence from 2010 through 2017, spanning most of the Obama administration. In that capacity he frequently testified before various Congressional committees regarding subjects related to national security. Each year, he provided a summary of key threats to the United States to the Senate Committee on Armed Services.

DOCUMENT

In the interest of time and to allow for questions, I will only cover some of the wave tops on behalf of both of us. Two overall comments at the outset:

One, unpredictable instability is the new normal. The year 2014 saw the highest rate of political instability since 1992, the most deaths as a result of state-sponsored mass killings since the early 1990s, and the highest number of refugees and internally

displaced persons, or IDPs, since World War II. Roughly half of the world's currently stable countries are at some risk of instability over the next 2 years.

The second overall comment is, this pervasive uncertainty makes it all the harder to predict the future. 2014 and 2015 saw a number of events that illustrate this difficulty: the North Korean attack on Sony, the most serious and costly cyberattack against U.S. interests to date, the ebola epidemic, and the small-scale but dramatic terrorist attacks in Australia, Belgium, Canada, Denmark, France, and the United States.

Again this year, I'll start with cyber threats. Attacks against us are increasing in frequency, scale, sophistication, and severity of impact. Although we must be prepared for a catastrophic large-scale strike, a so-called "cyber Armageddon," the reality is that we've been living with a constant and expanding barrage of cyberattacks for some time. This insidious trend, I believe, will continue. Cyber poses a very complex set of threats, because profit motivated criminals, ideologically motivated hackers, or extremists in variously capable nation-states, like Russia, China, North Korea, and Iran, are all potential adversaries, who, if they choose, can do great harm. Additionally, the methods of attack, the systems targeted, and the victims are also expanding in diversity and intensity on a daily basis.

2014 saw, for the first time, destructive cyberattacks carried out on U.S. soil by nation-state entities, marked first by the Iranian attack against the Las Vegas Sands Casino Corporation, a year ago this month, and the North Korean attack against Sony in November. While the both of these nations have lesser technical capabilities in comparison to Russia and China, these destructive attacks demonstrate that Iran and North Korea are motivated and unpredictable cyber actors.

Russia and China continue to develop very sophisticated cyber programs. While I can't go into detail here, the Russian cyber threat is more severe than we had previously assessed. And Chinese economic espionage against U.S. companies remains a major threat, despite detailed private sector reports, scathing public indictments, and stern U.S. demarches.

With respect to non-nation-state entities, some ideologically motivated cyber actors expressing support for ISIL have demonstrated their capabilities by hacking several social media accounts. The so-called "Cyber Caliphate" successfully hacked CENTCOM's Twitter account and YouTube page in January, and, 2 weeks ago, hacked Newsweek magazine's Twitter handle.

The most pervasive cyber threat to the U.S. financial sector is from cyber criminals. Criminals were responsible for cyber intrusions in 2014 into JPMorgan, Home Depot, Target, Nieman Marcus, Anthem, and other U.S. companies. And, in the future, we'll probably see cyber operations that 24 change or manipulate electronic information to compromise its integrity instead of simply deleting or disrupting access to it. In the end, the cyber threat cannot be completely eliminated. Rather, we must be vigilant in our efforts to detect, manage, and defend against it.

. . .

Senator Fischer: Okay. And if I could shift gears, here, I'd like to ask you something about cybersecurity. As you know, the Senate is looking at a bill to authorize greater information sharing. There are some concerns out there about the entities that the—that we might be sharing that information with. I'd like to ask you, How do we balance that? How do we balance the risks between really valuable information sharing and the need not to provide information either to private individuals,

hackers that are out there, or to a foreign government that may be able to pick up information that we give our colleagues, in trying to work with this, that they could then, in turn, use against us?

Mr. Clapper: Well, that's exactly the issue. In fact, that's a general dilemma that we have across the board, whether it's cyber or any other dimension. You know, the—sharing versus security. And that's the same issue here. There is no silver-bullet answer here.

I do think there, though, needs to be some form of legislation that would protect, from a liability standpoint, commercial concerns so that they would more freely—they'd be in a position to share with the government. This is not something government can do all by itself. There has to be—given the pervasiveness of cyber in our society, we must have the partnering of the civilian sector, which means promoting sharing, both ways.

But, you're right, there's always this concern, there's always a tradeoff between security and sharing.

SOURCE: U.S. Senate Committee on Armed Services, *Hearing to Receive Testimony on Worldwide Threats*, February 26, 2015, 8–13, 48–50, https://www.armed-services.senate.gov/imo/media/doc/15-18%20-%202-26-15.pdf

ANALYSIS

While much of Clapper's testimony was classified, and hence not open to the public, even this unclassified portion makes some interesting assertions with regard to cyber. First, he notes that both Iran and North Korea brazenly launched destructive cyberattacks against corporations in the United States. While both attacks were designed to inflict economic damage, and were successful in the endeavor, the fact that those nations felt empowered to launch such clear, provocative attacks without regard for the U.S. response is an important departure from past activities. Clapper's call for legislation protecting companies that share their information with the government as a means of enhancing cybersecurity is illustrative—neither the Las Vegas Sands Casino nor the Sony Pictures Corporation was willing to grant full access to federal investigators and cybersecurity experts, even after the loss of millions of dollars. Instead, each company essentially chose to accept its losses rather than calling in the full power of the federal government. Also, it is entirely likely that both Iran and North Korea felt empowered to launch their attacks because both were already subject to devastating economic sanctions originating in the United States. Short of a military attack, it is unlikely that the United States could bring much more punishment to either of the rogue states.

- ***Document 83:*** *Glenn S. Gerstell, "Confronting the Cybersecurity Challenge"*
- ***When:*** February 25, 2017
- ***Where:*** Durham, NC

- ***Significance:*** Glenn Gerstell, while serving as the general counsel for the NSA, offered his thoughts on the inherent challenges associated with responding to cyber crises. In particular, the inability to unify authority and responsibility in a single organization has led to sluggish and dysfunctional responses when major challenges have emerged in the cyber domain.

DOCUMENT

As I've already alluded to, there has been no dearth of strategies proposed to address the cyber threat on a national level. They range from a recent Center for Strategic and International Studies report (advocating for making cybersecurity an independent operational component at DHS while also strengthening other key agencies), to GWU's Center for Cyber and Homeland Security (recommending the development of a framework that would allow technologically advanced private entities to engage in level of proactive cybersecurity measures that fall between traditional passive defense and offense). Separately, the Presidential Commission on Enhancing National Cybersecurity recommended, among other things, improving public/private partnerships and increasing use of the current Cybersecurity Framework laid out in Executive Order 13636. Meanwhile, Representative Michael McCaul, the Chairman of the House Homeland Security Committee, has been working to pass a bill that would codify certain cybersecurity authorities at DHS's National Protection and Programs Directorate, which would be renamed the Cybersecurity and Infrastructure Protection Agency.

As you can see, much attention has been paid to the nation's cybersecurity, but a consensus has not yet developed regarding the preferred approach. What's revealing, however, is that virtually all of these studies seek to advance two overarching goals: *integration* and *agility*. Any new approach to cybersecurity must be integrated, in that it must include major national-level structures in which all divisions of government know their roles in clearly defined, non-duplicative assignments appropriate to the particular expertise and position of the government entity. Integration isn't merely a governmental imperative. A national coordinated solution by definition must involve both the public and private sectors, and equally must take full advantage of the intelligence and insights generated by our national security apparatus. Most importantly, it must coalesce around a national will—the creation and sustaining of that should be the work of not only the executive and legislative branches but also corporate America and academia.

A new framework must also be agile. From my position at NSA, I've witnessed the challenges in sharing classified threat indicators within government and across the private sector, and I've also seen firsthand that the process for determining who can act and what approach should be taken in response to a cyber threat is slow and cumbersome, involving formal requests for assistance, several layers of approval, and time-consuming fiscal considerations. It is akin to calling county water officials

when your house is on fire, who must ask for assistance from the fire department, which must then receive approval from the mayor and money from the city treasury before a truck can be dispatched. By the time this administrative legwork is complete, our cyber house has been reduced to cinders. It is essential that our cybersecurity framework be equipped with both the resources and the authority to anticipate, protect against, and respond to cyber threats with the speed that will make a difference.

So how do we accomplish this? One obvious and affirmative strategy, and the one that I think may have the most potential for achieving real gains, would be to unify the government's cybersecurity activities by establishing a new lead department or agency for cybersecurity. Easily said perhaps—but exactly how would one go about doing it? Well, much as we did two centuries ago, we can again look to our neighbors across the pond for ideas. The United Kingdom faces the same cyber threats we do, but for a variety of reasons one could speculate on (perhaps having to do with their size, institutional strengths and political culture), they sometimes are able to achieve solutions more quickly than can our arguably more fractious democracy. The UK within the past few months has selected a new integrated model, by creating the National Cybersecurity Centre or NCSC. Like the U.S., the UK had various entities, all with disparate responsibilities for cybersecurity. Their new center brought together and replaced four different entities. The NCSC is intended to act as a bridge between industry and government, providing a unified source of advice, guidance, and support on cybersecurity and management of cyber incidents. In other words, the NCSC model is intended to address both prevention and remediation of cyber threats and incidents by pulling together under one roof the full range of critical cybersecurity functions, including research, advice and guidance, and incident response and management. I am not necessarily proposing this precise model as the solution; after all, the UK has, as I noted a moment ago, a different culture, it is smaller, and the actual details of its legal system are quite unlike ours despite being obviously erected upon similar concepts. It is still useful, however, to examine the ground that they've started to break to determine whether there is anything that we can and should import.

The understanding that victims of cyber attacks were receiving conflicting advice and views depending on the government agency to which they turned was a major rationale for the UK to establish a unified cyber center—but what really kick-started the UK to action was that the realization that relatively unsophisticated cyber intrusions, such as the attack against TalkTalk, a UK telecom provider, by a teenage boy, were turning into national level events because of a lack of basic cyber hygiene and because the government was not appropriately transparent about cyber threats and intrusions. Increased information sharing alone, however, was not the answer; UK experts decided that a more interventional approach was required in order to create consistency and coherency.

The UK carefully considered whether to organize the NCSC inside or outside the intelligence community. Much like in the U.S., there was apprehension in the UK after the Snowden disclosures about the role of its intelligence apparatus. Ultimately, however, the UK elected to stand up the NCSC as an agency wholly within the Government Communications Headquarters, which is the UK's version

of NSA. This was done because, as I mentioned previously with respect to NSA, GCHQ already had the technical expertise and the intelligence insights that would be needed by the new organization. In order to overcome the public's apprehension, the NCSC committed itself to transparency: it publishes comprehensive data on cyber threats and, whenever possible, includes supporting evidence. Its facility is largely unsecured, so that it can bring in subject matter and technical experts from the private sector to teach NCSC personnel about their industries.

In conjunction with the establishment of the NCSC, the UK also rolled out its comprehensive National Cyber Security Strategy, which sets out the UK's approach to tackling and managing cyber threats to the country. It advocates for developing an innovative cyber security industry and provides for an active, nationwide cyber defense program. As an example, they've begun deploying a web check service, which scans for web vulnerabilities or misconfigurations in the websites of all public sector organizations in the UK. Website owners are provided a tailored report about any issues identified. Overall, the UK has committed to investing over $2 billion over the next five years to transform their cybersecurity posture.

Naturally, there are drawbacks to a model such as the NCSC. For example, concentrating cybersecurity responsibilities in one lead agency misses an opportunity to marry cyber expertise with the unique insights and understanding of requirements possessed by each agency in their own fields. In addition, as we've seen with the Department of Homeland Security, there are always bureaucratic and political issues associated with standing up a new national organization. The potential advantages of this approach, however, seem for the UK to outweigh the disadvantages.

Could we do the same thing here? At least on its face, this could satisfy the two principles I suggested a minute ago—namely, integration and agility. Most importantly, through unification, the cyber protection mission would be informed by the foreign intelligence mission that uncovers malicious cyber activity from nation states and political groups adverse to us. The benefits of that proximity are precisely what led NSA, in an internal reorganization last year, to combine its information assurance teams with the signals intelligence ones in a combined operations directorate. And in a slightly different but still highly relevant context, the decision to co-locate and partially integrate the new US Cyber Command with NSA was a critical factor in seeking efficiency and synergy for the new organization. If we were to follow the UK model, cyber security would be the principal mission for a newly-created organization, rather than a secondary or tertiary support function, as it currently is for many federal agencies, and it stands to reason that that focus would yield better outcomes. Unifying cybersecurity responsibilities in one organization would enable the federal government to eliminate redundancies and to concentrate and streamline cybersecurity resources and expertise—both of which can be hard to come by in an era where the cost of purchasing and updating equipment and retaining cyber talent creates challenges to the implementation of cyber best practices. And manifestly, housing the cyber threat discovery, protection, defense, and remediation capabilities in one entity would afford the agility and timeliness that is critical to an effective cyber strategy. In short, I think the case for such a unified, central approach is fairly compelling.

Even if we all concurred that such an approach was the right one, there would still be many details to be worked out. One key question would be how to sufficiently

empower the new organization so that it could effectively defend the various networks of many federal entities—which would include the power to, in some sense, police those networks, setting and enforcing standards, perhaps even shutting them down if needed—while at the same time letting each entity have some authority and responsibility for its own unique operations. A unified and nationally prioritized budgetary authority would clearly be a critical component of such an approach. Similarly, Congress would need to embrace this approach on multiple levels, including centralizing to some significant extent the jurisdiction over cyber matters that is now accorded to many committees and subcommittees. The very process of deciding what we are going to do, however, will require us to face these questions head on. This exercise will be valuable in forcing us to decide how cyber responsibilities will be shared across the government, how the public and private sectors should work together, how to enforce compliance with standards, and how to respond to malicious cyber actors.

If this nationally unified approach were adopted, I am not necessarily proposing that such an organization fall within NSA. Although that is certainly worth exploring, we recognize that there are very real concerns about the scope of government surveillance and the potential use of "zero-day vulnerabilities" or cyber vulnerabilities that could be discovered by the government—but at a minimum, NSA should have a special relationship with any new cybersecurity organization. It would make no sense to deny such a new organization the insights and warnings about cyber threats developed by NSA through its foreign intelligence mission. That would fly in the face of the very need for integration and agility. Whether that relationship takes the form of, for example, some deeper partnership between NSA and truly integrated cybercenter in a new Cabinet-level Department of Cyber, or housed, say, within the existing DHS, is something that the executive and legislative branches will have to sort out.

I want to make clear that by advocating that we avail ourselves of the infrastructure already paid for with taxpayer dollars and of the expertise and position of NSA, I am not, however, suggesting that NSA be granted additional surveillance authorities. We recognize that—while increased communications monitoring might be an inevitable byproduct of confronting the cyber threat—it's equally true that monitoring and implementing other technological approaches are fraught with understandable concern about government intrusion. Undoubtedly, there are portions of the population with unanswered questions (or worse) about us, but just because that perception exists does not mean folks like me are doomed to silence. Instead, I feel like we owe it to ourselves and to the public to enter the debate on topics like cybersecurity. The cybersecurity threat is grave, and we've got the unique expertise needed to help safeguard the nation against those threats. It's important to share some of our knowledge, developed over many years, in order to foster a vital public debate about the right way to address threats to our national security, and part of that debate includes an honest discussion about the pros and cons of locating a lead cyber agency or department within the intelligence community.

SOURCE: Glenn S. Gerstell, *Confronting the Cybersecurity Challenge*, Speech at Law, Ethics, and National Security Conference, Duke University Law School, February 25, 2017, https://www.nsa.gov/news-features/speeches-testimonies/Article/1619236/confronting-the-cybersecurity-challenge-keynote-address/

ANALYSIS

Gerstell made the interesting decision to utilize the British experience as a potential model for how to streamline responses to cyberattacks. But, he also had to be careful not to arouse the suspicions of his audience regarding the recent history of his employer, the NSA, which had revealed that it had conducted an enormous domestic surveillance program, ostensibly in pursuit of terror organization supporters within the United States. Gerstell's speech deftly sidestepped many of the key criticisms of placing the NSA in charge of such an effort—the mysterious agency is mistrusted by much of the U.S. public due to its past track record of abusing authorities granted to it. The Edward Snowden disclosures regarding NSA methods and operations also provided a substantial amount of material for critics of the organization, who responded to this speech by demanding that the NSA not be given further power to collect intelligence from American citizens in any fashion. While Gerstell is correct that unifying the responsibility for coordinating a response to cyberattacks within a single organization would create significant efficiencies, the idea that it might be the NSA (or its closely related military counterpart, USCYBERCOM), is a much more far-fetched notion for many listeners.

- ***Document 84:*** *Glenn S. Gerstell, "How We Need to Prepare for a Global Cyber Pandemic"*
- ***When:*** April 9, 2018
- ***Where:*** Sea Island, GA
- ***Significance:*** Glenn Gerstell served as the general counsel of the NSA. In that regard, he was at the cutting edge of the development of norms and laws governing cyberspace. In this speech, Gerstell offered his perspective on how the spread of popular do-it-yourself hacking tools made a massive eruption of malicious cyber activity far more likely in the near future.

DOCUMENT

2018 represents another year in which the Intelligence Community has highlighted the gravity of the cyber threat in its annual worldwide threat assessment. That assessment reports that over 30 countries are now believed to possess cyberattack capabilities. This number, which has increased almost every year since 2007, reflects the ease with which malicious cyber actors can now obtain and deploy cyber weapons. Cyberspace has proven to be a relatively accessible vector in

which to carry out malicious activities, and so we are seeing that less sophisticated nation states and criminal actors are becoming better equipped in the use of cyber toolkits.

We continue to see China, Iran, North Korea and Russia as the nation states posing the greatest cyber threat to the US. For example, last November, the Department of Justice indicted some Chinese hackers for deliberate intrusions seeking trade secrets in the financial, engineering and technology sectors. Iranian cyber actors are reported to have conducted cyber operations against dozens of networks across the Saudi Arabian government and private sectors in late 2016 and early 2017, deleting data from those networks. And just a few months ago, the White House publicly attributed the pervasive WannaCry ransomware to North Korean actors. The Intelligence Community expects that North Korea may continue to use cyber operations as a means to raise funds to offset heavy sanctions, to gather intelligence, or to launch malicious cyber activities against adversaries. Rounding out this malicious foursome, the IC has predicted that Russia—which has heretofore acted with impunity in this sphere—will conduct bolder and more disruptive cyber operations over the next year. It remains to be seen whether recent sanctions and diplomatic expulsions will have an effect on their cyber activities.

Despite our best efforts across the government, the threats posed by malicious cyber activity have now combined with even greater toxicity to present unprecedented challenges across our personal, professional, and political lives in a way that's hard to overstate. History and our own experience have taught us that we collectively tend to underestimate the gravity—and perhaps the probability—of risks, and that we as a society react only after a crisis or calamity.

. . .

Our society has generally made decisions about emerging technologies based upon whether the benefits of the technology outweigh the costs or fundamental risks to our way of life. For example, in the medical industry, we've made a decision that new drugs—no matter how quickly invented or discovered—cannot be brought to market unless and until they are tested and approved. I don't think we've consciously confronted that question yet with respect to cyberspace, but the time to do so is upon us—if it isn't already too late. This question opens up an enormously broad topic which ought not be trampled unexamined in the stampede of technological advancement. But let me leave that weighty topic with you for further reflection, and now focus on the narrower issue of the federal government's functions with respect to cyberspace.

Let me first note that the current and prior administrations have taken important steps at the federal level to address the complexity and pervasiveness of the cyber threat. But work remains to be done by the private sector and Congress, as well as the Executive Branch. Cyber authorities are spread across government agencies. Private sector companies and individuals have taken disparate approaches to cybersecurity. Significant gaps remain in issuing standards and guidance for connected products. Our country is still in the development stage of national-level cyber strategy and policy.

We've seen other nations make strides in adopted unified cyber strategies or national cyber policies. For example, a few years ago, the UK adopted a national

cyber strategy covering 2016 through 2021. More recently, Canada has set aside over $500 million in its 2018 federal budget to fund development of a new cybersecurity strategy and to develop a new Canadian Centre for Cyber Security.

. . .

To date, the US government has played a leading role in defending against and responding to malicious international cyber activity, whether acting alone or in concert with close allies like the UK. The US already deploys non-cyber tools, such as sanctions, public attribution, criminal charges, and extradition, in its responses to that activity. Other nations should recognize the global nature of the problem and take a multilateral approach to cyber threat response—and not merely leave it to the US.

Even so, this isn't a problem solely for governments to solve; as I've already noted, the private sector has a role to play as well. In general, the private sector is well aware of the seriousness of the cyber threat, and some industries, such as the financial and electric sector, have invested significant time and resources into shoring up their critical components and networks. There are many individuals and small businesses, however, who may not have the resources to invest in upgrading and maintaining expensive equipment, may not have access to trained personnel who can provide cybersecurity services, who may be confused by complicated cybersecurity guidance, or who may simply think that they are too small to be a target. Some private network owners—including those who control critical infrastructure—may be willing to accept some security risks in their networks that would be unacceptable to the government. Because we are dealing with a range of expertise and resources, we need to more clearly define private sector responsibilities for cybersecurity and tailor laws and standards accordingly.

We also need the private sector to throw their weight behind government efforts to address threats in cyberspace. If we're going to be successful, companies must share information about what they're seeing on their own networks and to take the initiative to propose their own solutions. Indeed, because the vast majority of our nation's critical infrastructure is privately owned, one could argue that those private sector companies actually share with us a piece of our national security mission.

The enormity of these challenges cannot be overstated. Malefactors of cyber will, in all probability, be ever more successful before we as a society will be able to blunt or negate this threat. But this very probability—the sheer foreseeability of possible and grave harm—underscores the need for our society to do more to counter this almost existential threat. The alternative is to wait until one cyber incident after another forces us to adopt piecemeal solutions to what we all recognize is actually an overarching issue that must be addressed through a comprehensive approach. We need to own this problem that we've all created, and take aggressive steps to manage it before a calamity occurs.

SOURCE: Glenn S. Gerstell, *How We Need to Prepare for a Global Cyber Pandemic*, Speech at the Cipher Brief Threat Conference (Sea Island, Georgia, April 9, 2018), https://www.nsa.gov/news-features/speeches-testimonies/Article/1611673/how-we-need-to-prepare-for-a-global-cyber-pandemic/

ANALYSIS

The notion that individuals with minimal cyber knowledge will be able to launch substantial numbers of dangerous attacks upon computer networks creates a vision of a terrifying future in which the cyber domain is effectively overrun with criminals, saboteurs, and spies. And, to a certain extent, that future is a possibility, particularly if there is no further effort given to creating useful norms and boundaries for behavior in cyberspace. Gerstell's warning offers a terrible vision, but it also offers some commonsense solutions that might mitigate the worst aspects of technological development. In particular, the idea of treating cyberspace in the same fashion as the medical field, with new products and concepts subjected to extremely rigorous screening prior to their release, has merit. However, it also discounts the fact that medical advances are very rarely the product of individuals working without formal training and backed by laboratories—whereas cyber innovations might occur in almost any location, with far less warning. Thus, Gerstell's metaphor has obvious natural limits and should not be considered a panacea for the problems plaguing the cyber domain.

- ***Document 85:*** *Glenn S. Gerstell, "Failing to Keep Pace with the Cyber Threat and Its Implications for Our Privacy Laws"*
- ***When:*** May 23, 2018
- ***Where:*** Georgetown University, Washington, D.C.
- ***Significance:*** Glenn Gerstell, the general counsel for the NSA, offered his position on how advanced computer technology has influenced the perception of the protections afforded by the Fourth Amendment, specifically of government intrusions into the privacy of individual citizens.

DOCUMENT

But I submit that in the case of rapidly developing technology, a case-specific approach, especially one where the legal premise is grounded in the very technology before the court, is inherently problematic. It results in a patchwork quilt of legal precedent about privacy that takes into account only the particular technology directly before the court in each case, which in turn leads to decisions that are sometimes hard to reconcile or are distinguishable only by factors that seem of dubious significance. Most importantly for both the government and the private sector, it yields a set of legal determinations in this area that are, at best, of uneven value in predictive utility. For example, the government needs to know where the lines are to

be drawn and equally the private sector wants some degree of certainty as to exactly what will and will not be protected.

Even the Supreme Court has begun to recognize the limitations on its ability to set out a legal framework that suitably marries Fourth Amendment doctrine with emerging technology. In 2012, Justice Sotomayor called into question the third party doctrine's continued practicality in her concurrence in *United States v. Jones*, writing that "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age." In *Riley v. California*, which was decided in 2014, Chief Justice Roberts wrote that comparing a search through a wallet, purse, or address book to a search of a cell phone "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, wallet, or a purse." At some point, as the Justices have signaled, the quantity of information that an individual shares online or stores in an electronic device may, in aggregate, provide a composite picture of that person that is qualitatively deeper and more insightful than any individual piece of information.

Beyond just its inability as currently applied to keep pace with technology, the Fourth Amendment also suffers from even greater limitations when it comes to protecting your privacy: it is powerless to protect you against any private sector activity. It simply doesn't apply to private companies. This legal framework is far different from the notion of privacy that has driven European lawmaking and court decisions. Unlike the US, the concept of privacy in Europe focuses instead on the dignity of the person and it very much extends to private sector activity. Traditionally, this has resulted in laxer regulation of government surveillance, but much stricter laws about, for example, data protection, credit reporting, and workplace privacy. Europeans value the right to be left alone and protection from public embarrassment or humiliation. These concepts are so important to Europeans that they were woven into the EU's Charter of Fundamental Rights, which mandates respect for private and family life and protection of personal data.

As cyber technology has progressed, the European concept of privacy has resulted in relatively strict laws in Europe about the handling of electronic information. For example, the General Data Protection Regulation, or GDPR, which takes effect in just a few days, applies to all EU organizations, any organizations seeking to offer goods or services to EU subjects, and any companies holding or processing the personal data of people in the EU. Companies who fail to comply with the GDPR can incur penalties of up to 4% of annual global income or €million, whichever is greater. The GDPR seeks to strengthen consent rules, requiring that disclosures be clear, intelligible, and easily accessible, and that it be easy for a user to withdraw consent. It ensures the right to be forgotten, which includes erasing data and preventing its further dissemination. The law also mandates privacy by design; data protection must be designed into systems, rather than added on. If a data breach occurs, companies must provide notification regarding within 72 hours.

Whether we applaud it or not, the European, Japanese and other nations' movement toward comprehensive privacy regulation forces everyone in this digitally

connected world to consider how we are going to reconcile different notions of privacy. We've been persistent in scrutinizing government intrusion into our daily lives—which is certainly a worthy focus—but have we done so at the expense of our personal dignity or the integrity of our private information, particularly given the rapid pace of technological development? Some might say that Europe's approach is better suited to manage the privacy challenges posed by the digital age. Let me make crystal clear that the NSA is not, and I am not, advocating for diminished privacy protections or an increased ability to conduct surveillance. Rather, we at NSA feel duty bound to discuss these types of issues, and we'd like to do so transparently and openly to help reach a consensus as to the best approach.

My key point is that I believe we no longer have the luxury of addressing this issue in an *ad hoc* fashion through our court system, which is largely where our privacy laws have been shaped to date. With Europe pushing ever more aggressive data protection laws, the choice may soon be out of our hands. Companies operating internationally are being forced to adapt their policies and procedures to adhere to regulations implemented in foreign countries. If we want to play a role in shaping those policies to suit our own notions of privacy, we need an overarching effort to address privacy and digital technology here in the US.

The public and private sectors will need to take a holistic approach to addressing privacy concerns associated with our increasing reliance on digital technologies. Similar to the way that new drugs must be reviewed and approved for safety and efficacy before they come to market, perhaps we need laws or regulations requiring review of privacy and cybersecurity safeguards in new connected products before they can be made available to the public. Perhaps, as in Europe, we need stronger notice and consent requirements to regulate how our personal information can be used, shared, or disseminated online. Or perhaps, in some industries, we need to mandate the adoption of low-tech redundancies to safeguard against the loss or manipulation of personal information stored online. This need not necessarily entail government regulation, as industry-generated approaches might be sufficient—but my point is simply that we must have a societal dialogue about how we want to confront the problem.

We also need to consider what privacy means to us here in the US. Because we've emphasized freedom from government surveillance in our current privacy regime, and because the fact-specific legal analysis of that surveillance has focused, as discussed above, on the type and location of the surveillance, the same piece of electronic personal information may be protected from interception by the government, but could be disseminated, sold, or otherwise used by a private company with few, if any, limitations. In only narrow areas, such as HIPAA regulations for health records and Fair Credit Reporting Act requirements for financial records, do our laws focus on the type of information at issue. As I noted earlier about the absence of a focus on the content of communications, we could, for example, have a privacy scheme that was dependent in greater part on the substantive nature of communications rather than how communications are collected. To address these inconsistencies that have grown up around our legal privacy framework, we must evaluate carefully the manner in which private companies rely on connected technology to carry out their business activities. This includes considering not only how and when they collect

personal information from customers, whether to store it online, and whether and to whom it should be disseminated, but also whether relying solely upon networked devices and systems is even the right choice for certain activities when particular sensitivities may be involved.

We also can't forget that each one of us has a great deal of personal responsibility for our own private information. Regard less of what steps the government ultimately takes, we need to maintain awareness of and exercise some amount of discretion about how we are exposing our personal data over the internet.

SOURCE: Glenn S. Gerstell, National Security Agency General Counsel, *Failing to Keep Pace with the Cyber Threat and Its Implications for our Privacy Laws*, Speech at Georgetown Cybersecurity Law Institute, May 23, 2018, https://www.nsa.gov/news-features/speeches-testimonies/Article/1608850/failing-to-keep-pace-the-cyber-threat-and-its-implications-for-our-privacy-laws/

ANALYSIS

Gerstell's reference to European privacy laws in the digital age is an important consideration. A series of European court decisions effectively created a "right to be forgotten," which essentially allowed citizens to demand that their personal information be removed from computer networks upon their request. Not surprisingly, a wide variety of high-technology companies objected to the idea, in part due to the costs associated with enabling such a privilege (and the potential penalties being levied by governments for negligence and noncompliance.) In the United States, there has not been a groundswell of popular support for such a system as yet. But, if the European system functions as it is designed, it might become a useful model for the United States. Making it difficult to retain personal information about individuals would certainly have the side effect of reducing the number and severity of data breaches when they occur, and making it easier to hold companies responsible for their failure to safeguard consumer information. His conception of cyberlaw being developed in a patchwork fashion is also noted, although that same approach is the norm for any radically different branch of law when it first becomes necessary to develop standards and norms. In the United States, federal legislation might serve to unify the expectations of behavior in the cyber domain—but it might also enshrine some deep flaws if it is enacted without the benefit of expert analysis from a diverse array of perspectives.

CHRONOLOGY

1948 The RAND (Research And Development) Corporation is formed, creating a direct partnership between the U.S. Air Force and the Douglas Aircraft Company.

1952 The National Security Agency (NSA) is established to oversee all U.S. government signal intelligence collection efforts, as well as signal counterintelligence activities.

1958 The U.S. government creates the Advanced Research Projects Agency (ARPA) later renamed the Defense Advanced Research Projects Agency (DARPA), an organization dedicated to preventing strategic surprise through technological development.

Jack St. Clair Kilby invents the integrated circuit while working for Texas Instruments. It is the first great leap forward in miniaturization since the completion of the transistor.

Seymour Cray, an engineer for the Control Data Corporation, finishes the first supercomputer, a machine that pushes the limits of processing speed for any given technology. Cray's first model relies upon transistors and will soon be surpassed by integrated circuit machines.

1968 Intel Corporation is founded in Santa Clara, California, and quickly becomes the world's leading producer of microprocessors.

1969 ARPANET is introduced, linking a handful of government and academic computer networks.

1972 The transmission control protocol/internet protocol (TCP/IP) system is created, providing a specific model for how data should be formatted, addressed, transmitted, routed, and received by computers on a network.

1976 Steve Jobs and Steve Wozniak start Apple Computer Corporation and begin to build home computers designed for ease of use.

1978 The Foreign Intelligence Surveillance Act is passed, limiting the ability of federal intelligence agencies to engage in domestic surveillance without court approval.

1979 The first computer worm is developed but is not released on a network.

1983 The movie *WarGames* is released, in which a young hacker nearly starts a nuclear war by accessing a Department of Defense computer system.

The Domain Name System (DNS), a hierarchical naming system for computers connected to networks, is created.

MILNET, the dedicated U.S. military network, is split from ARPANET.

1984 William Gibson publishes the science fiction novel *Neuromancer*, in which the term "cyberspace" is coined.

The term "internet" is created, and the TCP/IP system is selected for communication on it.

1988 The Morris Worm is released from a Massachusetts Institute of Technology laboratory, where it was developed by student Robert Morris. It infects thousands of machines on the nascent internet and reveals the lack of protections against such programs.

Donald Gene Burleson is the first American convicted for the malicious use of software, after writing code to destroy the payroll data of his former employer, creating one of the first logic bombs in history.

The first computer emergency response team (CERT) is formed by DARPA at Carnegie Mellon University, in response to the effects of the Morris Worm.

1993 The Mosaic Web browser is released by the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign. This Web browser makes the internet accessible for nonexpert home users.

1995 The U.S. Congress requires a national policy to protect information infrastructure from strategic effect, as part of the fiscal year 1996 Department of Defense budget authorization bill.

Admiral Arthur K. Cebrowski publicly describes the U.S. military's new concept of network-centric warfare, an attempt to incorporate sensors, commanders, and operators into a single system, making for a reflexive, adaptive military organization.

1997 The U.S. Department of Defense conducts Eligible Receiver, its first information warfare exercise. The thirty-five-person red team easily demonstrates an ability to hack into power grids, government websites, and industry networks using off-the-shelf technology.

1998 Moonlight Maze hacking attacks against government, academic, and corporate networks begins. It is not discovered until 2000, and the culprits have never been identified, although the attacks have been traced to a server in Russia.

In the Solar Sunrise incident, two California high school students and their teenage Israeli mentor compromised more than five hundred computer networks, but because they did not remove any classified data, the Department of Justice declined to press charges.

The U.S. federal budget includes $1.14 billion for critical infrastructure cybersecurity.

Larry Page and Sergey Brin incorporate Google while PhD students at Stanford University.

The Internet Corporation for Assigned Names and Numbers (ICANN) is founded in Los Angeles, California. It coordinates multiple databases to assign unique namespaces on the internet, ensuring its smooth function.

The President's Commission on Critical Infrastructure Protection (PCCIP) is created.

Three thousand Chinese hackers attack Indonesian government websites to protest anti-Chinese riots in Indonesia.

1999 The science fiction blockbuster *The Matrix* is released, in which the protagonist discovers that the entire human population on earth is living in a virtual reality world.

Chinese colonels Qiao Liang and Wang Ziangsui release *Unrestricted Warfare*, a book advocating unconventional strategies to defeat the United States or other technologically advanced nations, including massive cyberattack campaigns.

2000 The ILOVEYOU virus spreads so quickly that it causes $10 billion in damages.

2001 The USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act is passed, creating massive new opportunities for signal intelligence collection in both domestic and international locations.

The Code Red worm exploits a vulnerability in Microsoft's Internet Information Server software, allowing defacement of infected websites and possible theft or destruction of data.

The Nimda worm uses a five-method approach to spread, including through backdoors created by the Code Red worm.

The U.S. federal budget includes over $2 billion for critical infrastructure cybersecurity.

The U.S. Department of Homeland Security is established.

2002 NATO begins its Network Enabled Capabilities Transformation, adopting the network-centric warfare concept for the military alliance.

2003 The U.S. government releases its first National Cyber Security Strategy.

Titan Rain cyberattacks target U.S. government and corporate networks, eventually exfiltrating more than twenty terabytes of data before being discovered. The attacks are eventually traced to China, which denies all culpability.

The SQL Slammer worm is released. It spreads so quickly that it completely shuts down the entire internet for twelve hours. Fifteen years later, it remains one of the most commonly detected pieces of malware.

The MS Blaster worm replicates much of SQL Slammer's success, demonstrating the transitory nature of most security fixes.

John McAfee, creator of McAfee antivirus software, announces the identification of nearly sixty thousand computer virus threats, with an additional ten to fifteen discovered daily.

The Department of Homeland Security announces the creation of the U.S. Computer Emergency Response Team at Carnegie Mellon University.

2004 The Mydoom worm spreads throughout computers operating any recent version of Windows, causing $2 billion in damages worldwide.

2005 General Keith B. Alexander is named director of the National Security Agency, and the organization begins attempts to collect the full electronic communication stream of entire global regions.

2006 General Michael Hayden is named director of the Central Intelligence Agency (CIA), returning from retirement to assume the position as a four-star U.S. Air Force general.

Google begins censoring Chinese search results, as required by the Chinese government in exchange for doing business in the People's Republic of China.

2007 Israel bombs a suspected Syrian nuclear facility, using a cyberattack to blind the Syrian air defense network in the process.

Estonia decides to move a bronze statue depicting a Soviet soldier, provoking a massive cyberattack by Russian hackers against the Baltic nation's cyber infrastructure.

The NSA commences PRISM, a massive data-collection program that targets foreign communications that pass along the backbone of the internet.

Distributed denial of service (DDoS) attacks are launched against the internet's core domain name servers, essentially stopping almost all internet traffic.

2008 Russian hackers contribute to an attack on the republic of Georgia, cutting off Georgia's access to news outlets and attacking Georgian government websites.

WikiLeaks publishes a State Department cable alleging that foreign hackers stole fifty megabytes of email messages, as well as usernames and passwords.

TJX Corporation reports a breach of its credit card information, a cyberattack that eventually costs the company more than $250 million.

Israel launches Operation Cast Lead against Palestinian militants in the Gaza Strip. A massive cyber war erupts between Israeli and Arabic hackers. Both state and nonstate hackers are involved on both sides.

The U.S. military bans the use of all flash drives due to the high incidence rate of worms and viruses on the devices.

2009 A North Korean cyberattack uses a botnet to bring down U.S. and South Korean government websites in response to a planned joint military exercise near the Korean peninsula.

Five million machines participate in a coordinated attack against Israeli internet infrastructure during Israeli attacks in the Gaza Strip.

French naval databases are infected by the Conficker worm, forcing the grounding of naval aircraft.

Google, the internet's largest search engine, announces that it will no longer filter results in the People's Republic of China largely because Chinese hackers have penetrated Google's software and used it to persecute religious dissidents.

Hamas hacktivists deface eight hundred American and Israeli websites.

North Korean government hackers launch attacks in response to UN sanctions over nuclear weapons testing.

Canadian researchers discover "GhostNet," a network of infected computers in 103 countries that are all connected to a single espionage effort against the Tibetan government-in-exile.

2010 U.S. Cyber Command (USCYBERCOM) is activated at Fort Meade, Maryland. It incorporates the separate cyber organizations of each of the military services, as well as the National Security Agency.

The Stuxnet virus is first discovered and publicly reported. Earlier versions of the worm had already significantly damaged the Iranian nuclear program at Natanz.

Google reveals it was attacked as a means to track and hit Chinese subversives.

The "Iranian Cyber Army" hacks the Chinese search engine Baidu and disrupts its service.

2011 Secretary of Defense Robert Gates announces that the United States may consider cyberattacks to be acts of war, and retaliate in any fashion it deems appropriate.

The Georbot worm infects Georgian government systems, allowing both snooping and exfiltration of data. A Georgian CERT team reverses the attack, seizes control of the botmaster's computer, and manages to film him with his own Web camera.

2012 The Shamoon virus attack against Saudi Aramco renders thirty thousand workstations unusable. A previously unknown group, Cutting Sword of Justice, claims responsibility.

The Flame worm is discovered and publicized. It is quickly regarded as the most complex malware ever developed.

The *New York Times* claims the U.S. government engineered the Stuxnet virus. The government refuses to verify the claims, but the Federal Bureau of Investigation (FBI) begins searching for the source of the leaks about Stuxnet.

The Gauss worm is discovered, targeting Lebanese financial institutions used by Hezbollah.

The director of the NSA declares that cyberattacks on U.S. infrastructure increased 1,600 percent between 2009 and 2011.

An Iranian hacker group, Izz ad-Din al-Qassam, launches Operation Ababil, a sustained DDoS attack against Western financial and corporate targets. The attacks continue throughout 2013.

Al Qaeda's recruitment and propaganda websites are attacked and knocked offline for two weeks.

2013 NSA contractor Edward J. Snowden engages in a massive whistleblowing operation, exposing an enormous domestic surveillance program undertaken by the NSA.

Target Corporation reports a data breach in which more than fifty million consumers' credit card information was stolen. The company had failed to engage in even the most basic security measures.

Major media outlets, including the *New York Times*, *Washington Post*, and *Bloomberg News*, announce that they have been under continual Chinese cyberattack for years.

North Korean hackers release DarkSeoul, a malware program targeting South Korean media and financial corporations and specifically designed to evade South Korean antivirus software.

The Syrian Electronic Army hacks into U.S. and European media outlets that have urged intervention in the Syrian civil war.

Hackers encrypt elements of al Qaeda's English-language website, making it unreadable.

Israeli cyber-security experts foil an attempt by the Syrian Electronic Army to disrupt water supplies to the city of Haifa.

Edward J. Snowden releases documents demonstrating that the United States had engaged in cyber espionage against China.

President Barack Obama issues an executive order instructing the United States to aid allies being attacked by North Korean and Iranian hackers.

Mandiant Corporation, a cybersecurity firm, releases a massive report detailing sustained Chinese cyberattacks, probably launched by PLA Unit 61398, against hundreds of Western private corporations and government agencies.

FireEye purchases Mandiant for $1.05 billion.

2014 Admiral Michael S. Rogers is named commander of USCYBERCOM and director of the NSA, continuing the pattern of one military officer commanding both organizations.

A U.S. federal grand jury returns indictments for five members of the Chinese PLA Unit 61398, who are accused of cyber espionage, cyber sabotage, and other computer crimes against private American corporations.

A member of the Islamic State in Iraq and Syria (ISIS) beheads American journalist James Foley on a live video feed broadcast through the internet.

JP Morgan Chase reveals it is the victim of a cyberattack that compromised eighty-three million accounts.

Sony Corporation is hacked probably by North Korean state agencies.

2015 Al Qaeda Electronic emerges, the first cyber franchise of the global terror organization.

The FBI indicts four men, including two Israelis, for hacking JP Morgan Chase's servers.

Kaspersky Lab announces the discovery of Equation Group, an organization reportedly linked to the creation of Stuxnet and Flame.

Microsoft opens its Cyber Defense Operations Center, and signs an information-sharing agreement with NATO.

According to the UN International Telecommunications Union, 3.2 billion people use the internet.

The U.S. Office of Personnel Management detects a data breach affecting 22.1 million current, former and prospective federal government employees' records.

The CIA launches the Directorate for Digital Innovation.

Hacker collective Anonymous declares war on ISIS.

Apple Inc. refuses an FBI demand that it break the security features on an Apple iPhone that had belonged to a terrorist in San Bernardino, California.

2016 The European Union announces new rules on net neutrality that require all citizens have internet access.

Microsoft purchases LinkedIn, expanding its social media presence.

The European Union and NATO sign the Technical Arrangement on Cyber Defense.

Two members of the Syrian Electronic Army are added to the FBI's "Cyber Most Wanted" list.

Tallinn Manual 2.0 is released, focusing on cyber terror, cyber espionage, and cybercrime.

Kevin Mandia is named CEO of FireEye.

WikiLeaks publishes twenty-eight thousand files from Democratic National Committee internal communications, exposing dissent within the party.

Russian hackers are accused of interfering in the U.S. presidential election on behalf of Republican nominee Donald Trump.

2017 President Barack Obama commutes the thirty-five-year sentence of Bradley [Chelsea] Manning after six years.

WikiLeaks publishes more than eight thousand documents demonstrating the CIA's immense ability to break into encrypted devices and networks. The publication includes the source code for dozens of hacking tools.

US-CERT attributes a series of DDoS botnet attacks against media and technology-based corporations to the North Korean government.

Equifax, a credit monitoring firm, discloses that a data breach has exposed more than 140 million people's names, social security numbers, birth dates, and addresses. More than two hundred thousand credit card numbers were also exposed.

Ransomware attacks relying upon NSA-created exploits begin against corporations and government systems.

2018 The Department of Homeland Security confirms that Russian hackers penetrated voter registration rolls in several U.S. states prior to the 2016 election, although no evidence of vote tampering is found.

Ransomware effectively shuts down online services of the cities of Baltimore and Atlanta, in separate incidents.

The U.S. Treasury Department announces sanctions against five Russian companies and three individuals for their roles in Russian cyberattacks against the United States.

The U.S. Department of Justice indicted twelve intelligence officers from Russia for their roles in hacking the Democratic National Committee during the 2016 election cycle.

Australia, Canada, New Zealand, the United Kingdom, and the United States accused the People's Republic of China of conducting

more than a decade of cyber espionage targeting intellectual property and trade secrets of corporations in twelve countries.

2019 USCYBERCOMMAND announces that it blocked internet access for the Russian Internet Research Agency, which had participated in information operations to disrupt the 2016 presidential election.

The Australian Signals Directorate conducted cyberattacks against ISIS to disrupt their communications.

The Israeli Defense Forces conducted airstrikes against Hamas targets in retaliation for attempted cyberattacks by the Palestinian organization.

A previously unknown Chinese cyber espionage organization is found to have conducted a seven-year campaign against corporations involved in telecommunications, medical care, and manufacturing.

BIBLIOGRAPHY

Abbate, Janet. *Inventing the Internet*. Cambridge, MA: The MIT Press, 2000.

Alfreda, Dudley, and James Braman. *Investigating Cyber Law and Cyber Ethics: Issues Impacts and Practices*. Hershey, PA: IGI Global, 2011.

Anderson, Ross. *Security Engineering*. Indianapolis, IN: Wiley, 2008.

Andress, Jason, and Steve Winterfield. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham, MA: Syngress, 2011.

Arquilla, John, and David Ronfeldt. *Cyberwar Is Coming!* Santa Monica, CA: RAND Corporation, 1992.

Arquilla, John, and David Ronfeldt, eds. *In Athena's Camp*. Santa Monica, CA: RAND Corporation, 1997.

Awan, Imran, and Brian Blakemore. *Policing Cyber Hate, Cyber Threats, and Cyber Terrorism*. Burlington, VT: Ashgate, 2011.

Bartlett, Jamie. *The Dark Net: Inside the Digital Underworld*. New York, NY: Melville House, 2015.

Bayuk, Jennifer L. *Cyber Security Policy Guidebook*. Hoboken, NJ: Wiley, 2012.

Blaker, James R. *Transforming Military Force: The Legacy of Arthur Cebrowski and Network Centric Warfare*. Westport, CT: Praeger Security International, 2007.

Blane, John V., ed. *Cyberwarfare: Terror at a Click*. New York, NY: Novinka Books, 2002.

Bossler, Adam M., and Thomas J. Holt. *Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses*. Basingstoke: Routledge, 2016.

Bousquet, Antoine. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. New York, NY: Columbia University Press, 2009.

Bowden, Mark. *Worm: The First Digital World War*. New York, NY: Atlantic Monthly Press, 2011.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York, NY: Penguin Press, 2011.

Brenner, Joel. *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World*. New York, NY: Penguin, 2013.

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State*. New York, NY: Oxford University Press, 2009.

Bryen, Stephen D. *Technology Security and National Power: Winners and Losers*. New Brunswick, NJ: Transaction Publishers, 2016.

Bush, George W. *Decision Points*. New York, NY: Crown Publishers, 2010.

Campbell-Kelly, Martin, William Aspray, Nathan Ensmenger, and Jeffrey R. Yost. *Computer: A History of the Information Machine*. Boulder, CO: Westview Press, 2013.

Carlin, John P., and Garrett M. Graff. *The Dawn of the Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat*. New York, NY: PublicAffairs, 2019.
Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly Media, 2009.
Ceruzzi, Paul E. *Computing: A Concise History*. Cambridge, MA: The MIT Press, 2012.
Chander, Anupam. *The Electronic Silk Road: How the Web Binds the World Together in Commerce*. New Haven, CT: Yale University Press, 2013.
Chapple, Mike, and David Seidl. *Cyberwarfare: Information Operations in a Connected World*. Burlington, MA: Jones and Bartlett Learning, 2015.
Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Great Threat to National Security and What to Do about It*. New York, NY: HarperCollins, 2010.
Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso, 2014.
Deibert, Ron, and Rafal Rohozinski. *Tracking Ghostnet: Investigating a Cyber Espionage Network*. Toronto: Centre for International Studies, University of Toronto, 2009.
Deibert, Ronald. *Black Code: Surveillance, Piracy, and the Dark Side of the Internet*. Toronto: McClelland & Stewart, 2013.
Demchak, Chris. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens: University of Georgia Press, 2011.
DeNardis, Laura. *The Global War for Internet Governance*. New Haven, CT: Yale University Press, 2014.
Dunham, Ken, and Jim Melnick. *Malicious Bots: An Inside Look into the Cyber-criminal Underground of the Internet*. Boca Raton, FL: CRC Press, 2009.
Erickson, Jon. *Hacking: The Art of Exploitation*. 2nd ed. San Francisco: No Starch Press, 2008.
Fowler, Andrew. *The Most Dangerous Man in the World: The Explosive True Story of Julian Assange and the Lies, Cover-ups and Conspiracies He Exposed*. New York, NY: Skyhorse, 2011.
Futter, Andrew. *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Washington, D.C.: Georgetown University Press, 2018.
Gellman, Barton. *Dark Mirror: Edward Snowden and the Surveillance State*. London: Penguin, 2016.
Graham, David. "Cyber Threats and the Law of War." *Journal of National Security Law & Policy*. Vol. 4: 87, 2010.
Green, A. James, ed. *Cyber Warfare: A Multidisciplinary Analysis*. New York, NY: Routledge, 2015.
Greenberg, Andy. *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers*. New York, NY: Plume, 2013.
Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, NY: Metropolitan Books, 2014.
Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley, 2011.
Haerens, Margaret, and Lynn M. Zott, eds. *Hacking and Hackers*. Detroit, MI: Greenhaven Press, 2014.
Hafner, Katie, and Matthew Lyon. *Where Wizards Stay Up Late: The Origins of the Internet*. New York, NY: Simon & Schuster, 1996.
Halpin, Edward, Philippa Trevorrow, David Webb, and Steve Wright, eds. *Cyberwar, Netwar, and the Revolution in Military Affairs*. New York, NY: Palgrave Macmillan, 2006.
Harding, Luke. *The Snowden Files: The Inside Story of the World's Most Wanted Man*. New York, NY: Vintage Books, 2014.
Hardy, Marianna, ed. *The Target Store Data Breaches: Examination and Insight*. New York, NY: Nova Science Publishers, 2014.
Harris, Shane. *The Watchers: The Rise of America's Surveillance State*. New York, NY: Penguin Press, 2010.

Hayden, Michael V. *Playing to the Edge: American Intelligence in the Age of Terror*. New York, NY: Penguin Press, 2016.
Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Washington, D.C.: Atlantic Council, 2014.
Heickerö, Roland. *The Dark Sides of the Internet: On Cyber Threats and Informational Warfare*. Translated by Martin Peterson. New York, NY: Peter Lang Publishing Group, 2013.
Holt, Thomas J., and Bernadette H. Schell. *Hackers and Hacking: A Reference Handbook*. Santa Barbara, CA: ABC-CLIO, 2013.
Isaacson, Walter. *The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution*. New York, NY: Simon & Schuster, 2014.
Johnson, Thomas A., ed. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. Boca Raton, FL: CRC Press, 2015.
Kaplan, Fred. *Dark Territory: The Secret History of Cyber-war*. New York, NY: Simon and Schuster, 2016.
Kello, Lucas. *The Virtual Weapons and International Order*. New Haven, CT: Yale University Press, 2018.
Kerschischnig, Georg. *Cyberthreats and International Law*. The Hague, Netherlands: Eleven International Publishing, 2012.
Kizza, Joseph Migga. *Guide to Computer Network Security*. London: Springer, 2015.
Knake, Robert K. *Internet Governance in an Age of Cyber Insecurity*. New York, NY: Council on Foreign Relations, 2010.
Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Dulles, VA: Potomac Books, 2009.
Lee, Wenke, Cliff Wang, and David Dagon. *Botnet Detection: Countering the Largest Security Threat*. New York, NY: Springer, 2008.
Levy, Steven. *Hackers: Heroes of the Computer Revolution*. Beijing: O'Reilly, 2010.
Lewis, James Andrew. *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. Lanham, MD: Rowman & Littlefield, 2018.
Li, Jennifer J., and Lindsay Daugherty. *Training Cyber Warriors: What Can Be Learned from Defense Language Training?* Santa Monica, CA: RAND, 2015.
Liang, Qiao, and Wang Ziangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.
Libicki, Martin. *Brandishing Cyberattack Capability*. Santa Monica, CA: RAND Corporation, 2013.
Libicki, Martin. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2007.
Libicki, Martin. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.
Libicki, Martin. *Cyberspace in Peace and War*. Annapolis, MD: U.S. Naval Institute Press, 2016.
Lin, Herbert, and Amy B. Zegart. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Washington, D.C.: Brookings Institution Press, 2018.
Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York, NY: Oxford University Press, 2015.
Lucas, George. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. Oxford: Oxford University Press, 2016.
Mahmood, Zaigham, ed. *Continued Rise of the Cloud: Advances and Trends in Cloud Computing*. London: Springer, 2014.
Mandiant Corporation. *APT1: Exposing One of China's Cyber Espionage Units*. Alexandria, VA: Mandiant Corporation, 2013.
Marvel, Elisabette M., ed. *China's Cyberwarfare Capability*. New York, NY: Nova Science Publishers, 2010.

Merrin, William. *Digital War: A Critical Introduction*. New York, NY: Routledge, 2019.
Mitnik, Kevin. *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. New York, NY: Little, Brown and Company, 2011.
Moschovitis, Christos J. P., Hilary Poole, Tami Schuyler, and Theresa M. Senft. *History of the Internet: A Chronology, 1843 to the Present*. Santa Barbara, CA: ABC-CLIO, 1999.
Mueller, Milton. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010.
Nagaraja, Shishir, and Ross Anderson. *The Snooping Dragon: Social-malware Surveillance of the Tibetan Movement*. Cambridge: Computer Laboratory, University of Cambridge, 2009.
Nicks, Denver. *Private Bradley Manning, WikiLeaks, and the Biggest Exposure of Official Secrets in American History*. Chicago, IL: Review Press, 2013.
Olson, Parmy. *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency*. New York, NY: Back Bay Books, 2012.
Poindexter, Dennis F. *The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interests*. Jefferson, NC: McFarland, 2013.
Poroshyn, Roman. *Stuxnet: The True Story of Hunt and Evolution*. Denver, CO: Outskirts Press, 2013.
Reveron, Derek S., ed. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, D.C.: Georgetown University Press, 2012.
Richards, Julian. *Cyber-war: The Anatomy of the Global Security Threat*. London: Palgrave, 2014.
Rid, Thomas. *Cyber War Will Not Take Place*. New York, NY: Oxford University Press, 2013.
Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*. Santa Barbara, CA: Praeger Security International, 2013.
Russell, Alison Lawlor. *Strategic A2/AD in Cyberspace*. New York, NY: Cambridge University Press, 2017.
Sambaluk, Nicholas Michael, ed. *Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology*. Santa Barbara, CA: ABC-CLIO, 2019.
Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York, NY: Cambridge University Press, 2013.
Schneier, Bruce. *Secrets and Lies: Digital Security in a Digital World*. New York, NY: John Wiley & Sons, Inc., 2000.
Shakarian, Paulo, Jana Shakarian, and Andrew Ruef. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Waltham, MA: Syngress, 2013.
Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press, 2014.
Spinello, Richard A. *Cyberethics: Morality and Law in Cyberspace*. Sudbury, MA: Jones & Bartlett, 2011.
Springer, Paul J. *Cyber Warfare: A Reference Handbook*. Santa Barbara, CA: ABC-CLIO, 2015.
Stiennon, Richard. *Surviving Cyber War*. Lanham, MD: Government Institutes, 2010.
Stocker, Gerfried, and Christine Schöpf. *Info War*. New York, NY: Springer-Verlag, 1998.
Stryker, Cole. *Hacking the Future: Privacy, Identity, and Anonymity on the Web*. New York, NY: Overlook Duckworth, 2012.
Taddeo, Mariarosaria. *The Ethics of Cyber Conflicts: An Introduction*. London: Taylor and Francis Group, 2016.
Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York, NY: Oxford University Press, 2018.
Ventre, Daniel, ed. *Cyberwar and Information Warfare*. Hoboken, NJ: John Wiley & Sons, 2011.
Verma, Nina. *Social Engineering: A Means to Violate a Computer System*. New Delhi, India: Global Vision Publishing House, 2011.
Vigna, Paul, and Michael J. Casey. *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order*. New York, NY: St. Martin's Press, 2015.

Wang, Jie, and Zachary A. Kissel. *Introduction to Network Security: Theory and Practice*. Hoboken, NJ: Wiley, 2015.

Weiman, Gabriel. *Terror on the Internet: The New Arena, the New Challenges*. Washington, D.C.: USIP, 2006.

Whyte, Christopher, and Brian M. Mazanec. *Understanding Cyber Warfare: Politics, Policy and Strategy*. New York, NY: Routledge, 2019.

Zettner, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY: Broadway Books, 2015.

INDEX

ABOUT THE AUTHOR

PAUL J. SPRINGER, PhD, is a full professor of comparative military studies and the chair of the Department of Research at the Air Command and Staff College, Maxwell Air Force Base, Alabama. He is the author or editor of *America's Captives: Treatment of POWs from the Revolutionary War to the War on Terror* (2010); *Military Robots and Drones: A Reference Handbook* (ABC-CLIO, 2013); *Transforming Civil War Prisons: Lincoln, Lieber, and the Politics of Captivity*, with Glenn Robins (2014); *Cyber Warfare: A Reference Handbook* (ABC-CLIO, 2015); *9/11 and the War on Terror: A Documentary and Reference Guide* (Greenwood, 2016); *Encyclopedia of Cyber Warfare* (ABC-CLIO, 2017); *Outsourcing War to Machines: The Military Robotics Revolution* (Praeger, 2018); *Daily Lives of U.S. Soldiers*, with Christopher R. Mortenson (2019); and *Propaganda from the American Civil War* (ABC-CLIO, 2019). He is also a senior fellow of the Foreign Policy Research Institute.