DCAF HORIZON 2015 WORKING PAPER NO. 7

On Cyberwarfare

Fred Schreier






On Cyberwarfare

Fred Schreier






Table of Contents

On Cyberwarfare

The digital world has brought about a new type of clear and present danger: cyberwar. Since information technology and the internet have developed to such an extent that they have become a major element of national power, cyberwar has become the drumbeat of the day as nation-states are arming themselves for the cyber battlespace. Many states are not only conducting cyber espionage, cyber reconnaissance and probing missions; they are creating offensive cyberwar capabilities, developing national strategies, and engaging in cyber attacks with alarming frequency. Increasingly, there are reports of cyber attacks and network infiltrations that can be linked to nation-states and political goals. What is blatantly apparent is that more financial and intellectual capital is being spent figuring out how to conduct cyberwarfare than for endeavors aiming at how to prevent it.[1] In fact, there is a stunning lack of international dialogue and activity with respect to the containment of cyberwar. This is unfortunate, because the cyber domain is an area in which technological innovation and operational art have far outstripped policy and strategy, and because in principle, cyberwarfare is a phenomenon which in the end must be politically constrained.

Many prominent authors see a war being waged in cyberspace today – a fact not undisputed by those who think that the threat of cyberwar has been grossly exaggerated.[2] Cyberspace is increasingly used as a theater of conflict as political, economic, and military conflicts are ever more often mirrored by a parallel campaign of hostile actions on the internet. Attacks can rapidly go global as covertly acquired or hacked computers and servers throughout the world are kicked into service, with the result that many nations are quickly drawn in. And it is in this context that the term 'cyberwar' has become a frequently used buzzword to refer to any kind of conflict in cyberspace with an international dimension. Such a broad use of the term, however, is not helpful, particularly not in view of the fact that the difficulties in determining the origin and nature of the attack, and assessing the damage incurred, are three of the major problems encountered with cyber attacks. What is required instead is a conceptual categorization of the various forms of conflict in cyberspace as a precondition for assessing the danger they pose and the potential damage they can cause.

This is what this contribution will try to do. The aim is to examine broad cyberwarfare issues: what cyberwar means, what it entails, and whether threats

1 Exact figures are hard to pin down. While budgets for cybersecurity are readily available, for the UK, for example, it will grow by some £650 million over the next four years, those for offensive activities are all classified and, in the case of the UK, contained in the Single Intelligence Account, which provides for 2011-12 £2.1 billion funding for the Security Service, the Secret Intelligence Service and the GCHQ. The US DoD provided Congress with three different views of its cybersecurity budget estimates for fiscal year 2012 ($2.3 billion, $2.8 billion, and $3.2 billion respectively). These do not include costs for offensive operations, which are funded from the national intelligence and military intelligence program budgets.

2 See: Marc Rothenberg & Bruce Schneier, The cyber war threat has been grossly exaggerated, Arlington, Intelligence Squared U.S., 8 June 2010.

can deter it or defense can mitigate its effects. Its focus is on cyberwarfare activities sponsored by nation-states. (1) The basic building blocks of the subject are presented: cyberspace, cyberpower, cyberwarfare, and cyberstrategy. (2) The distinction will be made between cyberwar and information warfare, the latter a concept of much wider scope, followed by the presentation of the elements that seem to make cyberwar attractive. (3) The major problems are listed that derive from the nature of cyberspace – understanding the cyber threat. (4) The cyber vulnerabilities are addressed that show how cyber attacks are enabled. (5) Some of the major issues, ambiguities, and problems of cyberwar will be discussed, showing the use and limits of power in cyberspace. In Annex 1, we will show in which ways cyberwarfare is different from the other warfighting domains, and in Annex 2 we present a summary of some of the major instances of cyber conflict.

It is important to point out that other kinds of cyber attacks take place regularly, which are much more frequent than state-sponsored activities.[3] These are committed by hackers that have expertise in software programming and manipulation. They concentrate their actions on exploiting the intricacies of computer networks. Some hackers are state-sponsored and perform lawful activities, but some are not. Both kinds can be instrumental in the conduct of cyberwarfare. When cyberwarfare operators conduct cyber attacks for authorized state-sponsored attacks and use legal means, they are considered to be legal hackers. Legal hackers conduct cyberspace operations under legal authority for legal purposes with no adversarial intent. For example, cyber security experts deliberately hack into computer networks to find inherent weaknesses. Members of the armed forces and government intelligence services also deliberately hack into military computer networks to find vulnerabilities, and to test defensive and offensive abilities. These hackers are either industry or government-sponsored and are not hacking for personal gain. If hackers are attempting to gain access into computer networks for the sake of political gain, it can be part of a state-sponsored campaign. What determines the legality of these operations is intent.

Other kinds of cyber attacks that take place regularly and which are much more frequent than state-sponsored activities are unauthorized attempts to access computers, computer controlled systems, or networks. However, these will not be addressed in this essay. Such activities can range from simply penetrating a system and examining it for the challenge, thrill, or interest, to entering a system for revenge, to steal information, cause embarrassment, extort money, or cause deliberate localized harm to computers or damage to larger critical infrastructures. Among these cyber attacks three forms can be distinguished: cyber vandalism, cyber crime, and cyber espionage. The realm for the resolution of these attacks normally lies in law enforcement and judicial systems, and legislative remedy where necessary.

Cyber vandalism is 'cyber hacktivism,' which is a common term for hackers who use illegal digital tools in pursuit of political ends.[4] Hacktivists cause damage

3 See: Cyber Security: The Road Ahead, DCAF Horizon 2015 Working Paper Series (4), Geneva, Geneva Centre for the Democratic Control of Armed Forces, 2011.

4 These tools include website defacements, redirects, denial of service attacks, malware, information theft, website parodies,

through virtual modification or destruction of content by hacking websites and disrupting or disabling servers by data overload. Some conduct cyber operations on behalf of personal political causes such as the environment, human rights, and animal rights. Cyber vandalism, sometimes also called 'cyber hooliganism,' is the most widespread form of cyber conflict and garners a great deal of public attention. The effects of such incidents are, however, generally limited in time and more often just a relatively harmless annoyance.

Cyber crime or Internet crime, undertaken for criminal gain, is taking place regularly and independently of conflicts. Cybercrime provides an environment in which attack techniques can be refined: "It is the laboratory where the malicious payloads and exploits used in cyberwarfare are developed, tested, and refined."[5] Directed primarily against the financial system, these illegal acts seek to extort or extract money. The main victims are the banking sector, financial institutions, and the corporate sector. Government networks with classified data are also affected, but are targeted less often. Though it is difficult to get undisputed data, the global costs of cybercrime are enormous and estimated to lie in the range of US$ 1 trillion annually,[6] thus more than the gains from drug trafficking. A study by the UK Cabinet Office suggests that cybercrime costs the UK alone £27 billion annually, £2.2 billion to government, £3.1 billion to individuals, and by far the largest portion, £21 billion, to industry, in the form of theft of intellectual property, customer data and price-sensitive information.[7]

Cyber espionage is a routine occurrence and an expansion of traditional efforts to collect information on an opponent's secrets, intentions, and capabilities. It consists of the search for access to classified, personal or corporate data, intellectual property, proprietary information and patents, or results from research and development projects, for reconnaissance, probing, and testing of information and communications technology (ICT) defenses, and clandestine manipulation of data, information and critical infrastructure for war preparation. The return on investment for targeting sensitive information can be extremely high compared to the skills and technology required to penetrate the systems, which are relatively low.[8] And acts of cyber espionage can be as much or more pervasive than acts of cyberwarfare, as the publication of 250,000 classified US embassy cables in November 2010 by WikiLeaks testified.

virtual sit-ins, virtual sabotage, and software development.

5 Jeffrey Carr, Inside Cyber Warfare, Gravenstein Highway North, Sebastopol, CA, O'Reilly Media, Inc., 2010, p. 5.

6 Seymour M. Hersh, "The Online Threat", The New Yorker, 1 November 2010, p. 51, citing President Obama who, referring to corporate cyber espionage, said in a speech in May, 2009, "It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to one trillion dollars." According to the UK's National Security Strategy 2010, cybercrime has been estimated to cost as much as $1 trillion per year globally, with untold human cost. UK Cabinet Office, A Strong Britain in an Age of Uncertainty, p. 29.

7 Detica and Office of Cyber Security and Information Assurance, The Cost of Cybercrime, London, February 2011.

8 Eleanor Keymer, "The cyber-war," Jane's Defence Weekly, No. 39, 29 September 2010, p. 24.

1. The Basic Building Blocks: Cyberspace, Cyberpower, Cyberwarfare, and Cyberstrategy

A synoptic view and comprehension of the subject of cyberwar require familiarization with the four *basic building blocks*: *cyberspace*, *cyberpower*, *cyberwarfare*, and *cyberstrategy*.

Cyberspace

Cyberspace, the novel 5th space of warfare after land, sea, air, and space, is all of the computer networks in the world and everything they connect and control via cable, fiber-optics or wireless. It is not just the Internet – the open network of networks.[9] From any network on the Internet, one should be able to communicate with any computer connected to any of the Internet's networks. Thus, cyberspace includes the Internet *plus* lots of other networks of computers,[10] including those that are not supposed to be accessible from the Internet. Some of those private networks look just like the Internet, but they are, theoretically at least, separate. Other parts of cyberspace are transactional networks that do things like sending data about money flows, stock market trades, and credit card transactions. In addition, there are the networks which are Supervisory Control and Data Acquisition (SCADA) systems that just allow machines to speak to other machines: control panels talking to pumps, elevators, generators, etc. Thus, cyberspace is composed of the now two billion computers existing, plus servers, routers, switches, fiber-optic cables, and wireless communications that allow critical infrastructures to work.

Numerous definitions of cyberspace exist. According to one such definition "cyberspace is not a physical place – it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, IT systems, and telecommunication infrastructures commonly referred to as the World Wide Web."[11]

9 The Internet is an open network of end points, devices, and computer networks that communicate with each other using the TCP or IP communications protocol. It is built in an open, decentralized manner, and from any end point in it it is possible to communicate with any other end point. Countless applications have been created on top of this basic design, and among them are those that are intended to limit access, verify identify, encrypt information transferred over the web, verify receipt of information, and so on.

10 Many networks have been designed and built in order to carry out defined tasks. For example: GPS, ACARS, SWIFT; GSM Cellular, and thousands of other mission-specific computer networks.

11 Thomas C. Wingfield, The Law of Information Conflict: National Security Law in Cyberspace, Aegis Research Corp., 2000, p. 17.

For the US Department of Defense: "cyberspace is a domain characterized by the use of computers and other electronic devices to store, modify and exchange data via networked systems and associated physical infrastructures."[12] For one well informed expert, "cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via inter-connected information and communication technology-based systems and their associated infra-structures."[13] Already these few examples illustrate the difficulty in defining the term, which may be one of the difficulties in creating any type of common agreement among states as to how international law should be applied to warfare conducted in cyberspace.

These networked and interconnected information systems reside simultaneously in both physical and virtual space, and within and outside of geographical boundaries. Their users range from nation-states and their component organizational elements and communities down to individuals and amorphous trans-national groups who may not profess allegiance to any traditional organization or national entity. They rely on three distinct yet interrelated effects of three dimensions: the *physical*, the *informational*, and the *cognitive*. In the aggregate, these comprise the global information environment as outlined in the doctrine for Information Operations: the physical platforms, systems and infrastructures that provide *global connectivity* to interconnect information systems, networks, and human users; the massive amounts of *informational content* that can be digitally and electronically sent anywhere anytime to virtually anyone; and the *human cognition* that results from greatly increased access to content, which can have a dramatic impact on human behavior and decision making.[14]

Warfare of the 21st Century involving opponents possessing even a modicum of modern technology is not possible without access to cyberspace. New operational concepts such as 'Network Centric Warfare'[15] in an 'informationalized battlespace' would be impossible without cyber-based systems and capabilities. The ability to reprogram the targeting data within a weapon on its way to the target, then rely on real-time updates from a GPS satellite to precisely strike that target, is possible only through the use of cyberspace. Cyberspace exists across the other domains of land, sea, air, and space and connects these physical domains with the cognitive processes that use the data that is stored, modified, or exchanged. However, it is the use of *electronic technologies* to create and 'enter' cyberspace, and use the energies and properties of the *electromagnetic spectrum* (EMS)[16] that sets cyberspace apart from the other domains, and what makes cyberspace unique.[17]

12 Joint Chiefs of Staff, *Joint Publication 1-02*, Washington D.C., US Department of Defense, 12 April 2001.
13 Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr & Larry K. Wentz, eds., *Cyberpower and National Security*, Washington D.C., National Defense University Press, Potomac Books, 2009.
14 Ibid.
15 The concept of 'network centric warfare' dates to 1998. See: Arthur K. Cebrowski & John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *United States Naval Institute Proceedings*, January 1998.
16 Definition of electromagnetic spectrum (EMS): The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands, JP 1-02.
17 Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," op. cit.

One characteristic of cyberspace is that *it cannot exist without being able to exploit the naturally existing EMS*. Without the EMS, not only would millions of information and communications technologies (ICT) be unable to communicate with each other, but the ICTs themselves would be unable to function. Integrated circuits and other microelectronic devices depend on electrons to function. Fiber-optic cables are nothing if they are unable to propagate light. Moreover, ICT networks are also dependent upon the myriad properties of the EMS for their essential connectivity via *radio frequency* and *microwaves*.[18]

A second characteristic is that *cyberspace requires man-made objects to exist*, which again makes cyber-space unique when compared to the land, sea, air, and space domain. Cyberspace would not exist were it not for the ability of human beings to innovate and manufacture technologies capable of exploiting the various properties of the EMS.

A third characteristic is that *cyberspace can be constantly replicated*. There can be as many cyberspaces as one can possibly generate. But there is one portion of the air, sea, or land domain that is important: the portion that is contested. With cyberspace, however, there can be many in existence at any one time – some contested, some not. In addition, for the most part, *nothing is final in cyberspace*.[19] And due to relatively inexpensive and readily available hardware, *IT systems and networks, if damaged, can be quickly repaired and reconstituted.*[20]

A forth characteristic is that *the cost of entry into cyberspace is relatively cheap*. The resources and expertise required to enter, exist in, and exploit cyberspace are modest compared to those required for exploiting the land, sea, air, and space domains. Generating strategic effects in cyberspace does not require a budget of billions, large numbers of manpower and weapons. Rather, modest financial outlays, a small group of motivated individuals, and access to networked computers can provide entry into cyberspace. The character of cyberspace, however, is such that the number of actors able to operate in the domain and potentially generate strategic effect is *exponential when compared to the other domains*.

A further characteristic is that, for the time being, *the offense rather than the defense is dominant in cyberspace*, for a number of reasons. First, defenses of IT systems and networks rely on vulnerable protocols and open architectures, and the prevailing defense philosophy emphasizes threat detection, not elimination of the vulnerabilities.[21] Second, attacks in cyberspace occur at great speed, putting defenses under great pressure, as an attacker has to be successful only once, whereas the defender

18 David J. Lonsdale, The Nature of War in the Information Age: Clausewitzian Future, London, Frank Cass, 2005, pp. 179-200.
19 Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, New York, Cambridge University Press, 2007, pp. 5-6.
20 Ibid., pp. 84-85.
21 See: Richard A. Clarke & Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About it*, New York, Ecco, 2010, pp. 103-149.

has to be successful all the time. Third, range is no longer an issue in cyberspace since attacks can occur from anywhere in the world.[22] Fourth, the attribution of attacks is particularly difficult, which is complicating possible responses.[23] And fifth, modern society's overwhelming reliance on cyberspace is providing any attacker *a target-rich environment*, resulting in great strain on the defender to successfully defend the domain.[24]

Many consider cyberspace as the newest and most important addition to the *global commons*, which comprise four domains: maritime, air, space, and now cyber. Maritime and air are the international oceans and skies that do not fall under the jurisdiction of any nation. Outer space begins at a point above the earth where objects remain in orbit. And cyberspace is the EMS that enables digital processing and communications. The maritime domain has been used by humans for millennia, air for a century, and space for six decades. Cyberspace as the newest and most important of the global commons has been widely available for less than thirty years, yet more than a quarter of the world's population now uses it every day, and that number continues to expand. Thus, cyberspace has become the *center of gravity* for the globalized world, and for nations the center of gravity not only for military operations but for all aspects of national activity, to include economic, financial, diplomatic, and other transactions.

Cyberspace can also be seen as the *'terrain' of technology mediated communication*. Reduced to basics, cyberspace is the proverbial ether within and through which electromagnetic radiation is propagated in connection with the operation and control of mechanical and electronic transmission systems. Moreover, it is a medium in which information can be created and acted on anytime, anywhere, and by essentially anyone.

Cyberspace is qualitatively different from the sea, air, and space domains, *yet it both overlaps and continuously operates within all of them*. More importantly, it is the only domain in which all instruments of national power – diplomatic, informational, military, and economic – can be concurrently exercised through the manipulation of data and gateways. Just like the other commons, it is one in which continued uninhibited access can never be taken for granted as a natural and assured right. Were unimpeded access to the EMS denied through hostile actions, satellite aided munitions would become useless, command and control mechanisms would be disrupted, and the ensuing effects could be paralyzing. Accordingly, cyberspace has become an emerging theater of operations that undoubtedly will be contested in future conflicts. Successful exploitation of this domain through network warfare operations can allow an opponent to dominate or hold at risk any or all of the global commons. Yet uniquely among the other three, cyberspace is a domain in which the

22 Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, Franklin D. Kramer. Stuart H. Starr & Larry K. Wentz, eds., Dullas, VA, Potomac Books, 2009, 255-256.
23 Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*, New York, Oxford University Press, 2009.
24 Richard A. Clarke & Robert K. Knake, *Cyber War,* op. cit., 170-175.

classic constraints of distance, space, time, and investment are reduced, sometimes dramatically, both for us and for potential enemies.

Cyberpower

Power based on information resources is not new; cyberpower is.[25] While cyberspace is the domain in which cyber operations take place, cyberpower is the sum of strategic effects generated by cyber operations in and from cyberspace. According to one widely used definition, "cyberpower is the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power."[26] Its strategic purpose revolves around the ability in peace and war to manipulate perceptions of the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment. Transforming the effects of cyberpower into policy objectives is the art and science of strategy, defined as "managing context for *continuing advantage according to policy*."[27] Basically, cyberpower is the capability to control IT systems and networks in and through cyberspace. "Cyberpower is the use, threatened use, or effect by the knowledge of its potential use, of disruptive cyber attack capabilities by a state."[28] Power depends on context, and cyberpower depends on the resources that characterize the domain of cyberspace. And across the other elements and instruments of power, cyberpower creates synergies between those elements and connects them in ways that improve all of them.

Cyberpower is shaped by multiple factors. While cyberspace just exists as an environment, cyberpower is always *a measure of the ability to use that environment*. Technology is one factor, because the ability to 'enter' cyberspace is what makes its use possible. That technology is constantly changing, and some users – countries, societies, non-state actors, etc. – may be able to leap over old technologies to deploy and use new ones to dramatic advantage. Organizational factors also play a role, because organizations reflect human purposes and objectives, and their perspectives on the creation and use of cyberpower are shaped by their organizational mission, be it military, economic or political. But the element most closely tied to cyberpower is *information*. Cyberspace and cyberpower are dimensions of the *informational instrument of power*, and there are myriad ways that cyberpower links to, supports, and enables the exercise of the other instruments of power.[29] Thus, information is the *currency or DNA of cyberpower*.

25 Joseph S. Nye, *Cyber Power*, Cambridge, Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010, p. 3. See also: Patrick Gorman, "The Road to Cyberpower: Seizing Opportunity While Managing Risk in the Digital Age," Booz Allen Hamilton, 11 February 2010.
26 Kuehl, in Kramer, op. cit., p. 38.
27 Everett C. Dolman, Pure Strategy: Power and Principle in the Space and Information Age, London, Frank Cass, 2005, p. 6.
28 Franklin D. Kramer, *Cyberpower and National Security*, op. cit. p. 48.
29 Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," op. cit.

In the global economy of the 21st Century, cyberspace is probably the single most important factor linking all the players together, boosting productivity, opening new markets, and enabling management structures that are simultaneously flatter and with far more extensive reach. The same applies for the development of new technologies in their creation, exploitation, and measurement of success. And cyberpower's impact on political and diplomatic affairs is hardly less intensive. The world's most ubiquitous influence medium remains satellite television, carried by systems and network that connect via cyberspace. The influence campaigns being waged by the US government and by terrorist networks of the al Qaeda type are both using cyberpower in their struggle for hearts, minds, and ideas.[30]

Cyberspace is also transforming how information is created: the raw material that fuels economies and societies. And new forms of content – images, sounds, information and data in multiple forms – and the connectivity used to transmit and exchange that content, are transforming the ways in which influence can be exerted. This also by employing 'soft power' and 'smart power' in the pursuit of strategic goals. As cyberpower has exerted increasingly widespread impacts across society during the past two decades, states are forced to adapt to those impacts in new ways. Perhaps the most significant and transformative impact cyberspace and cyberpower are having is that of linking people and organizations in new ways in an increasingly wired world in which traditional borders are being altered and new relationships among people are being forged, now ever more often also with governments and individuals interacting with each other across national borders.

Cyberpower can be used to produce preferred outcomes *within* cyberspace, or it can use cyber instruments to produce preferred outcomes in other domains *outside* cyberspace. The key elements of cyberpower are the science of the electromagnetic spectrum, the technology of electronics, and integrated manmade infrastructure. The key aspect of cyberpower is its capability to manipulate or access a target's cyber infrastructure via exploitation and attack. Means of cyberpower come via cyberwarfare. Cyberwarfare is the use of cyberpower to either inflict or threaten punishment against an adversary, or to achieve political objectives through force without the opponent's acquiescence.[31]

Cyberpower relies on hardware and software. Hardware is the mechanical, magnetic, electronic, and electrical devices comprising a computer system, such as the central processing unit,[32] disk drives, key-board, or screen. Cables, satellites, routers, computer chips, and the like are also considered hardware. Software consists of the programs used to direct computer operations and uses. Malware is malicious software that interferes with normal computer and Internet-based application functions and is a key weapon in cyberwarfare.

30 Ibid.
31 Lech Janczewski & Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism*, Hershey, Idea Group Inc., 2007, p. xiv.
32 Central Processing Unit (CPU): A microprocessor chip that serves as the heart of a computer. It interprets and carries out instructions, performs numeric computations, and controls the peripherals connected to it.

Cyberpower has three main characteristics: it is *ubiquitous*, it is *complementary*, and it can be *stealthy*. Land, sea, air, and space power are able to generate strategic effect on each of the other domains. But nothing generates strategic effect in all domains so absolutely and simultaneously as cyberpower,[33] because *cyberpower is ubiquitous*.

Unlike land, sea, and airpower, but in some respects like space power, cyberpower is a *complementary instrument*, particularly when used autonomously. It is indirect because the coercive ability of cyberpower is still limited. While cyber attacks can be damaging and disruptive, neither the attacks suffered by Estonia in 2007 and by Georgia in 2008, nor the Stuxnet attack on Iranian nuclear facilities in 2010/11, have been really coercive. This may well change in the future. But for this to happen, coercion must first be proven. Shutting down a power grid via cyberpower, for example, would most likely have catastrophic consequences. But rather than coercing its victim to concede to an attacker's demands, it may only invite an even more catastrophic response. Thus, until cyberpower will prove its coercive capability, it can be said to be a *complementary instrument*.

The last characteristic, *that cyberpower can be stealthy*, makes it attractive to many users. They can use this ability to wield it surreptitiously on a global scale without it being attributable to the perpetrator. Databases can be raided for classified or proprietary information without the owners being any wiser after terabits of data have been stolen. Malicious software can be planted in adversary IT systems and networks without knowledge until these weapons are activated and cause their intended damage. Such stealthy use of cyberpower, aided by the inherent difficulties of attributing the identity and motivation of most attackers, makes it an attractive instrument for governments and other actors.[34]

Cyberwarfare

Militarily, cyberpower has been the most influential instrument of the past two decades. Both cyberpower and cyberspace have been at the heart of *new concepts* and *doctrines of war*. Across the levels of conflict, from insurgency to main-force conventional warfare, *cyberpower has become an indispensable element of modern technology-based military capability*.

As with the term cyberspace, there is no universally accepted definition of cyberwarfare. According to one general definition "cyberwarfare refers to a massively coordinated digital assault on a government by another, or by large groups of citizens. It is the action by a nation-state to penetrate another nation's computers and networks for the purposes of causing damage or disruption." But it adds that "the term cyberwarfare may also be used to describe attacks between corporations,

33 David J. Lonsdale, *Nature of War in the Information Age*, op. cit., pp.284-186.
34 See: Brenner, *Cyberthreats,* op. cit., and Clarke, *Cyber War*, op. cit., pp. 197-200

from terrorist organizations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent."[35] Another definition is: "Cyberwarfare is symmetric or asymmetric offensive and defensive digital network activity by states or state-like actors, encompassing danger to critical national infrastructure and military systems. It requires a high degree of interdependence between digital networks and infrastructure on the part of the defender, and technological advances on the part of the attacker. It can be understood as a future threat rather than a present one, and fits neatly into the paradigm of Information Warfare."[36] The US Department of Defense defines cyber operations as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[37] A computer network attack is defined as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and network themselves."[38] A 2001 Congressional Research Service Report notes that "cyberwarfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same."[39] A later report defined computer network attacks as "operations to disrupt or destroy information resident in computers and computer networks."[40] A further definition of cyberwar is "a conflict that uses hostile, illegal transactions or attacks on computers and networks in an effort to disrupt communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defenses."[41] And finally, according to a recent UN Security Council Resolution, "Cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another state including: intentional access, interception of data or damage to digital and digitally controlled infrastructure. And production and distribution of devices which can be used to subvert domestic activity."[42]

A successful cyberwar depends upon two things: means and vulnerability. The 'means' are the people, tools, and cyber weapons available to the attacker. The vulnerability is the extent to which the enemy economy and military use the Internet and networks in general.[43] We do not know who has what cyberwar capabilities exactly. But a growing number of states have organized cyberwar units and ever more skilled Internet experts for combat in this domain.[44]

35 See: http://definitions.uslegal.com/c/cyber-warfare/
36 Shane M. Coughlan, "Is there a common understanding of what constitutes cyber warfare?," The University of Birmingham School of Politics and International Studies, 30 September 2003, p. 2.
37 Joint Chiefs of Staff, *Joint Publication 1-02, Dictionary of Military and Associated Terms* (JP 3-0), Department of Defense, Washington D.C., 8 November 2010 (As Amended Through 15 October 2011).
38 Ibid.
39 Stephen A. Hildreth, *Cyberwarfare*, Congressional Research Service Report for Congress, No. RL30735,19 June 2001.
40 Clay Wilson, *Information Operations and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service Report for Congress, No. RL31787, 14 September 2006.
41 Kevin Coleman, *The Cyber Arms Race Has Begun*, CSO Online, 28 January 2008.
42 UN Security Council, Resolution 1113 (2011), 5 March 2011.
43 James F. Dunnigan, The Next War Zone: Confronting the Global Threat of Cyberterrorism, New York, Citadel Press, 2002, p. 11.
44 James A. Lewis & Katrina Timlin, *Cybersecurity and Cyberwarfare 2011,* Washington D.C., CSIS, UNIDIR

A National Strategy for Cyberspace

Cyberpower is technically, tactically, and operationally distinct from the other instruments of military power. But it is not beyond strategy. Nor does it subvert the enduring nature of war, which is unchanging. The key strategic attribute of cyberpower is the ability in peace and war to manipulate the *strategic environment* to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment. This *strategic utility extends to all the other strategic domains*, given their ubiquitous dependence upon cyberspace. Manipulation produces the strategic effect of misdirection and deception that in turn allows other military and national instruments of power to achieve policy objectives directly. Cyberpower is subservient to the needs of policy, and strategy is the process of translating those needs into action. Cyber operations take place in cyberspace and generate cyberpower, but they do not serve their own ends: they serve *the ends of policy*. Strategy is the bridge between policy and the exploitation of the cyber instrument.

Cyberpower is exerting itself as a *key lever in the development and execution of national policy*. Its capabilities challenge the strategist to integrate those capabilities with other elements and instruments of power. And this requires the crafting of a *cyberstrategy*, which is "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational realms, to achieve or support the achievement of objectives across the elements of national power."[45]

Cyberstrategy builds on a systematic and structured combination of *ends* (goals and objectives), *means* (resources and capabilities), and *ways* (how the means are used to accomplish the ends), tempered with due analysis and considerations of the risks and costs. To develop a national strategy for cyberspace, therefore, is to simultaneously create cyber resources and procedures that can contribute to the achievement of specific national security objectives. The most important part of cyberstrategy concerns the ends for which cyber capabilities might be used. These ends are part of the larger military, political, economic, diplomatic, and national security objectives being sought. Cyberpower is created to support the attainment of larger objectives: strategic goals across the elements of national power as a means of satisfying the vital national needs and interests of the *National Security Strategy*. The key contribution of a national strategy for cyberspace will be to explicitly and clearly demonstrate how it makes possible the attainment of all the other strategies, most especially the National Security Strategy.[46] While the national strategy must embrace and understand cyberwarfare, in the process of doing so the national strategy must itself be reviewed and adapted.

Resources, 2011.
45 Kuehl, in Kramer, op. cit., p. 39.
46 Ibid.

2. The Difference between Information Warfare and Cyberwarfare

Information Warfare or Information Operations

In most countries *Cyberwar* is seen as a subsection of *Information Warfare*. Control of information has always been part of military operations. Information Warfare is an evolving construct with historical roots back to antiquity. The late 1970s saw the emergence of *Information Warfare* and *Command and Control Warfare* as US warfighting constructs integrating diverse capabilities. These, in turn, evolved into what the military now call *Information Operations*, recognizing the critical role of information as an element of national power through the full spectrum of peace, conflict, and war. Today, most armed forces view Information Operations as a *core military competency*. They see information as both a weapon and a target in warfare, and they think that information and knowledge superiority can win wars.

The value of information is enhanced by technology, such as networks, IT systems, and computer databases. These enable the armed forces to create a *higher level of shared situational awareness*; to *better synchronize command, control, and intelligence*; and to *translate information superiority into combat power*. With ever more weapons increasingly relying on data and technical information – such as smart munitions that use Global Positioning System (GPS) guidance – the armed forces expect information to become more directly relevant in warfare of the future. In a warfighting sense, sensor technologies have extended the engagement envelope; computers and communications technologies have led to an increase in the tempo of operations through the improved ability to coordinate actions;[47] and the integration of sensors into weapons has made these more precise and lethal. However, the real transformation has not been in sensors, weapons or IT *per se*, but in shifting the focus from the physical dimension to the information dimension. These values of information constitute the ground layer for *Information Operations*. They are also a prime example for the need for tight *governance* of this sector, clearly addressing what is permitted in situations that range from relative peace to all out nuclear war.

Information Warfare spans a much broader field of action than *Cyberwarfare*. For the conduct of Information Operations, major armed forces – though not all have

47 David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, London and New York, Frank Cass, 2004, pp. 91-92.

identical doctrines[48] – bank on five *core capabilities*: (1) Psychological Operations, (2) Military Deception, (3) Operations Security, (4) Computer Network Operations, and (5) Electronic Warfare. These capabilities are interdependent, and are increasingly integrated to achieve the desired effects.[49] Information Operations are defined as "the integrated employment of these core capabilities in concert with *specified* and *related* capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting the own."[50]

- *Psychological Operations* (PSYOP) are planned operations to convey selected information to targeted foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups and individuals.[51]
- *Military Deception* (MILDEC) guides an enemy into making mistakes by presenting false information, images, or statements. Deception is defined as "actions executed to deliberately mislead adversary military decision-makers with regard to friendly military capabilities, thereby causing the adversary to take – or fail to take – specific actions that will contribute to the success of friendly military operations."[52]
- *Operations Security* (OPSEC) is defined as a process of identifying information that is critical to friendly operations and which could enable adversaries to attack operational vulnerabilities.
- *Computer Network Operations* (CNO) include the capability to attack and disrupt computer networks, defend the own information and communications systems, and exploit enemy computer networks through intelligence collection, usually done through use of computer code and computer applications.
- *Electronic Warfare* (EW) is defined as any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy. High-power electromagnetic energy can be used as a tool to overload or disrupt the electrical circuitry of almost any equipment that uses transistors, micro-circuits, or metal wiring. Directed energy weapons amplify, or disrupt, the power of an electro-magnetic field by projecting enough energy to overheat and permanently damage circuitry, or jam, overpower, and misdirect the processing in computerized systems.[53]

In most armed forces, these 5 core capabilities are supported by 5 *Additional or Supporting Capabilities* that provide additional, less critical, operational effects: (1)

48 Neil Chuka, "Note to File – A Comparison of the Information Operations Doctrine of Canada, the United States, the United Kingdom, and NATO," *Canadian Army Journal*, Vol. 12, No. 2, Summer 2009. The author argues that although the IO doctrine of these countries has improved through the absorption of lessons from operations over the past decade and stronger conceptual thinking on the subject, the topic of IO continues to generate much debate and some confusion. However, it is possible, to a degree, to reconcile the new and emergent national doctrines and that of NATO.
49 NATO Allied Joint Publication (AJP) 3.10, *Allied Joint Doctrine for Information Operations*, 23 November 2009.
50 Ibid.
51 Ibid. In the US Armed Forces, PSYOPs have been renamed "Military Information Support Operations" (MISO) in late 2010.
52 Ibid. See, for example, the activities of General Patton's "Army Group" at the Pas de Calais, which was a decisive contribution to the Allied victory in Normandy in 1944.
53 See: JCS, Joint Publication 3-51 Joint Doctrine for Electronic Warfare, Washington D.C., GPO, 7 April 2000.

Counterintelligence, (2) Imagery/Combat Camera, (3) Physical Attack, (4) Physical Security, and (5) Information Assurance.

- *Counterintelligence* (CI) consists of the information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassination conducted by or on behalf of foreign governments or elements thereof, foreign organizations, persons, or international terrorist activities.[54]
- *Imagery/Combat Camera* consists of the acquisition and utilization of still and motion imagery in support of combat, information, humanitarian, Special Forces, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the military.[55]
- *Physical Attack* is actions taken to employ kinetic power or fires against physical information targets.
- *Physical Security* is that part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. In the communications security domain it is the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.
- *Information Assurance* (IA) consists of measures that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.[56]

The UK, the US, and some other armed forces,[57] despite different terminology and organization, use three additional or *Related Capabilities*: (1) Public Affairs, (2) Civil-Military Operations, and (3) Defense Support to Public Diplomacy, which have to contribute to the accomplishment of *Information Operations*. These often have regulatory, statutory, policy restrictions or limitations regarding their employment, which must be observed.

- *Public Affairs* (PA) are those public and command information, and community relations activities directed towards both the external and internal publics interested in what the armed forces do.
- *Civil-Military Operations* (CMO) are the activities of a commander that establish, maintain, influence, or exploit relations between the armed forces, governmental and non-governmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to facilitate

54 NATO Allied Joint Publication (AJP) 3.10, *Allied Joint Doctrine for Information Operations*, 23 November 2009.
55 Ibid.
56 Ibid.
57 *Campaign Execution. Joint Doctrine Publication 3-00,*(JDP 3-00), 3rd edition, Shrivenham, MoD, The Development, Concepts and Doctrine Centre, October 2009. And: US Department of Defense, *Joint Publications 3-13 Information Operations*, Washington D.C., 13 February 2006.

military operations, to consolidate and to achieve national operational objectives. CMO may include performance by military forces of activities and functions normally the responsibility of the local, regional, or national government. These activities may occur prior to, during, or subsequent to other military actions. They may also occur, if directed, in the absence of other military operations. CMO may be performed by designated civil affairs, by other military forces, or by a combination of civil affairs and other forces.

- *Defense Support to Public Diplomacy* (DSPD) consists of those activities and measures taken by components of the armed forces or the Ministry of Defense to support and facilitate public diplomacy efforts of the government.

Effects of *Information Operations* typically take longer to achieve, and are more difficult to measure than conventional operations. Therefore, a long-term commitment to effectively employ information to affect target behavior is critical. *Theater Security Cooperation Plans* are a vital part of this effort. Waiting until a crisis occurs and then initiating Information Operations against the crisis is an exercise in futility. Likewise, the idea of employing decisive combat operations in one area, while employing Information Operations in another as an economy of force measure, is a misapplication of Information Operations.

An appropriate understanding of the target's culture and norms is critical. The tendency to 'mirror' friendly cultural values and perspectives must be avoided at all costs. The preparation of products of Information Operations and an evaluation of their potential effectiveness must be done from the perspective of the recipient or target audience through their cultural lens. This is especially true during the planning, product review, and approval process when what may appear to be an unsophisticated and even amateurish looking product like TV or radio broadcast, messaging with mobile systems, leaflets, flyers, handbills, etc., may, in fact, be exactly the proper vehicle for conveying the desired message.

In all this, *intelligence* is the enabler to achieve military dominance in the framework of Information Operations. Intelligence coupled with Command and Control Warfare leads to *Information Dominance*, which may be defined as superiority in the generation, manipulation, and use of information sufficient to afford its possessors *military dominance*. It has three sources:

- *Command and Control* that permits everyone to know *where* they and their cohorts are in the battlespace, and enables them to execute operations *when* and *as quickly as* necessary.
- *Intelligence* that ranges from knowing the enemy's disposition to knowing the location of enemy assets in real-time with sufficient precision for precision kills.

- *Information Operations* that confound enemy information systems at various points – sensors, communications, processing, and command – while protecting one's own.[58]

The superiority is achieved by gaining superior intelligence and protecting information assets while fiercely degrading the enemy's information assets. The goal of such superiority is not the attrition of physical military assets or troops. It is the *attrition of the quality, speed, and utility of an adversary's decision making ability*.

Signals Intelligence (SIGINT) has always been intertwined with Information Operations because the first step is usually the same for both: to find a communications link and tap it, or to find a computer and hack it. Once in, one can either listen passively to learn the enemy's intentions, plans, and to anticipate his moves, or to actively insert own data, to deceive or jam his systems, and make him fall behind the own decision cycle. But there is no single approach that is always best.

Effective Information Operations leverage the power of information to compliment the other instruments of national power, resulting in the achievement of national objectives with less expenditure of blood and treasure. But the perennial question of Information Operations is: deny, deceive, destroy, or exploit? The best military answer is probably: to collect, analyze, and move the own information faster than the opponent to get an edge; to cut off the opponent from his own information sources, distort his processing, or prevent him from issuing orders and commands; and to fight the war inside weapon's circuits or inside the enemy commander's head.

Potentially, Information Operations are a potent weapon with a scope ranging from the enemy in the battlespace to the functioning of society. However, battlespace, fronts, and areas of responsibility can no longer be precisely defined. And the information revolution is weakening hierarchy and strengthening networks, which are lateral in nature. These networks are diluting the traditional hierarchical structure of the armed forces. At the same time, Information Operations are also a great leveler. Non-state actors can wage them with the same felicity as the established legitimate organs of the state.

When juxtaposed against traditional warfare, Information Operations show the following differences:[59] Traditional warfare has a geographically defined theater of war, while Information Operations know no geographical boundaries. And traditional warfare has a defined decision matrix: strategic, operational, and tactical, but there is no clear decision matrix in Information Operations. Moreover, in Information Operations, there is no clear distinction between war and peace, warlike and criminal, rogue and normal states. But most important: while it is possible to achieve conflict resolution with traditional warfare, this cannot be ensured with Information

58 Martin C. Libicki, "Information Dominance" in *Strategic Forum*, Nr. 132, Washington D.C., National Defense University, Institute for Strategic Studies, November 1997.
59 Yashwant Deva, "Information Warfare For The Theatre Commander", at: www.idsa.india-org/an-aug-7.html

Operations.[60] In other words: one can start a war with Information Operations, but not win it exclusively with Information Operations.

The claims made by enthusiasts of Information Warfare about successful applications of Information Operations seem often exaggerated or misleading.[61] When the theory is put to the test the results seem decidedly mixed. On the strategic level, the results are least convincing, judging from the state of the current War on Terror. But the actual practice of Information Warfare is also tricky to pull off at the operational-tactical level. There have been some real achievements nonetheless, alongside a growing realization that Information Warfare is a sword that cuts both ways in that the insurgents are also benefitting from the revolution. Despite their technological edge, Western armed forces are often at a disadvantage. In large part these problems have been due to the relative openness of the states concerned, the fact that they are expected to provide a greater amount of unbiased accurate information than undemocratic regimes, and also to the higher ethical expectations that they have to meet.[62]

The greatest problem with Information Warfare and Information Operations is the lack of, or chronically *insufficient, democratic governance, particularly regarding control, oversight, and transparency*. As with cyber security in general, oversight challenges are exacerbated by network complexity, technical and legal complexities, by the heterogeneity of actors involved, by mandate perceptions, and by the breaking of principal/agent bonds.[63] The pace with which security concerns are outstripping the ability of control, oversight, and regulatory bodies to hold the armed forces and the government accountable is particularly worrying when one considers the implications for the *rights to privacy*, to *freedom of expression* and of *association*. National legislation is of limited use in protecting users of a borderless communications tool. Thus, there is a need for a *common strategy and shared norms at the international level*. However, there remain the yet unanswered questions of what international approaches and norms are conceivable and needed, and of who should take the lead in this issue.

Information Operations may change the way in which governments and the armed forces conduct business. But cyberspace operations are not synonymous with Information Operations. Information Operation is a set of operations that can be performed in cyberspace and other domains. Operations in cyberspace can directly support Information Operations, and non-cyber based Information Operations can affect cyberspace operations. Activities in cyberspace can enable freedom of action for

60 The inability of Information Warfare to achieve conflict resolution leads to the definitive requirement and the primacy of traditional military forces to achieve a decision in war. Information Warfare, however, is most effective for neutralizing conventional military asymmetry. When thus employed, it becomes a potent weapon in the hands of the emerging foes of the 21st century.

61 See, for example, James Dao & Eric Schmitt, "Pentagon Readies Efforts to Sway Sentiments Abroad," *New York Times*, 19 February 2002, A1.

62 Tim Benbow, The Magic Bullet? Understanding the Revolution in Military Affairs, London, Brassey's, 2003.

63 See Benjamin S. Buckland, Fred Schreier & Theodor H. Winkler, *Democratic Governance Challenges of Cyber Security*, DCAF Horizon 2015 Working Paper No. 1, Geneva, Geneva Centre of the Democratic Control of Armed Forces, 2011.

activities in the other domains, and activities in the other domains can create effects in and through cyberspace.

Cyberwarfare

Cyberwar exists in the military and intelligence realm and refers to conducting military operations according to information-related principles. It means disrupting or destroying information and communications systems. It also means trying to know everything about an adversary while keeping the adversary from knowing much about oneself.[64] Cyberwar is a warlike conflict in virtual space with means of information and communication technology (ICT) and networks. As other forms of warfare, cyberwar aims at influencing the will and decision making capability of the enemy's political leadership and armed forces in the theater of *Computer Network Operations* (CNO).[65]

Three forms of Computer Network Operations can be distinguished: (1) *Computer Network Attack* – operations designed to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers or networks themselves; (2) *Computer Network Exploitation*, which means retrieving intelligence-grade data and information from enemy computers by ICT means; and (3) *Computer Network Defense*, which consists of all measures necessary to protect own ICT means and infrastructures against hostile Computer Network Attack and Computer Network Exploitation.[66] Thus conceptually, *Computer Network Operations cover only a narrower section of all cyber attacks*. But the potential for damage that cyberwar can inflict on national and economic security of a state could be large.

Computer Network Attack, or the deliberate paralyzation or destruction of enemy network capabilities, is only one of many instruments in the framework of military missions. While the importance of Computer Network Attack will certainly increase in the coming years, with regard to the state of developments in offensive cyberwar capabilities, there is still a lack of established knowledge about Computer Network Attack capabilities already available. There are very few case studies, and most information lies outside the public domain. And most organizations are still unsure about the state of their own cyber security. Thus, some of the estimates in this area seem exaggerated, particularly those linked to the expectation that the future will bring not only an arms race in cyberspace, but also *strategic cyberwars*. Conducting an 'information operation' of strategic significance would not be easy, but neither is it impossible. However, cyber alone is still unlikely to win wars. Given the intrinsic difficulties of operating surgically in cyberspace, and since it is, with few exceptions,

64 John Arquilla & David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy*, Vol. 12, 1993, p.146. Also: Arquilla & Ronfeldt, *Networks and Netwars*, Santa Monica, RAND Corporation, 2001.
65 NATO Allied Joint Publication (AJP) 3.10, *Allied Joint Doctrine for Information Operations*, 23 November 2009. Joint Publication 3-13 Information Operations, Joint Staff, Department of Defense, 13 February 2006.
66 Ibid.

still not possible today to conduct precisely targeted cyber attacks, great doubts remain as to whether strategic cyberwar is really feasible.[67]

One important aspect of this is that uncontrollable blowback effects in the highly networked virtual space constitute considerable risks for an attacking state. This factor is all the more relevant since the states that are most likely to develop the technological know-how for strategic cyberwar are also the most dependent on their own infrastructures, thus highly vulnerable in a cyberwar. Due to uncontrollable side-effects, a cyberwar would also undermine trust in cyberspace over the long term, with possible detrimental effects for the global economy, and thus for all parties involved. Strategic cyberwar, by itself, would probably annoy but not disarm an adversary. And any adversary that merits a strategic cyberwar campaign to be subdued also likely possesses the capability to strike back in ways that may be more than annoying. The fact remains that no one really knows how destructive a strategic cyber attack in a conflict conducted in the virtual realm would be. It may well be less decisive.

If a strategic cyber attack is less likely to be decisive, then cyberwarfare capabilities at the operational level for actions against military targets during a real war might become more important. Operational cyberwar may have the potential to contribute to warfare. How much is unknown and, to a large extent, still unknowable. Because a devastating cyber attack may facilitate or amplify military operations, and because an operational cyberwar capability seems relatively inexpensive, it may well be worth developing. But for operational cyberwar to work, its targets have to be accessible and offer vulnerabilities.[68] These vulnerabilities have to be exploited in ways the attacker finds useful, the result of which he can only assess if the effects can be monitored – what may still be an inconclusive endeavor.

Certainty in predicting the effects of operational cyber attacks is undermined by the same complexity that makes cyber attacks possible in the first place. Investigations may reveal that a particular system has a particular vulnerability. But predicting what an attack can do requires knowing how the system and its operators will respond to signs of dysfunction, and knowing the behavior of processes and systems associated with the system being attacked. Even then, operational cyberwar operations may rarely harm individuals directly, nor do they, with some exceptions, destroy equipment.[69] At best, such operations are more likely to confuse and frustrate operators of military systems, and then only temporarily because, due to the exponential innovation, even the best cyber attacks have a limited shelf life. Thus, cyberwar at the operational level may well only be a support function for other elements of warfare. "Attempting an operational cyberattack in the hopes that success will facilitate a combat operation

67 Myriam Dunn Cavelty,"Cyberwar: Concept, Status Quo, and Limitations," *CSS Analysis in Security Policy*, CSS ETH Zürich, No. 71, April 2010, p. 2.
68 Cyberdeterrence and Cyberwar, op. cit., p. xiv.
69 Ibid., pp. xiv-xv.

may be prudent; betting on the operation's success on a particular set of results may not be."[70]

Throughout all this, *cyber defense* remains the most important activity for the armed forces in cyberspace. The vast majority of attacks about which concern has been expressed apply only to Internet-connected computers. As a result, systems which are stand-alone or communicate over proprietary networks or are air-gapped from the Internet should be safe from these. Victims of cyber security lapses and cyber attacks include many civilian systems, and for this reason the value of a purely military approach to cyber security defense is limited. The armed forces have an important role in protecting their own systems and in developing potential offensive capabilities. Although most of what it takes to defend military networks can be learned from what it takes to defend civilian networks, the former differ from the latter in important ways. Hence, the armed forces must think hard as they craft their cyber defense goals, architectures, policies, strategies, and operations.

It should have become obvious by now that the debate on cyberwar is prone to speculation. Some proponents think that cyberwar will sooner or later replace kinetic war. More frequently, cyberwar is presented as a new kind of war that is cheaper, cleaner, with less or no bloodshed, and less risky for an attacker than other forms of armed conflict. This seems to make cyberwar attractive.

What are the elements that make cyberwar attractive?

- Cyberwar is cheaper since it does not require large numbers of troops and weapons.
- The entry costs are low: with a computer and Internet access anyone can engage in cyberwarfare.
- Cyberwar is easy to deliver by stealth via global connectivity from anywhere.
- Tools for attack are cheap and openly available on the Internet.
- The proliferation of such tools happens without any control.
- There are no technological, financial or legal hurdles to overcome against that proliferation.
- There is an advantage for the attacker who can profit from the latest and newest innovations.
- Cyberspace offers the attacker anonymity because it is so difficult to trace the origin of an attack.
- Cyberspace gives disproportionate power to small and otherwise relatively insignificant actors.

70 Ibid., p. xv.

- Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity, at least in the short term.
- Cyberwar may help to avoid the need to engage in combat operations and thus saves lives.
- Cyberwar leads to the ability to disrupt the adversary rather than destroy his forces.
- Blurred traditional boundaries: Cyberwarfare creates its own 'fog and friction of war.'
- Inherent in cyberwar are the difficulties of tactical warning and attack or damage assessments.
- Cyberwar enables actors to achieve political and strategic goals without the need for armed conflict.
- Cyberwar skips the battlefield. Systems that people rely upon, from banks, the electric power grid to air defense radars, are accessible worldwide from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defenses.
- Cyberwar happens at almost the speed of light. As photons of attack packets stream down fiber-optic cables, the time between the launch of an attack and its effects is barely measurable, thus creating more risks for decision makers, particularly in a crisis.
- The victim of an attack has to invest considerable resources into neutralizing the threat, which requires teams of dedicated software and hardware experts with specific skill sets. Such persons are difficult to recruit and to retain as private industry offers more attractive terms for their talent.
- The vulnerabilities of countries increasingly dependent on complex, interconnected, and networked information systems increase over time, thus providing adversaries with a target rich environment.

For many, the term cyberwar conjures up images of deadly, malicious programs causing computers to freeze, weapon systems to fail, thwarting vaunted technological prowess for a bloodless conquest. This picture, in which cyberwar is isolated from broader conflict, operates in a different realm from traditional warfare. While such a scenario is not completely beyond the realm of possibility, offers a bloodless alternative to the dangers and costs of modern warfare, and thus seems attractive, it is not very likely. A pure cyberwar is an event with the characteristics of conventional war but fought exclusively in cyberspace. *It is unlikely that there will ever be a pure cyberwar fought exclusively with cyber weapons.*

Future wars and the skirmishes that precede them will involve a mixture of conventional or kinetic weapons with cyber weaponry acting as a disrupter or force multiplier.[71] The reasons are: (1) many critical computer systems are protected against

71 Peter Sommer & Ian Brown, "Reducing Systemic Cybersecurity Risks," *OECD,* OECD/IFP Project on "Future Global Shocks," 14 January 2011, pp. 6 and 13.

known exploits and malware so that designers of new cyber weapons have first to identify new vulnerabilities and exploits. (2) The effects of cyber attacks are difficult to predict – they may be less powerful than hoped for, but may also have more extensive outcomes arising from the interconnectedness of systems, resulting in unwanted damage to perpetrators and their allies. And (3) there is no strategic reason why an aggressor would limit himself to only one class of weaponry. Hence, cyberwarfare is prone to have real physical consequences.

Like other elements of the modern military, cyber forces are most likely to be integrated into an overall battle strategy as part of a *combined arms campaign*. Cyber weapons will be used individually, in combination, and also blended simultaneously with conventional kinetic weapons as force multipliers.[72] Computer technology differs from other military assets, however, in that it is an integral component of all other assets in modern armed forces. From this perspective, it is the one critical component upon which many modern militaries depend, a dependence that is not lost on potential enemies.

Countries around the world are developing and implementing cyber strategies designed to impact an enemy's command and control structure, logistics, transportation, early warning, and other critical military functions. In addition, nations are increasingly aware that the use of cyber strategies can be a major force multiplier and equalizer. Smaller countries that could never compete in a conventional military sense with their larger neighbors can develop a capability that gives them a strategic advantage if properly utilized. The entry costs for conducting cyberwar are rather modest. Not surprisingly, therefore, countries that are not so dependent on high technology within their military establishment consider such dependence a potential 'Achilles heel' of their enemies.

Advanced, post-industrial societies and economies are critically dependent on interlinked computer information and communication systems. Sophistication has itself become a form of vulnerability for enemies to exploit. Disruption of civilian infrastructures is an attractive option for countries and non-state actors that want to engage in *asymmetric warfare*, and lack the capacity to compete on the traditional battlefield.

But war is typically defined as the use of force, or violence, by a nation-state to compel another to fulfill its will. Military conflict is a way for nation-states to achieve their political objectives when other means, such as diplomacy, are not working or are less expedient than violence. The use of force, however, may be less obvious in a new battlespace made up of bits and bytes, where the borders between countries blur, the weapons are much more difficult to detect, and the soldiers can easily be disguised as civilians. It is difficult to envision cyberwarfare because history lacks experience in

72 Ibid., p. 6.

cyber conflict. There is no past to learn from, much less envision how a national-level cyber conflict would be fought.

Multiplying and complicating the uncertainties about cyberwar are the problems that derive from the nature of cyberspace, the steadily growing vulnerabilities that enable cyber attacks, plus the major issues, ambiguities and additional problems of cyberwarfare. These then set the stage for showing how a modern war may be conducted – a clue of cyberwar to come – and in which ways cyberwar may be different from the other warfighting domains.

3. Understanding the Threats in Cyberspace

Cyberspace is a borderless 'global commons' that all actors, including states, share. From personal use to business platforms and military applications, the reliance on cyberspace is only accelerating. Since the beginning of the 21st century, the ability to leverage cyberspace has become the most important source of power. Due to the amazing proliferation of ICT systems into all aspects of life, the importance of information for political matters has increased. And with it the ability to master the generation, management, use, and manipulation of information has become a highly desired power resource in international relations.

Although cyberspace is agnostic to politics and ideology, state and non-state actors can use this power to achieve objectives in cyberspace and the physical world. Low cost, high potential impact and general lack of transparency make cyberpower attractive to both powerful and less powerful actors. The former can combine cyberpower with existing military capabilities, economic assets, and soft-power means. Less powerful actors can gain asymmetrically in cyberspace by inflicting damage on vulnerable targets. The virtual terrain of cyberspace is said to favor the offense because cyber attacks are inexpensive and conducting them rarely has consequences. These two facts are a major reason why cyber attacks have become ubiquitous, increasing in scope, and at a scale far greater than national resources to respond and defend can handle.

Along with many other countries, the US, for example, is under constant assault in cyberspace and currently witnessing some 1.8 billion cyber attacks alone on the IT systems of Congress and executive branch agencies each month.[73] Such series of incidents have led to the term *Advanced Persistent Threats*, which is commonly used to refer to cyber threats, in particular that of Internet enabled espionage, but is primarily used in reference to a long-term pattern of targeted sophisticated hacking attacks aimed at governments by well-resourced state actors, or agents affiliated with nation-states.[74] Such attacks have targeted governments around the world, global oil, energy, and petrochemical companies, the mining sector, military contractors, the science and technology sector, critical infrastructure, and many additional sectors. Ever more they are also targeting high-tech companies that could enable future targeting.

73 Senator Susan Collins, "How to Make Internet More Secure'", *Politico*, 7 March 2011, and Principal Deputy Under Secretary of Defense for Policy James Miller in testimony before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, 10 February 2011. In February 2011, US Deputy Secretary of Defense said that more than 100 foreign intelligence agencies have tried to breach DoD computer networks, and that one was successful in breaching networks containing classified information. See: William J. Lynn, III, Remarks on Cyber at the RSA Conference, 15 February 2011.

74 See: Advanced Persistent Threats: A Decade in Review, Command Five Pty Ltd, June 2011.

The Problems that derive from the Nature of Cyberspace

Cyberspace is a unique domain in that it does not itself occupy physical space. It does, however, depend on physical nodes, servers, and terminals that are located in nations that exert control and sometimes ownership. The public good that travels the information highway is manmade and hard to categorize or locate.[75] Until recently, most hackers were after the information that constitutes the payload of cyberspace, rather than its infrastructure. This, however, is changing. The infrastructure and information base of cyberspace is almost entirely in the hands of private and commercial enterprises, rather than governments or the military. To complicate things further, unlike the other domains, cyberspace does not depend primarily on state power for security; the great majority of networks are private and competitive in nature. In this environment, providers have been quite resistant to regulation and security, preferring self-regulation and less assurance rather than accept limitations and higher costs that increase safety and reliability.[76]

Threats, vulnerabilities, and risks have grown exponentially with the proliferation of use and dependence on cyberspace infrastructure. The electronic dependence of modern civilization on physical infrastructure, data and information, and the resulting critical infrastructure functionality requires a seamless Internet environment. Consequently, cyberspace has become a warfighting domain with the inherent potential to destroy or render useless logical, physical, technical, and virtual infrastructure, and to damage critical national capabilities, such as economic, government, military, educational, health, social, and other capabilities.

Threats within and from cyberspace are disparate, diffuse, and some may also be disproportionate in the harm they could cause. However, threats to cyber security are not synonymous with threats to national security. The majority of cyber threats do not threaten national security. Threats, dangers, and risks arising from action in cyberspace have three general characteristics: (1) they are *broad*; (2) they are *embedded*; and (3) they are *diverse.*

(1) The nature of the threat in cyberspace is *as broad as cyberspace itself*. Any aspect of the world that is dependent on the cyber domain is potentially at risk. Hence, of concern are adverse actions that threaten the integrity and security of critical national infrastructures; destabilize the financial system; enable access to nationally significant classified information or commercially exploitable trade secrets; or undermine in

75 For example, a discrete transmission may start via a cell tower (USA terrestrial), be converted to trans-Atlantic fiber-optic signal (maritime), then be relayed via microwave tower (EU terrestrial) to a French satellite in space, ending as a SATCOM signal to a commercial Korean ship at sea. Transmissions like this occur millions of times each day, illustrating not only the ubiquitous nature of cyberspace, but also the complexity of these elaborate systems.

76 *The Global Commons Project*, Brussels, NATO, SACT, 18 November 2010, p. 9.

any other significant way the ability to rely upon information and communications technology (ICT) systems for relevant national security objectives.

(2) Threats to the integrity of information and security in cyberspace are *deeply embedded* in the cyber domain. They arise from vulnerabilities inherent, or from malware[77] placed, in complex software operating systems, and from malicious hardware. They are embedded because the threat is an intrinsic feature of cyberspace, which may never be fully eradicated.

(3) The threat in cyberspace is *as diverse as the plethora of potentially hostile actors* who exploit these vulnerabilities, the actions they take, and the targets they attack.[78] There are more than nation-state actors: among the great diversity of actors are also ideological and political extremists, terrorist organizations, well-organized criminal gangs, and all sorts of state-sponsored, mercenary or individual hackers. Each poses a distinct threat, requiring a differentiated response.

Rosenberg, the rapporteur of a workshop on *national security threats in cyberspace*, argues that the nature of cyberspace makes threats from that domain fundamentally different from those existing in the 'real world.'[79] At least nine factors contribute to this difference:

- The span of cyberspace is global, creating conflicting and overlapping realms of control by nation-state actors with differing legal and cultural approaches and distinct strategic interests.
- The world has become so dependent upon the cyber domain that disassociation is impossible. Cyber globalization cannot be undone; neither can our reliance on cyberspace for national security functions.
- The now globalized production of both cyber hardware and software in many different countries makes it virtually impossible to provide reliable supply chain assurance or good product assurance.
- The scalability of the cyber domain makes it qualitatively different. We do not deal with kinetic force of physically limited range, but with mechanism by which operations on a global scale are controlled.
- Operations within the domain are controlled by a small number of people. Everyday users cannot modify or control software and hardware they use, thus only few have control of the cyber universe.
- Because of the interconnectedness and interoperability of cyberspace, no locus of positive control is feasible. Efforts to mitigate the threat, if possible at all, will require close international cooperation.

77 Malware = malicious software and hardware.
78 Paul Cornish, David Livingston, Dave Clemente & Claire Yorke, *On Cyber Warfare*, London, A Chatham House Report, The Royal Institute of International Affairs, November 2010, p. 5.
79 *National Security Threats in Cyberspace*, a Workshop of the National Strategy Forum, Part of the McCormick Foundation Conference Series, September 2009.

- Changes in the cyber domain occur ever more rapidly. The interconnectedness of cyberspace enhances this consequence of acceleration. But each change creates again a new cycle of vulnerabilities.
- The distribution of cyber assets spans all types of organizations, from closed to government controlled systems to those operated by the public, each with different resources, capabilities, and concerns.
- The nature of cyberspace is such that the technical capacity to attribute actions to the responsible actor with a sufficient degree of confidence is still lacking. Hence, anonymity is easily achievable.

Insecurity in cyberspace is caused by three conditions that distinguish it from other domains of activity and fundamentally shape the nature of cyber threats: (1) the *architecture of the Internet*; (2) *exponential innovation*, and (3) the Internet's widespread *integration into the economy, society, government, and the armed forces.*

The Internet Architecture

The architecture of the Internet enables nearly instant movement of information globally at low cost. The Internet has been designed to connect multiple networks, computational facilities, and institutions seamlessly and reliably. Yet it was hard to foresee the vulnerabilities that would emerge as the Internet proliferated from a Pentagon-sponsored research project into a global communications network that pervades modern life. It is the Internet's openness that carries downsides in that it makes it easier to attack applications and operating systems that are not adequately defended. Designed as a decentralized system, the users of the Internet are functionally anonymous, generating information that travels in undifferen-tiated packets that can be encrypted to disguise the origin. This anonymity provided by the architecture leads to an attribution challenge that renders most cyber attacks untraceable. Establishing, let alone authenticating identity is challenging if it is possible at all.

The attribution problem empowers both strong and weak actors who benefit from having their identities disguised since the online anonymity makes identifying and punishing cyber attackers extremely difficult. Interlinked individuals or groups operating from globally dispersed locales can, with no warning and only milliseconds between decision and impact, attack scores of digital targets simultaneously without revealing their identities. Those who try to locate attackers often find themselves chasing ghosts or ending up at hacked botnets when the attacks originate from a multitude of computers and servers in multiple countries.

Exponential Innovation

Innovation has expanded the availability, use, and functionality of the Internet at an amazing rate. Today, there are more than 2 billion Internet users globally, a vast increase from the 361 million users online in 2000.[80] The spread of mobile devices, which surpassed 5 billion subscriptions worldwide in 2010, gives an even greater number of people access to the Internet as mobile devices continue to offer better functionality, particularly for the developing world.[81] Ever-growing processor speeds and improved algorithms continue to facilitate greater reliance on the Internet, which adds trillions of dollars to the global economy each year. Global e-commerce activity totaled 10 trillion dollars in 2010, and is expected to amount to 24 trillion dollars by 2020.[82]

Thus, continued innovation offers increasing opportunities for productive use of the Internet. However, it also aids all those with malicious intent by providing more targets and tools for attack. Cyber security is time consuming and expensive. Moreover, the pressure security companies feel to unveil innovative products quickly leads to introduction of technologies that are less secure than they would be if more time were devoted for bolstering their security. McAfee identified more than 20 million new pieces of malware in 2010, or an average of nearly 55,000 per day, each one representing a new weapon for attackers. It also reported increases in targeted attacks, in their sophistication, and in the number of attacks on the new classes of devices in 2010.[83]

Widespread Integration

The architecture has facilitated Internet's integration into almost every aspect of modern life. While this has yielded most remarkable advances in productivity and efficiency, it has also created vulnerabilities that exceed understanding of the potential consequences. The integrated nature of cyberspace increases the chances that any disruption will ripple far beyond the original incident. Network disruptions resulting from cyber attacks can lead to damage and even potential loss of life through cascading effects on critical systems and infrastructure.

Three Major Information Infrastructures

The widespread integration has brought about *three major information infrastructures*. The first is the *National Information Infrastructure*, which is the key

80 McAfee, A Good Decade for Cybercrime, January 2011, p. 4.
81 International Telecommunication Union (ITU), "Key Global Telecom Indicators for the World Telecommunication Service Sector," Geneva, 21 October 2010.
82 Robert D. Atkinson et. al., *The Internet Economy 25 Years After, Com: Transforming Commerce & Life*, Washington D.C., The Information Technology and Innovation Foundation, March 2010, p. 43.
83 McAfee, McAfee Threat Report: Fourth Quarter 2010, February 2011, p. 7.

network element within a country that enables its information society to function, and determines the efficiency of its functionality. The second is the *Defense Information Infrastructure*, which serves a country's defense organization, both military and civilian. And the third is the *Global Information Infrastructure*, which provides the international connectivity to the National Information Infrastructure. In defense terms, these infrastructures largely determine the functional efficiency of a country's warfare capability. And in both defense and broader national security terms, they provide a pathway to cyberwar and information operations.

The *National Information Infrastructure* is the nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, television, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the National Information Infrastructure.[84]

The National Information Infrastructure also comprises the *Critical Infrastructure*, which is deemed critical because its incapacitation or destruction would have a debilitating impact on the national security, and the economic and social welfare of the nation. These infrastructures include key sectors such as information and telecommunications, energy, banking and financial services, general utilities, transport and distribution, emergency rescue services, and public administration, plus lists of additional elements that vary across countries and over time.[85]

Most of these infrastructures rely on Supervisory Control and Data Acquisition (SCADA) and other software-based industrial control systems for their smooth, reliable, and continuous operation. With these systems, service providers use cyberspace to communicate and control sensitive processes, such as the opening and closing of valves; regulating temperatures; controlling the flow of oil, gas, water and waste water; balancing levels of chlorination in water; regulating power generation plants as well as power supply via the electric grid; controlling ground transportation and air traffic, etc. If disrupted by a cyber attack, even for only a short period of time, the effects could interrupt supply chains, damage control facilities' operations remotely, create scarcities or emergencies, destroy property, and potentially harm or even kill innocent civilians. As attacks grow in magnitude and intensity, the risks of incidents with cascading social effects increase.

84 Dictionary of Military and Associated Terms, US Department of Defense, 2005.
85 Critical infrastructures in the US include in alphabetical order: Agriculture & Food; Banking & Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Healthcare & Public Health; National Monuments & Icons; Nuclear Reactors, Materials & Waste; Postal & Shipping; Transportation Systems; and Water.

Critical Infrastructures are generally regarded as inherently insecure. Most of the components are developed in the private sector, where the pressure of competition means security does not drive system design. Computer and network vulnerabilities are therefore to be expected, and these lead to infrastructures with in-built instabilities and critical points of failure.[86] A relatively small attack can achieve a great impact, thus offering a 'force-multiplier' effect to those carrying out infrastructure attacks.[87]

The *Defense Information Infrastructure* is the shared or interconnected system of telecommunications networks, computers, databases and electronic systems serving the Ministry of Defense's national and global information needs. It is a subset of and comprises the National Information Infrastructure, and includes the people who manage and serve the infrastructure, and the information itself. It includes information infrastructure which is not owned, controlled, managed or administered by the Ministry of Defense.[88]

The *Global Information Infrastructure* is the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact discs, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, television, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the Global Information Infrastructure.[89] It is not identical with the Internet, which is the global network of networks. Other dedicated networks that are stand-alone and not networked, are not part of the Internet.

Key Characteristics of Information Infrastructure

A number of key characteristics of these information infrastructures flow from above definitions[90] that are important to targeting considerations. These include *components, connectivity, bandwidth, functional interdependence*, and *ownership and control.*

86 Michael Näf, "Ubiquitous Insecurity? How to 'Hack' IT Systems," *Information & Security: An International Journal*, No. 7, 2001, pp. 104-118.
87 Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, *Threat Analysis No. TA03-001*, 12 March 2003.
88 Australian Defence Doctrine Publication (ADDP) 3-13, *Information Operations*, 2006.
89 Department of Defense Dictionary of Military and Associated Terms, Washington D.C., Joint Publication 1-02, 17 October 2007.
90 The above definitions vary between authorities and authors within and between countries, but all boil down to the same essential characteristics.

Components: The National, Defense and Global Information Infrastructures comprise five distinct interdependent components. The first four are explicit in the definition while the 5th is more implicit:

- The *hardware* – the computers; sensors; physical transmission components such as cables; radio and wireless; satellites and transmission towers;
- The *software* applications – processes; protocols; encryption; and firewalls;
- The *information* itself – the databases; and information in transmission including voice, facsimile, text messages, imagery, or information in other forms;
- The *people* who operate and maintain the infrastructures; and
- *Power supply*, without which hardware and software cannot function and information cannot be transmitted or accessed. While integrated backup power supply could be considered part of the hardware component, mains supply is not. Most uninterrupted power supply systems (UPS) have only a limited capability in terms of both duration and capacity, and mains supply remains critical for full and enduring functionality.

Connectivity: The very broad, virtually instantaneous and seamless connectivity and reach across the various domestic and international information domains of the National, Defense, and Global Information Infrastructure networks is a characteristic that also contributes significantly to infrastructure functional efficiency. Users of these infrastructures have adjusted business or other practices accordingly. Real-time communications are critical in many areas of business and government. This real-time dependence also applies to many emergency services and especially to defense functions across the whole C4ISTAR spectrum, including sensor to weapon configurations during combat operations. Disruption to connectivity, even for relatively brief periods of time, could have a major impact on outcomes.

Bandwidth: Is constantly increasing across all 3 infrastructures, particularly over data networks in parallel with technology improvements. Client demand has not only kept pace with bandwidth availability, but has outstripped it. Broad bandwidth allows access to vast quantities of information in a very short space of time. In a defense context, in particular, it is an important feature of real-time delivery of surveillance and reconnaissance imagery, and the immediate 'pull-down' accessibility for deployed combat forces to their headquarters' intelligence databases.

Functional interdependence: Between information and its supporting systems, and between the supporting systems themselves, is a major factor related to the functional efficiency and security of any information infrastructure. The more complex the system or network, the greater is that interdependence. Failure in whole or by a part of any component of an interdependent system can impact on the functionality of another part or, potentially, on the whole system. Depending on the type of system affected and the scale of the failure, the cascade effect can have significant implications for specific or general services and capabilities, and ultimately affect how people live

and behave. In military terms especially, this cascade 'knock-on' effects fits the classic mould of targeting outcomes in 'effect-based' operations.[91]

Ownership and control: Ownership of the networks varies between the government and private sector, depending on the country, and what part of the network within that country is involved. In most countries, the major telecommunications service providers are privately owned. And in the globalized world, those services may be owned or partly owned by foreign private corporations. The percentage of the Defense Information Infrastructure that is made up of and dependent on the National, and the Global Information Infrastructure also varies from country to country, but is generally assessed in most advanced countries as 80 to more than 90 percent. Thus, only 10 to 20 percent of the Defense Information Infrastructure in these countries is owned, controlled, managed or administered by their defense organization. Moreover, the infrastructure that they do own, control, and manage exists primarily at the tactical level only. Apart from the US, there are few countries that can afford to have their own fully independent strategic and operational broadband communications systems. One important conclusion is, therefore, that a significant proportion of any defense organization's C4STARS capability is outside its total control, and may well be foreign owned or under *de facto* foreign control. The diverse and distributed ownership of infrastructure presents enormous security challenges because it is impossible to homogenize policies and best practices.

The Challenges of Situational Awareness

In *The Art of War* Sun Tzu said "All warfare is based on deception … Know your enemy and know yourself and you can fight a hundred battles without disaster … If you know neither the enemy nor yourself, you will succumb in every battle."[92] But in cyberspace, it is particularly difficult to know the enemy because many of the challenges of traditional warfare are magnified in cyberspace. Chief among these is the challenge of *situational awareness*,[93] which is defined as "the continuous extraction of environmental information, the integration of this information with previous knowledge to form a coherent mental picture, and the use of that picture in directing further perception and anticipating future event."[94] Having complete, accurate and up-to-the-minute situational awareness is essential where technological and situational complexities on the human decision maker are a concern. Situational awareness has been recognized as a critical, yet often elusive, foundation for successful decision making across a broad range of complex and dynamic systems, including aviation

91 Is a process for obtaining a desired strategic outcome or 'effect' on the enemy, through the synergistic, multiplicative, and cumulative application of the full range of military and non-military capabilities at the tactical, operational, and strategic levels. Joint Forces Command, Glossary.
92 Sun Tzu, *The Art of War*, translated by Lionel Giles, at: The Internet Classics Archive, http://classics.mil.edu
93 Mike Lloyd, "The silent infiltrator," *Armed Forces Journal*, June 2010, at: http://www.afji.com/2010/06/4612622
94 Dominguez, Vidulich, Vogel & McMillan, *Situation awareness: Papers and annotated bibliography*, Armstrong Laboratory, Human System Center, ref. AL/CF-TR-1994-0085. Also *Situation awareness*, Wikipedia, at: http://en.wikipedia.org/wiki/Situation_awareness

and air-traffic control, emergency response, military command and control operations, offshore oil and nuclear power plant management, etc.

Cyberspace is a vast, complex and rapidly changing battlespace. The key to prevailing in a hostile cyber-space environment may lie in the ability to generate a comprehensive picture of that environment.[95] In the kinetic realm, the *fog of war* is a term derived from Clausewitz referring to uncertain knowledge about the adversary, and the position and activities of the own forces in the midst of an operation. While situational awareness is a major challenge already in traditional warfare, the *fog of cyberwar* may well be so thick that it could become the primary impediment to victory. Thus, developing the techniques and tools for cyber situational awareness would be paramount to achieving strategic, operational, or tactical advantage in this novel domain.

A fundamental obstacle in the cyber domain is the difficulty of determining the *own defensive posture* in the continuous process of safeguarding computers and networks: the continuum of *protect*, *detect*, *respond*, and *recover* that helps organizations to anticipate dangers, neutralize, limit the impact of those dangers, and react quickly and effectively in the event of an attack. Two aspects make situational awareness difficult in cyberspace: its *vast complexity* and its *incredible rate of change*. Traditional manual techniques for gaining situational awareness of the own defensive posture are quickly over-whelmed by these effects. The complexity of cyberspace stems from several factors. One is that today's ICT systems, based on distributed computing concepts, are so intricate. Functionality is spread across a multitude of computer systems that are tied together in global networks. Every element in these archi-tectures must be assessed, monitored, and protected: applications, databases, webservers, host computers, networking gear, etc. Even basic knowledge such as the number of ICT systems deployed and how they are connected can be a challenge for those attempting to achieve situational awareness in these networks.

Redundancy adds to the complexity. Military ICT systems are mostly built to insure availability even if individual components fail. To achieve a high degree of availability, they have built-in redundancy, offering backup systems and failover network paths. While redundancy is important for availability, it also greatly enhances the complexity of security. A typical network offers many possible paths to connect a user to an application. If any single path is available, the application is available. But vulnerabilities in any of these paths also enable security breaches. "While availability is a function of the strongest link in the chain, security is a function of the weakest."[96]

In addition to the complexity of cyberspace, situational awareness is made very challenging because of constant and dynamic change. Even if the own position is accurately defined and assessed at a given time, the assessment can be quickly out of

95 Robert K. Ackerman, "Network Situational Awareness Looms Large in Cyberspace," *Signal Magazine*, May 2010.
96 "The silent infiltrator," op. cit.

date because unrelenting change is an inherent characteristic of cyberspace. There are different aspects of change. One is in the ICT systems themselves, which are constantly deployed, decommissioned, integrated, and updated with new software and hardware. This sort of change is fundamental to the power of distributed computing. It enables great flexibility, rapid reaction time, and rapid innovation, all of which are essential to effective and efficient mission support. While steps can be taken to manage this change, there are limits to how much control can be imposed without compromising the advantages that cyberspace offers.

The Challenges of Protection against Security Breaches

A more important aspect of change is mostly out of control for the forces deployed: *the changing nature of vulnerabilities and threats*. There are many thousands of known vulnerabilities in IT systems, and new ones are discovered every day. The cyber security company Sophos analyzed 95,000 malware pieces in its labs every day in 2010, nearly doubling the number of malware they tracked in 2009. This accounts for one unique file every 0.9 seconds, 24 hours per day, each day of the year. The threat experts of the company see 30,000 new malicious URLs each day – 70 percent of which are legitimate websites that were hacked.[97] This is a clear sign that the malware threat continues to grow at an alarming rate.[98]

And opponents are constantly developing new methods and mechanisms to exploit these vulnerabilities. The problem is that it is cheap to develop a cyber weapon, while defending against it costs a lot. Some of the most complex, commercially available defense software now has between 5 and 10 million lines of code. In contrast, the average malware has stayed more or less constant over the last decade at 170 lines of code.[99] Thus, what was considered impregnable yesterday may show subtle weaknesses today, and may likely be compromised tomorrow. Thus, cyber defenses must be in a constant state of flux to accommodate both changing ICT systems and changing threats. But because the traditional manual techniques are failing to provide the security needed, automated systems are required that continuously monitor security postures, and provide risk-based situational awareness to decision makers. Hence, to protect their vital assets, the armed forces must meet the threats proactively with a system-wide defensive approach employing superior technology.[100]

97 InfoWorld Data Management Alert, San Francisco, *InfoWorld Inc.*, 24 March 2011. A URL is a Uniform Resource Locator (URL) and a subset of the Uniform Resource Identifier (URI) that specifies where an identified resource is available and the mechanism for retrieving it. ...
98 *Sophos security threat report 2011*, Sophos Ltd. and Sophos Group, February 2011, p. 4.
99 William Lynn, "Cyber Warfare Unavoidable in the Near Future," *The New New Internet,* the Cyber Frontier, 9 April 2011, at: http://www.thenewnewinternet.com/2011/10/04/William-lynn-cyber-warfare-unavoidable-in-the-near-future/
100 Melissa E. Hathaway, *Strategic Advantage: Why America Should Care About Cybersecurity*, Cambridge, Belfer Center for Science and International Affairs, Harvard Kennedy School, October 2009.

There are three classes of systems for defensive posture management, which can be classified by when they operate in relation to an attack: *after*, *during*, and *before*. Forensic systems help organizations investigate attacks *after* they have occurred to understand both their impact and their root causes. The core of these solutions is historical logs that record activity on each aspect of the infrastructure, from software to network devices. These logs can be analyzed manually to determine the sequence of events that have led to an intrusion or disruption. But the volume and complexity of this data is enormous. Thus, organizations now implement log management systems that collect, store, and analyze that data auto-matically. These systems correlate information from multiple systems to identify patterns, and put together a timeline of the incident. Using this information, the armed forces can remediate the problems that enabled the breach, and identify, evaluate, and address the damage done.[101]

The next better class of situational awareness systems helps the forces to detect and respond to an *attack in progress*. Such systems rely on sensors and intrusion detection systems deployed throughout the infra-structure to identify suspicious behavior, deviation from normalcy, and to raise alarms. An alarm can be analyzed manually, but an intrusion may raise too many such alarms as it moves through the infra-structure. And sorting out a true attack from the normal background noise of false alarms is an extremely complex endeavor. To address this, systems for security information and event management can be deployed which collect events, analyze them on an infrastructure-wide basis, and identify where an exploit is occurring at that point in time. With information thus gained, incident response teams can take action to prevent the intrusion from progressing any further.

The last and most important class of situational awareness systems is designed to operate *before* an attack begins, focusing on stopping attackers before they gain entry.[102] For this, defenses that block malicious software and unauthorized access are crucial. In addition, baseline configuration standards must be established and monitored to prevent deviation and noncompliance that can create vulnerabilities in the system. This requires systems which identify vulnerabilities, misconfigurations, and other risks in the infrastructure. Like forensic and event-based systems, these systems are equipped with components that assess individual devices such as vulnerability scanners.[103] Scanners and similar tools identify vast numbers of potential device issues, most of which are effectively mitigated by the defense-in-depth architectures of security. Security posture management solutions can be deployed that analyze the configurations and vulnerabilities of the various devices and hosts throughout the infrastructure, correlate them together, and identify the system-wide security issues that exist in the infrastructure. Using this information, those responsible for security

101 "The silent infiltrator," op. cit.
102 See: "Attack Prevention," M86 Security, at: http://www.m86security.com/resources/attack-prevention.asp
103 David Shelly, Randy Marchany & Joseph Tront, *Losing the Gap: Analyzing the Limitations of Web Application Vulnerability Scanners*, The OWASP Foundation, Virginia Polytechnic Institute and State University, 8 November 2010.

can then prioritize and address problems to remediate *before they are exploited* by adversaries.[104]

As always with computer security, there are two things to remember. First, that security depends on a combination of technology and policy; and second, that no system is ever totally secure. It is safer to assume that there will be breaches, and work out how to minimize the damage. That means storing, and moving around, as little data as possible; anonymizing records and linking to personal details stored in a separate database; using encryption to protect data in transit, and using Intranet solutions where possible.

Security architectures are built on the premise that successful attacks will occur. The rapidly changing and inherently open nature of cyberspace makes this inevitable. The ultimate protection against attacks is to air-gap critical systems from sources that cannot be trusted. But this comes with high costs in timeliness, flexibility, and functionality. To retain functionality while still offering robust security, cyber defenses are built in layers. Even if an attack penetrates the first layer, deeper layers of defenses are designed to contain the attack before it can reach critical systems. Much like physical defenses, layered defenses can provide incident response teams the time to shut down an attack before it causes unacceptable damage.

Effective situational awareness systems are an integral part of layered defenses. But every layer increases the complexity of the defense exponentially, so maintaining multiple layers between changing threats and changing ICT systems requires automated assessment capabilities. Event management systems to respond to attacks in progress are now becoming more common. But security posture management systems to prevent attacks in the first place are only about beginning to emerge. In this domain, the US armed forces seem to be in the lead due to massive research and development investments made by the Defense Advanced Research Projects Agency (DARPA), founded in response to the surprise Sputnik launch in 1958, and which fathered the Internet.

With effective contingency plans, processes, tools, and competencies in place for the event of an intrusion or disruption, incident response teams can react swiftly to contain and eradicate the threat. With the help of timely incident reports, they can assess any system damage or data loss and move quickly to resume operations. And with recovery procedures and workarounds already thought out, incident response teams can quickly move forward after an attack to recover lost data or configuration information. They then can restore systems and tests to help ensure that all components are again in compliance, and thus reestablish mission assurance and confidence. A continuing review of security audit files provides the opportunity to learn from the

104 "The silent infiltrator," op. cit.

incident, so the lessons can be applied to help to improve existing security provisions and prevent recurrence.[105]

Supply Chain and Vendor Access, Remote Access, Proximity Access, and Insider Access

Ultimately, the current trends towards digitization, automation, and interoperability need not be mutually exclusive of security. But the cyber security challenge can only be addressed effectively by fully under-standing the wide range of the real *threat vectors* existing, which fall into four broad categories: *supply chain and vendor access*, *remote access*, *proximity access*, and *insider access* to ICT systems.

With respect to the *supply chain*, it is widely accepted that the global economy has given nations the ability to compete and purchase services in an expanding market that has driven down prices and promoted rapid invention and innovation. But the global supply chain also has substantially increased our vulnerabilities to adversarial manipulation of hardware and software. Computers or the architecture they ride on can be poisoned with dormant capabilities that can be awakened by adversaries. Even if our ICT systems come out of the factory in pristine condition, they can be manipulated by the delivery service, the wholesaler, the retailer, the installer, the repairman, or through the downloadable firmware update or patch. *Supply chain* and *vendor operations* are very difficult to monitor. Even without a global supply chain, these same exploits could be introduced domestically by organized crime, disgruntled employees, or foreign intelligence services.

Remote access by network intrusion or hacking is another avenue of attack. We see most of this threat vector either because it is the greatest problem or because it is the most easily tracked. Systems administrators typically are overwhelmed by the quantity of warnings issued by automated intrusion detection, prevention, and firewall systems, and by the additional need to study the logs associated with other technology services and applications. In fact, our visibility into remote access security is so great that an organization must prioritize its review and response efforts. Hacking and remote access provided by malicious email attachments and drive-by downloads might or might not be the worst of problems, but they are the most visible. From a strategic point of view, it is important to ensure that the volume of the perceived remote threat and the resources directed against it are not considered to the exclusion of other equally pernicious threat vectors.

Proximity access refers to the abilities adversaries have when they are physically close to our ICT systems but not directly inside them. The interception of wireless

105 See: Crisis Management Plan for countering Cyber Attacks and Cyber Terrorism, Department of Information Technology, Ministry of Communications and Information Technology, Government of India, Workshop on Crisis Management Plan for countering cyber attacks and cyber terrorism, 2 February 2010.

signals is a good example of this vector. Through common techniques such as passive electronic monitoring of information being transmitted, joining a wireless connection and obtaining the ability to access other computers connected to the same wireless network – so-called peer-to-peer connections – or the attacker posing as a legitimate wireless network in order to lure unsuspecting users, wireless connected devices and access points can turn into a significant cyber security liability. Wireless keyboards can present similar opportunities for eavesdropper, broadcasting keystrokes through the air, even user IDs and passwords.

Finally, *insider access* must be addressed. Current employees, contractors, and trusted business partners have unique opportunities to do harm because they have been provided authorized access to our physical and digital spaces. Once authorized, they can operate from within without being challenged by the hard outer shell of gates and guards, intrusion prevention devices, and firewalls. Operating from the inside also provides a distinct perspective on an organization's security weaknesses, including technical gaps, lapses in policy enforcement, knowledge of where the crown jewels are located, and even vacation schedules of security staff, just to name a few. Although a cyber attack is more likely to come from an outsider, research indicates that when an insider does strike, the damage can be substantially greater.[106]

These threat vectors can only be efficiently resolved by seeking the best options for lowering the factors that are used in the formula for risk assessment: Risk = Threat x Vulnerability x Consequence. Lowering any of the three variable factors will lower the risk. And driving any of the factors to zero will eliminate the risk altogether. Policymakers, strategists, and those who operate on the front lines of cyber security should carry out their direct and indirect roles in ways that help to lower the threat, vulnerability, and adverse consequences associated with *supply chain and vendor access*, *remote access*, *proximity access*, and *insider access*. Anything less leaves the advantage with the adversaries.

Cyber Security is Evolving from a Technical Discipline to a Strategic Concept

The fact remains that the anonymity, global reach, scattered nature, and the interconnectedness of information networks continue to reduce the probability of detection and discovery of the origin of an attack, *thus making attribution a permanent problem*. Attackers can use ever more means of deception, most of them offering plausible deniability. Smart hackers can route attacks through countries with which the victim's government has poor diplomatic relations or no law enforcement cooperation. But even successful investigations often lead only to another hacked computer. Thus, states and governments still face the prospect of losing a cyber conflict without ever knowing the identity of their adversary.

106 Verizon Business Risk Team, 2009 Data Breach Investigation Report 11, 2009.

Hence, responses limited to the level of the nation-state are inadequate: *coordinated international activity*, with all the associated problems of reaching agreement and then acting in concert, is what is required. The enemy can only be known through close international cooperation. And his vulnerability can be learnt of and exploited through such cooperation.

International cooperation is one key to reducing cyber security risks,107 for attacks on systems connected to the Internet can originate from anywhere on that network. Vulnerabilities in software developed in one country and installed in a second can be exploited remotely from a third. Failures in critical information infrastructures in one nation can cascade into dependent systems elsewhere. Governments and the private sector need to coordinate their efforts to enhance cyber security levels, develop safe and trusted methods for information sharing about vulnerabilities, block and deter attacks, and improve the resilience of critical infrastructure.108 This requires also a new look at the regulatory norms, international legal norms and approaches.

As General Abrial, NATO Supreme Allied Commander Transformation, emphasized in a recent New York Times article, it will require international collaborative information-sharing and problem-solving among commerce, academia, government, and the military. "Today, a critical element of any cyber-defense strategy is the understanding that cyberspace is international by nature. No one country can deal effectively with cyber threats on its own … The concept of 'in-depth cyber defense,' which was endorsed at the Lisbon NATO summit in November 2010, is not intended to be a military-only, or even a military-centric, strategy. It necessarily cuts across the portfolio of a variety of actors, as it spans the technology employed, the awareness of users, and the physical protection of key elements of our hardware."109

Cyber attacks may rise to the level of a national security threat when adversaries have invested enough time and effort into creative and well-timed strikes on a critical national infrastructure target such as the electrical grid. National security planners should consider that electricity has no substitute, and that all other infrastructures, including computer networks, depend on it. Because the cyber attack threat to critical infrastructures is strategic in scope, the national response must be equal to the task: public awareness, investment in education, scientific research, the development of cyber law, and international cooperation. Because cyber security is evolving from a technical discipline to a strategic concept, and because cyber attacks can affect national security at the strategic level, national leaders must look beyond the tactical arena. The *quest for strategic cyber security involves marshaling all of the resources of a nation-state.* In this quest for strategic cyber security, it is advisable to put emphasis on a security

107 See: Kamlesh Bajai, *The Cybersecurity Agenda, Mobilizing for International Action*, New York, The EastWest Institute, 2010.
108 Peter Sommer & Ian Brown, "Reducing Systemic Cybersecurity Risk," OECD, OECD/IFP Project on "Future Global Shocks," 14 January 2011, p. 85.
109 General Stéphane Abrial, NATO Supreme Allied Commander Transformation, "NATO Builds its Cyberdefenses," *New York Times*, 27 February 2011.

system architecture that employs multiple tiers of defenses, that can be segmented under attack, and that has a healthy component of resiliency to allow speedy recovery.

The main improvements that could be made would be to strengthen mechanisms for global cooperation and capacity building, and to further increase the number of parties to the Cybercrime Convention. "The United Nation's Internet Governance Forum already brings together stakeholders from the public and private sector as well as civil society groups from around the world, and has actively considered security issues. If the UN decides to continue the existence of the forum, it would be an ideal venue for further global debate."110

110 William J. Drake, ed., *Internet Governance: Creating Opportunities for All,* The Fourth Internet Governance Forum, Sharm el Sheikh, Egypt, 15-18 November 2009, United Nations, 10-06439, September 2010.

4. Cyber Vulnerabilities and how Cyber Attacks are Enabled

Hostile actions against an IT system or network can take two forms: *cyber attack* and *cyber exploitation*. A *cyber attack* is the use of deliberate actions to alter, disrupt, deceive, degrade, or destroy adversary IT systems and networks or the information and programs resident in or transiting these systems. *Cyber exploitation* is the use of operations to obtain information, usually clandestinely and conducted with the smallest possible intervention that still allows extraction of the information sought.[111] These should not disturb the normal functioning of the systems. The best cyber exploitation is one that a user never notices.

Cyber attacks and cyber exploitations are possible only because *IT systems and networks are vulnerable*. Most vulnerabilities existing are introduced accidentally through *design or implementation flaws*[112] as described below. As long as nations rely on IT systems and networks as a foundation for military and economic power, and as long as these are accessible from the outside, they are at risk of being attacked.[113]

Vulnerabilities[3]	Description
Software	Applications or system software may have accidentally or deliberately introduced flaws the use of which can subvert the intended purpose for which the software is designed.
Hardware	Vulnerabilities can be found in hardware, including microprocessors, microcontrollers, circuit boards, power supplies, peripherals such as printers or scanners, storage devices, and communications equipment such as network cards. Tampering with such components may secretly alter the intended functionality of the component or provide opportuni-ties to introduce malware.
Seams between hardware and software	An example of such a seam might be the reprogrammable read-only memory of a computer (firmware) that can be improperly and clandestinely reprogrammed.

111 If the requirement for stealth is met, the adversary is less likely to take countermeasures to negate the loss of the exfiltrated information. In addition, stealthiness enables penetration of an adversary's IT system or network to result in multiple exfiltration of intelligence over the course of the entire operation.
112 Cyberdeterrence and Cyberwar, op. cit., p. xiii.
113 Source: Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," Journal of National Security Law & Policy, Vol. 4, 2010.

Communications channels	The communications channels between a system or network and the 'outside' world can be used by an adversary in many ways. An adversary can pretend to be an authorized user of the channel, jam it, and thus deny its use to the adversary, or eavesdrop on the channel to obtain information intended by the adversary to be classified or kept secret.
Configuration	Most systems provide a variety of configuration options that users can set based on their own tradeoffs between security and convenience. Because convenience is often valued more than security, many systems are – in practice – configured insecurely.
Users and operators	Authorized users and operators of a system or network can be tricked or blackmailed into doing the bidding of an adversary, or sell their services.
Service providers	Many computer installations rely on outside parties to provide computer-related services, such as maintenance or Internet service. An adversary may be able to persuade a service provider to take some special action on its behalf, such as installing attack software on a target computer.

Cyber attacks and cyber exploitation[114] require vulnerability, access to that vulnerability, and a payload to be executed. The primary technical difference between cyber attack and cyber exploitation is in the nature of the payload to be executed. A cyber attack payload is destructive whereas a cyber exploitation payload acquires information or intelligence nondestructively.

The payload is the term used to describe the things that can be done once vulnerability has been exploited. For example, if a software agent, such as a virus, has entered a given IT system, it can be programmed to do many things – reproduce and retransmit it, and destroy or alter files on the system. Payloads can have multiple programmable capabilities. Moreover, the timing of actions can also be varied, and if a communications channel to the adversary is available, payloads may be remotely updated. In some cases, the initially delivered payload consists of nothing more than a mechanism for scanning the system to determine its technical characteristics, and another mechanism through which the adversary can deliver the best software updates to further the compromise.[115]

Cyberspace is a virtual medium, and as such far less tangible than land, sea, air, and space, or the radiofrequency (RF) spectrum. One way to understand cyberspace in general, and cyber exploitation[116] and cyber attacks in particular, is to view it as

114 *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, Joint Report: Information Warfare Monitor, Shadowserver Foundation, 6 April 2010.
115 Cyberdeterrence and Cyberwar, op. cit., p. 67.
116 In the lexicon of cybersecurity, 'using' or 'taking advantage' of a vulnerability is often called 'exploiting a vulnerability.' The term 'cyber exploitation' in an espionage context is a cyber offensive action conducted for the purpose of obtaining information. The context of usage will usually make clear which of these meanings

consisting of three layers: (1) the *physical layer*; (2) a *syntactic layer* sitting above the physical; and (3) a *semantic layer* sitting on top.[117]

All IT systems rest on a physical layer consisting of boxes and wires. Electrical energy, integrated circuits, processors, storage devices, communications infrastructures, copper and fiber-optic cables, transmitters and receivers comprise the building blocks of this layer.[118] If that physical layer is removed, the IT system disappears as well. While it is obvious that IT systems can be attacked by kinetic means, IT systems cannot be deceived by destroying its components – although it can be through sly substitution of one component for another.

It is the *syntactic* layer that contains the instructions that designers and users give the machine, and the protocols through which machines interact with one another – device recognition, packet framing, addressing, routing, document formatting, database manipulation, etc. And this is the place at which intrusions or hacking are prone to take place as human outsiders seek to assert their own authority over that of designers and users.

The topmost *semantic* layer contains the information that the machine holds, the reason computers exist in the first place. Some of the information, such as address lookup tables or printer control codes, is meant for system manipulation; it is semantic in form but syntactic in purpose. Other information, such as cutting instructions or process-control information is meant for computer-controlled machinery. The rest of a system's information is meaningful only to people because it is encoded in natural language. The distinction between information and instructions can be imprecise. Indeed, many hacking tricks insert instructions in guise of content. Examples include attachments that contain viruses, Trojan horses or worms, logic bombs,[119] overly long addresses that create buffer overflows sending the extra bits into the processing stream, and webpages with embedded malware or code.[120] It is possible to attack computers solely at the semantic level by feeding the false information. But for the most part, only machines whose instructions have been tampered with at the syntactic level will accept false information.[121]

Vulnerabilities enable *intrusions*. And *intrusions* can lead to *disruption* and *corruption*. *Disruption* takes place when systems are tricked into performing operations that make them shut down, work at a fraction of their capacity, commit obvious errors, or interfere with the operation of other systems. *Corruption* takes place when data and algorithms are changed in unauthorized ways, usually to the detriment of their

of 'exploit' is intended.

117 Cyberdeterrence and Cyberwar, op. cit., pp. 12-17.

118 Electronics is the infrastructure of the computer world today. However, electronics are not immune to the future: the possibility of exploiting a biological infrastructure for computer purposes has already been proven. The computerization of DNA uses molecular biology and DNA instead of electronic components. Another possibility is the computerization of peptides: bio-molecular computerization which is based on compounds made of at least 2 amino acids.

119 A logic bomb is a piece of software intentionally and maliciously inserted into a software system that will damage or destroy the system's functionality when a specific condition occurs (e.g. a certain date or time is reached) or by command.

120 For example, an email may purport to be from the Internal Revenue Service – as it already happened. See: Internal Revenue Service, "Suspicious e-Mails and Identity Theft," *IRS press release*, 13 June 2008.

121 Cyberdeterrence and Cyberwar, op. cit., p. 13.

correct functioning. To distinguish between disruption and corruption is not easy. But a good rule of thumb is that the effects of disruption are drastic, immediate, and obvious, while the effects of corruption are subtle, and may linger on or recur.[122] It is relatively easy to tell that a system is not working. It is harder to tell that it functions but generates wrong information or makes bad decisions.

Intruders into IT systems and networks can steal information, issue phony commands to IT systems to cause them to malfunction, inject corrupted information to lead men and machines to reach wrong conclusions, or to make bad decisions. Yet system vulnerabilities do not result from immutable physical laws. They occur because of a gap between theory and practice. In theory, a system should do only what its designers and operators want it to. In practice, it does exactly what its code and settings tell it to. The difference exists because systems are complex, and growing ever more so.[123]

In all of this lies a saving grace. Errors can be corrected, especially if cyber attacks expose vulnerabilities that need attention, and that can be *patched*. The degree to and the terms by which computer networks can be accessed from the outside can be specified. Thus, there is, in the end, no forced entry in cyberspace. Whoever gets in enters through pathways produced by the system itself – with the exception of Denial of Service attacks (DoS) or Distributed Denial of Service attacks (DDoS), which clog the entryways to the system, rather than get into it. Hence, it is barely an exaggeration to say that all organizations are vulnerable to cyber attacks to the extent they want to be.[124] In no other domain of warfare is this the case.

Cyber attacks can be launched from outside the network, using hackers, or from the inside, using agents and rogue components. External hacking is the exemplary and by far the most common path that a state would take, particularly if going after civilian targets. But also the armed forces and intelligence agencies with systems that are generally better protected cannot completely ignore insider attacks, for example, by disgruntled employees.

At the *syntactic* layer, where hacking tends to take place, cyberspace is hedged with authorities. A person who owns a computer can normally do with it whatever he wants. For the most part the user should expect to retain full control over the computer, even when it is exposed to others via networking. Computers in an enterprise setting tend to come under control by *systems administrators*, and parts of such systems are closed to mere users. To hack a computer is to violate these authorities. A hacker may send a user a rogue email or lure a user to a rogue site from which bad code is downloaded. Some types of code steal information on such machines. Other types permit the hacker to issue subsequent commands to machines, thereby 'owning' them for malicious purposes.

Hackers can also enter enterprise systems by linking to them and successfully

122 Ibid., pp. 15-16.
123 Ibid., p. xiv.
124 Ibid., p. xiv.

masquerading as legitimate users with the rights and privileges of any other user. In some cases, hackers go further: fooling the system into thinking they have the privileges of *systems administrators*. As such, a hacker can arbitrarily change nearly everything about a system, not least the privileges other users enjoy. Once hackers have wormed their way into a system and appropriated enough privileges, they can perpetrate many additional forms of mischief.[125] Hackers intent on causing later mischief often facilitate their efforts by dropping spyware,[126] rogue computer code, backdoors,[127] Trojan horses,[128] and logic bombs into systems for later use. What can be termed implants often lie dormant, only to be activated either by events on the target machine or by direct command from the hacker. Once activated, these time bombs would enable an aggressor to rapidly take control of a targeted system before the victim has become aware of either the intruder or the infiltration.[129] In some cases, implants operate autonomously, searching for computers on the network that lack such implants, and making sure they do not lack for long. Regardless of what the hacker intends to do, the first and often the most difficult step, is getting inside. For this reason, the early phases of Computer Network Exploitation look the same as the early phases of Computer Network Attack. As a corollary, those with the best capability to get inside another system tend to be best qualified to carry out Computer Network Attack.

125 Apart from what can be obtained from the Internet, there exists a large amount of published material about computer hacking. For the more popular among these see: Jon Erickson, *Hacking: the Art of Exploitation*, 2nd ed., San Francisco. No Starch Press, 2008, and: Stuart McClure, Joel Scambray & George Kurtz, *Hacking Exposed: Network Security Secrets and Solutions*, 5th ed., New York, McGraw-Hill Osborne Media, 2005.

126 Patricia Moloney Figliola, *Spyware: Background and Policy Issues for Congress*, Washington D.C., CRS Report for Congress, Congressional Research Service, 7-5700, RL32706, 9 December 2009.

127 A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, while attempting to remain undetected.

128 A Trojan horse is software that appears to perform a desirable function for the user prior to run or install, but steals information or harms the system.

129 *On Cyber Warfare*, op. cit, p. 9.

Common Categories and Methods of Cyber Attack[130]

Attack	Description
Denial-of-Service Attacks	
Flooding	Sending extraneous data or replies to block a host service
Synchronize/reset flooding	Exploiting limited cache in IP stack to block connections
Smurfing	Using the IP broadcast system and IP spoofing to multiply floods
Out of band/fragment attacks	Exploiting vulnerabilities in IP stack kernel implementations
Nuking	Using forged messages to reset active connections
Specific denial of service	Generating requests that block one specific vulnerable service
Malicious Software Attacks	
Backdoor	Program feature allowing remote execution of arbitrary commands
Worm	Program that spawns and spreads copies of itself
Virus	Code that self-reproduces in existing applications
Trojan	Program-in-a-program that executes arbitrary commands
Exploiting Vulnerabilities	
Access permissions	Exploiting read or write access to system files
Brute force	Trying default or weak login/password combinations
Overflow	Writing arbitrary code behind the end of a buffer and executing it
Race conditions	Exploiting temporary, insecure conditions in program
IP Packet Manipulation	

130 Source: Ankit Fadia, *Network Security: A Hacker's Perspective*, Cincinnati, Premier Press, 2003, pp. 165-230.

Port spoofing	Using commonly used source ports (entry points) to avoid filtering rules
Tiny fragments	Using small packets to bypass firewall protocol/port/size checks
Blind IP spoofing	Changing source IP to access password services without a password
Name-server ID "snoofing"	Blind spoofing with calculated false ID numbers name-server-caches
Sequence-number guessing	Calculating TCP sequence/acknowledge number to spoof a trusted host
Remote-session hijacking	Using spoofing to intercept and redirect connections
Insider Attack	
Backdoor daemons	Opening a port for further remote access
Log manipulation	Removing traces of attacks and unauthorized access
Cloaking	Replacing system files to hide unauthorized access
Sniffing	Monitoring network data to find sensitive data (e.g. passwords)
Nonblind spoofing	Monitoring network to hijack active or to make forged connections

Unlike nuclear or other weapons of mass destruction, cyber weapons and cyber attacks require less infra-structure, and no restricted materials or knowledge which is in short supply. Cyber weapons have become easier to obtain and to use, much more powerful, and ever more sophisticated. Botnets,[131] for instance, which are used for launching Distributed Denial of Service Attacks (DDoS), are comprised of advanced remote exploitation capabilities within as many computers as a hacker can compromise all over the world. These programs, mostly well disguised, have several advanced capabilities. The characteristics of the 'Storm' worm, for example, a Trojan horse spread through email, include self morphing – it changes code to evade antivirus; self defending – if you try to delete it copies itself; self replicating – it identifies and infects other computers; self encrypting – it can encrypt and decrypt itself to elude signature detection; and self cloaking – it changes its communications path to inhibit tracking. The vast Storm botnet first detected in 2007, running on anything from 20 to 115 million computers, has increased its capacity constantly as more and more com-

131 A botnet (ro**bot net**work) refers to multiple computers infected with remote-controlled software that allows a single hacker to run automated programs on the botnet behind the users' back. The remote-controlled software or rootkit is clandestinely installed in each computer, hiding its presence and tracks, making detection difficult. The hacker can use the botnet for many purposes: distributing spam, spreading Trojan horses, perpetuating phishing scams, or gathering information for identity theft or fraud, etc.

puters have become compromised. 2010 saw a sharp escalation in the scale, frequency, and severity of DDoS attack activity on the Internet. For the first time an attack of 100 Gbps bandwidth was reported.[132] That represents a dramatic escalation in the amount of information that is piled up on a network in order to shut it down. Over 50 percent of the observed Internet attack traffic in the last quarter of 2010 originated from 10 countries, with the US, Russia, and China accounting for 30 percent. The global average Internet connection speed is now about 2 Mbps. Therefore, to deliver a 100 Gbps attack would take some 7,000 to 50,000 bots. The Dutch police found a 1.5 million-node botnet.[133] Estimates suggest that the botnet can generate more instructions per second than many of the world's top supercomputers. With so much power, attacks can be launched with devastating consequences.[134]

Classes of Attack[135]

Attack	Description
Passive	Passive attacks include analyzing traffic, monitoring unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information (e.g., passwords). Passive intercept of network operations can give adversaries indication and warnings of impending actions. Passive attacks can result in disclosure of information or data files to an attacker without the consent or knowledge of the user. Examples include the disclosure of personal information such as credit card numbers and medical files.

132 Arbor Networks, *Infrastructure Security Report 2010*, 1 February 2011, at http://www.arbornetworks.com/report
133 Akamai State of the Internet 2010.
134 Kevin Coleman, *Cyber Warfare Doctrine. Addressing the most significant threat of the 21st century*, McMurray, The Technolytics Institute, Analysis, 6 January 2008, p. 4.
135 Source: Information Assurance Technical Forum, *Defense in Depth*, Washington D.C., GPO, 2002, p. 5.

Active	Active attacks include attempts to circumvent or break protection features, introduce malicious code, or steal or modify information. These attacks may be mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks can result in the disclosure or dissemination of data files, denial of service, or modification of data.
Close-in	Close-in attack consists of a regular individual's attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry, open access, or both.
Insider	Insider attacks can be malicious or nonmalicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. Nonmalicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as "getting the job done."
Distribution	Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks can introduce malicious code, such as a backdoor, into a product to gain unauthorized access to information or a system function at a later date.

Standard Cyber Attack Process, according to Technolytics, 2009.

Viruses and Worms

There are computer *viruses* and *worms*. Viruses are harmful software programs secretly introduced into an IT system with the characteristic feature of being able to generate and distribute multiple copies of it, thereby spreading throughout the system. Viruses piggyback on programs already resident in a computer. Each virus has a destructive payload that is activated under certain conditions. When activated, a virus can corrupt, alter, or destroy data, generate bogus transactions, and even transfer information.[136] Worms are programs in their own right, which hide within a computer and stealthily propagate themselves onto other machines. Viruses do not spread on the network, worms do, and a virus can be their payload. Moreover, so-called polymorphic and metamorphic malware can automatically mutate in an attempt to avoid detection by anti-virus technology.[137]

Other Software which enables Exploitation of Vulnerabilities

There are many other types of software weapons enabling software vulnerability exploitation, such as information blockades, rootkits,[138] malicious embedded code, keyloggers,[139] IP spoofing,[140] logic bombs, sniffing, spamming, backdoors,[141] and video morphing. There are also dual-use technologies like port vulnerability scanners and network monitoring tools. New types of weapons are being developed at a rapid pace and existing weapons are morphing.[142] It is a safe prediction that cyber weapons are becoming ubiquitous.

One of the more persistent threats of 2010 was fake anti-virus, also commonly known as scareware or rogueware. Over half a million fake anti-virus software variants have been encountered in 2010. In this widespread practice, software is inveigled into a victim's computer system, closely resembling – and in some cases directly impersonating – genuine security solutions. The user receives a warning that his system is infected with some nasty malware and forced to pay for a 'full' version of the software to remove the threat. Of course, paying money to the bad guys does not provide any protection. In many cases there is no real danger, but in some cases they are ac-

136 Department of Cyber Defense – An organization who's time has come!," McMurray, *technolytics*, November 2007, p. 2.
137 "Think Your Anti-Virus Software Is Working? Think Again," *Lumension*, Scottsdale, March 2011, p.2.
138 A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating systems functionality or other applications.
139 Keystroke logging, or key logging, is the action of tracking the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that his actions are being monitored. There are numerous methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis.
140 IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computer system.
141 A backdoor in a computer (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text, and so on, while attempting to remain undetected.
142 Cyber Warfare Doctrine, op. cit., p. 3.

tually installing additional malware.[143] The search engine is the gateway to the web, and cyber crooks are skilled at manipulating search results from the engines such as Google, Bing, and Yahoo! to lure victims to their malicious pages. These pages host security risks and browser exploits just waiting to infect users who are directed to these sites.

Social Networking Tools

At the beginning of 2012, *Facebook* recorded 800 million users, making it not only the largest social networking site, but also one of the most popular destinations on the web. People use the Internet differently because of social networking. Young people are less likely to use email, and more apt to communicate through *Facebook*, *Twitter*, *LinkedIn*, *Digg*, *MySpace*, *YouTube*, and others. Unsurprisingly, scammers and malware purveyors targeted this massive and committed user base, with diverse and steadily growing of attacks throughout 2010.[144]

But as we have seen people around the world challenging autocratic authorities via the eRevolution, from Iran to Tunisia, Egypt to Bahrain, Yemen, and Syria, these social media means have become the new weapons of *mass mobilization*. To silence these dissidents, the Egyptian regime made a move Friday 28 January 2011 that has few precedents: it turned off the Internet nationwide, the first Internet blackout of such magnitude in the history of the Internet. A government's ability to control the Internet depends on its *control of Internet Service Providers* (ISPs): the private sector companies that grant Internet access to customers. So what happens in any country depends on the control that the state has over those ISPs. Some countries regulate the ISPs much more heavily. China has in the past turned off the Internet in various regions.[145] Because landline communication was never blocked, Egyptians found another way to access the Internet through dial-up Internet and fax services. They used Optical Character Recognition technologies to convert the fax image into text contents, and post the contents, news and updates into Facebook, Twitter, and other types of blogs. Google, in the meantime, launched a new service called "speak2tweet", which allowed Egyptians to call a regular landline number in Cairo and speak their tweet to an IVR/Voice recognition system. The speak2tweet system would then convert the caller voice message into a text tweet.

Restoring back the Internet, however, seemed to have backfired. Egyptians now were able to upload on Facebook and YouTube some of the pictures and video clips showing the massacres conducted by the central police forces and thugs on civilians in the early days of protests: live bullets fired by snipers, people run over by cars, others beaten to death, and many other atrocities. These social network agents of change helped the Arab civilization achieve what they could not do for decades in just

143 Sophos security threat report 2011, p. 5.
144 Ibid., p. 7.
145 Nepal and Burma have done this in 2005 and 2007. In 2011, Algeria, Morocco, Tunisia, Libya, Syria, and Bahrain have done this partially, with irregular nationwide outages lasting from a few minutes to several hours or a few days.

a few days or weeks. For a change, the Internet is applauded for its power to influence and change history for the better.

On the very day the Egyptian government shut down the country's 4 ISPs, two US Senators reintroduced legislation which, if passed, would grant the President the power to do essentially the same in the US. The so-called "kill switch" bill was approved by the Senate's Homeland Security and Governmental Affairs Committee back in December 2010, but expired once the new Congress assumed power a few weeks later. Senator Collins, who served as the Republican ranking member of the Committee, said the legislation would not allow the President to actually 'kill' the Internet, but would simply give him the ability to shut down "*critical infrastructure*" in the event of a serious cyber attack on the country. First titled "Protecting Cyberspace as a National Asset Act of 2010" and then the "Cybersecurity and Internet Freedom Act of 2011," the bill, which had bipartisan support, contains more than just the provision for a kill switch. It would establish a White House Office of Cyberspace Policy, tasked with oversight over all "instruments of national power relating to ensuring the security and resiliency of cyberspace" and with the enforcement of security standards to be developed by the National Institute of Standards and Technology (NIST) across public and private-sector "critical infrastructure systems." It would also establish a National Center for Cybersecurity and Communications in the Department of Homeland Security to oversee the US Computer Emergency Response Team.[146]

Beyond the legalities and politics of drastic action, it is worth asking whether the type of Internet shutdown seen in Egypt is even possible in the US. It seems unlikely that the government could cow the more than 2,000 ISPs operating in the country to a shutdown at once. It would first probably focus on Tier 1 ISPs – those that provide Internet access to other ISPs, and whose disruption would have the biggest ramifications. Another possibility would be to shutdown major Internet exchange points, or 'carrier hotels,' that exist around the country. Yet another would be to go after major wireless providers. But bringing them all to a screeching halt would not only damage the networks. It would also damage all public safety efforts, which rely on the Internet in the event of an emergency or natural disaster.[147]

Cloud Computing

Ever greater amounts of sensitive data are stored, accessed, and manipulated in databases connected to company websites as businesses increasingly interact with their customers through the Internet. *Cloud computing* is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider

146 Jonathan Zittrain & Molly Sauter, "Will the US get an Internet "kill switch"?," *Technology Review*, published by MIT. 4 March 2011.
147 Evan Halperin, "The "Kill Switch" Bill: What it means to first responders and public safety," *Input Deltek Information Solutions*, 22 February 2011.

interaction.[148] Cloud computing frees up budget for companies hand-cuffed by IT expenses. Instead of purchasing additional software licenses and hardware for new employees and locations, businesses can simply open new employee accounts with providers of their cloud-based services to expand computing capacity. But cloud computing also opens up a full spectrum of dangers that require additional protection and investment in expert systems to rapidly and accurately spot, analyze, and classify newly emerging threats.[149]

Compromised Hardware

While most computer security efforts have been focused on software, tampering with *hardware circuitry* is amounting to an equally dangerous threat. That is because modern computer chips routinely comprise hundreds of millions, or even billions, of transistors. The increasing complexity means that subtle modifications in manufacturing or in the design of chips are virtually impossible to detect. Compromised hardware is, almost literally, a time bomb. Maliciously tampered integrated circuits cannot be patched. They are the ultimate sleeper cell.[150]

Trojan horses hidden in equipment circuitry are among the most severe threats nations face in the event of war in which communications and weaponry rely on computer technology. As advanced systems like aircraft, missiles, and radars have become dependent on their computing capabilities, the specter of subversion causing weapons to fail in times of crisis, or secretly corrupting crucial data, has come to haunt military planners. The problem has grown more severe as most US semiconductor manufacturing plants have moved offshore. Ever since, counterfeit computer hardware, largely manufactured in Asian factories, is viewed as a significant problem. This, so much so, that the Pentagon is now restarting its own transistor production.

Directed Energy Weapons

And there are the *directed energy weapons* (DEWs), a class of weapons capable of disabling enemy IT systems without the use of explosives. These include *high energy microwaves* (HEMs), *high power microwave* (HPWs), and *transient electromagnetic devices* (TEDs). This class of weapons, in the arsenals of the US, Russia, China, Israel, and a number of other high-tech countries, operates by using pulses or beams of electromagnetic energy to fry, melt, disrupt or destroy electronic circuits and components

148 Definition proposed by the US National Institute for Standards and Technology (NIST) in 2009. There are 4 service models for cloud computing: (1) Software as a Service, where applications are hosted and delivered online via a web browser offering traditional desktop functionality; (2) Platform as a Service, where the cloud provides the software platform for systems; (3) Infrastructure as a Service, where a set of virtualized computing resources, such as storage and computing capacity, are hosted in the cloud, and customers deploy and run their own software stacks to obtain services; and (4) Hardware as a Service, where the cloud provides access to dedicated firmware via the Internet. See: "The Cloud – Understanding the Security, Privacy and Trust Challenges", *RAND Europe Technical Report*, 2011.

149 Brent Dirks, ASIS Session Examines Cloud Computing, Opportunities, Dangers, 21 October 2010. And: Art Gross, The dangers of cloud computing, Entegration, Inc., 17 June 2010.

150 John Markoff, "Cyberwar: Old Trick Threatens the Newest Weapons," *New York Times*, 26 October 2009.

in a computer, missile, tank, or any smart weapon that has not been properly hardened against such attacks.

Peripheries of IT Systems

Moreover, there are the *peripheries of IT systems* that contain user equipment, whose functions and parameters are established by users, which are vulnerable to exploitation. If not air-gapped[151] or protected via consistent encryption, user systems and privileges can be taken over through password cracking, phishing,[152] social engineering, downloads from bad websites, or use of bad media such as corrupted thumb or zip drives,[153] etc. It is a fact that the security of the periphery as a whole is often not better than the security of the most feckless user. Overall, all these vulnerabilities set the stage for cyberwarfare.

Additional Vulnerabilities

Cyberspace is highly vulnerable to disruptions for another reason: More than 95 percent of Internet traffic, including financial, trade, and other transactions, flows through *international undersea cables*, the disruption of which would effectively close the network down, and for which no amount of satellites would be an effective substitute.[154] These fiber-optic cables, which are concentrated in several choke-points, can be damaged by everything from fishing equipment and anchors to earthquakes and malicious activity.[155] Any major loss of cable would be catastrophic for the global economy since there are no backup plans. Governments need to take steps to protect these vulnerabilities. For example, agreeing to open up new cable routes to avoid the choke-points that are risky, and building some geographic diversity into the system; eliminating bureaucratic obstacles that can delay repair ships seeking to work in another country's territorial waters; working with the private sector to set up a new governance mechanism for undersea cables, thus ensuring that necessary statistical information on outages is shared immediately with the relevant parties; and conducting joint emergency response exercises. Without such measures cyber security will remain an elusive goal, and the world economy will remain at risk.

151 Physically completely separated from the Internet.

152 Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, credit card or bank account details by masquerading as a trustworthy entity, often combining an unsolicitated email (spam) and an illegal website (or a simple page) with the same 'look and feel' as a legitimate site.

153 One example of what a corrupted thumb drive can do occurred in 2008 when highly classified US Department of Defense networks were infected by an unknown adversary that placed malicious code on USB thumb drives and then dispersed them in parking lots near sensitive national security facilities. After a curious finder inserted the drives into computers, the code spread across DoD networks. See: "Pentagon cyber security role expands," *Oxford Analytica: Global Strategic Analysis*, 2 July 2010.

154 The total carrying capacity of submarine cables is in the terabits per second while satellites typically offer only megabits per second and display higher latency. However, a typical multi-terabit transoceanic submarine cable system costs several hundred million dollars to construct.

155 There were 50 incidents recorded in the Atlantic Ocean in 2007 alone. As a result of the cables cut multiple times 5 miles off the Egyptian coast, near Alexandria in early 2008, Internet and commercial traffic stalled in at least 10 Middle Eastern and South Asian countries. More than 80 million Web users in India, Pakistan, Egypt and Saudi Arabia had connection problems.

Two global trends within the information and communications technology environment, while providing greater efficiency and better services to users, will only increase vulnerabilities and the consequences of security failures. The first is *network convergence*: the merging of distinct voice and data technologies to a point where all communications – for example, voice, facsimile, video, instant messaging, computers, control of critical infrastructure, and the Internet – are transported over a common network structure, which will come to completion within the next five years. This convergence amplifies the opportunity for, and the consequences of, disruptive cyber attacks and unforeseen secondary or tertiary effects on other parts of the critical infrastructure. The second is *channel consolidation*: the concentration of data captured on individual users by service providers through emails or instant messaging, Internet search engines, Web 2.0 social networking means, and geographic location of mobile service subscribers, which increases the potential and consequences for exploitation of personal data by malicious actors.

The increased interconnection of information systems and data inherent in these trends pose threats to *Information Assurance*,[156] which comprises 5 essential criteria for the protection of information and the own systems against unauthorized access: *availability*, *integrity*, *confidentiality*, *authentication*, and *non-repudiation*.

- *Availability* applies to the information itself, its supporting technology and the people who operate and serve the infrastructure;
- *Integrity* refers to the trustworthiness of information and system or process reliability;
- *Confidentiality* is about denying access to the information and sensitive aspects of supporting technology, to those persons without authorization;
- *Authentication* refers to assuring that those who do access the information or supporting systems have the requisite authorization; and
- *Non-repudiation* is linked to authentication and, effectively, is the digital signature.

The principle that applies to functionally-interdependent systems, whereby the failure of one component can impact on the functionality of one or more other components, also applies to *Information Assurance*. Thus, if any of the above criteria are compromised for any reason, at least some elements of information and/or functionality and efficiency of related information infrastructures is also likely to be compromised. The more significant the compromise, particularly in key areas or system choke-points or nodes, the more significant the impact will be on functionality and efficiency. Identifying existing vulnerabilities, or creating vulnerabilities that will enable Information Assurance to be compromised, is an important part of the *targeting process*. The effective implementation of Information Assurance involves a wide range of security

156 Dennis C. Blair, Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, Washington D.C., Senate Select Committee, 2 February 2010, p. 3.

processes and procedures, as well as physical measures. One important measure is redundancy and diversity, which is intended to counteract the effects of any failure within, or compromise of, a system, or at least to minimize those effects. However, the high-end functionality and efficiency of many of the processes, systems, services, and capabilities we rely on and take for granted is dependent on current-generation hardware and software. For high-tech systems, in particular, the rapid changes in technology resulting in increasingly more powerful hardware and software, means that planned redundancy and diversity to provide effective backup and continuity, must also largely keep pace technologically with primary-use hardware and software. Hence, *redundancy and diversity must be recognized as part of the Information Assurance equation*, and must therefore be factored into targeting considerations.

Further technological innovations, well described in chapter 4 of Technology Trends and Threats in the Quest for Cyber Peace,[157] will increase and multiply vulnerabilities, which will require more intensive basic research and appropriate solutions. One fundamental problem is the lack of design and analysis methods which are scientifically proven to master the enormous complexity of future interconnected digital systems, especially regarding safety, reliability, functionality, and security – privacy, authenticity, and data security. Developing solutions for this fundamental problem will be one of the most important challenges for the computer science and web science research communities.[158]

The Challenges in Attribution

Cyber attacks can be carried out from anywhere. There are more than 2 billion personal computers in the world today. There were 5 billion mobile phones in use by the end 2010, amounting to 67 percent of world population, most of which are digital or web-enabled. An additional 1,000 new mobile phones are added to the mix every minute. Facebook alone claimed more than 800 million active users at the beginning of 2012.

One of the most important changes worldwide is the transformation of the mobile phone into an Internet phone, replacing the PC as the favorite device for connecting to the Internet. Already 9.5 percent of the population worldwide has mobile broadband.[159] Every one of these devices is a potential weapon. Add to this the multitude of cybercafés and other WiFi nodes that dot every city around the globe. In New York City alone a user can access the Internet from 85 public libraries, hundreds of open-access business WiFi hotspots – cybercafés, Starbucks and the like, 145 FedEx Office locations, and untold thousands of unsecured, open private networks.[160] To attribute an attack with any measure of certainty to a specific device, let alone a specific

157 Hamadoun I. Touré & the Permanent Monitoring Panel on Information Security World Federation of Scientists, *The Quest for Cyber Peace*, Geneva, International Telecommunication Union, January 2011, pp. 31-42.
158 Ibid., p. 41.
159 Ibid., p. 14.
160 Eugene E. Habiger, *Cyberwarfare and Cyberterrorism*, White Paper, The Cyber Secure Institute, 1 February 2010, p. 24.

individual or entity, is virtually impossible.

In fact, attribution – determining the source, location, and the identity of an attacker – is extremely difficult for both technical and nontechnical reasons. Electrons do not bear national markings. Because the Internet's creators never envisioned the need, the Internet has no reliable means for tracing where a message comes from. Furthermore, the Internet was not designed to withstand malicious alteration of the transmission packets.[161] Moreover, attackers enjoy a formidable advantage: *anonymity.* Smart hackers hide within the maze-like architecture of the Internet. Those with sufficient technical skill can remain anonymous at will.

Plausible deniability is also a concern. Because hackers obscure the true origin of an attack by hopping through a series of compromised computers to reach their target, the attacker can always claim that his computer had been hacked and used in someone else's operation. They can even leave behind a 'false flag,' implicating an otherwise innocent individual, group, or government. The most sophisticated cyber attack or exploitation may never be discovered. And this situation is not likely to change soon; it is a systemic aspect of the Internet, not a simple problem that can be fixed. Thus, states face the prospect of losing a cyber conflict without knowing the identity of their adversary. This is particularly true of the recent attacks that are suspected to have been committed by China, Russia, and North Korea.

Other Opportunities to Hide the Attacker's Identity or to Assume another Identity

The rules for formatting and transmitting data – known as the Transmission Control Protocol/Internet Protocol (TCP/IP) – make the system work, and remain the foundation for today's Internet. The complexity of the TCP/IP task was accomplished by layering the rest of the communications process. At the bottom, a *Data Link layer* includes the hardware used to access the Internet. The TCP/IP takes up the next two levels with (1) a *Transport layer* that breaks up and reassembles data; and (2) a *Network layer* that routes data to its destination. At the top of the stack lies an *Applications layer* that converts data into webpages or files. Each layer performs its function without knowing what the other layers do. Internet Explorer works on the Applications layer, regardless of the connection – broadband, WiFi, satellite – used at the *Data Link layer*. Together, packet switching and network layering provide attackers numerous opportunities to hide their identity or assume another.

In lieu of personal identification, the *Network layer* uses an Internet Protocol (IP) address to identify the origin or destination of routed data. To uncover the source of an attack or cyber exploitation requires associating the IP address with a particular individual, group, or state. Social media like Twitter, for example, keep a record

161 The Internet transmits messages by breaking them into many discrete data packets, each of which may be sent across the Internet using different paths to arrive at the final destination, where the Internet Protocol reassembles the packets to reform the original message.

of every IP address visiting the site, which allows identification of the attacker's IP address. The Internet Service Provider (ISP) can be found via the Internet Assigned Numbers Authority (IANA) database that assigned the IP address. If that ISP keeps good records, it can reveal to which computer modem it had assigned that address. However, given the ever growing Internet data volumes, ISPs regularly empty out their logs. That means that sourcing requests have to happen quickly, otherwise any evidence to identify perpetrators is gone. But even where there are records, the IP address might go to a corporate account, numbering thousands of users. Or the trail might end sooner if it leads to a coffee shop that gives users free access. Moreover, the trace might lead to a botnet where the attacker can install several stepping stones between the attacking computers and the system used to control and command it.[162]

Attackers can also forge the address of an IP packet,[163] and make other individuals, groups or government IP addresses appear as the responsible party. And these are just the opportunities for anonymity on the Network layer. The *Data Link layer* has its own opportunities, such as the use of pre-paid, wireless and Internet-accessible devices that grant access without any record of the user's identity. At the *Application layer*, social engineering gives attackers additional opportunities to hide. They also routinely destroy or modify system logs so victims lack information on what happened.

Thus, the odds are that one simply may not know the attacker or where the attack came from – which is inhibiting *retaliation* as well as *deterrence.* It is exponentially harder to deter another nation when that nation is all but certain that it can carry out an attack without a return address. Attribution may be so uncertain that the odds that any one cyber attack could evoke a response would be fairly low. But the lower the probability of getting caught, the higher the penalty required convincing potential attackers that what they might achieve is not worth the cost.[164]

Digital Evidence

Because of the attribution problem, cyber attackers are rarely held accountable for their actions. Another explanation for the lack of possibilities to deter and to counterattack cyber intruders is the dependence on digital evidence. Digital evidence is different from evidence created, stored, transferred, and reproduced from a non-digital format. It is ephemeral in nature and susceptible to manipulation. These characteristics of digital evidence raise issues as to its reliability. Network-based evidence poses additional problems because it is volatile, has a short life span, and is frequently located in foreign countries. Investigators face the twin obstacles of identifying the author of a cyber attack and proving that the author had the intention to do it – or 'guilty knowledge.' Even more is at stake when the cyber attacker is a trusted insider who has

162 John Markoff, "Webs Anonymity Makes Cyberattack Hard to Trace," *New York Times*, 17 July 2009.
163 David Chaikin, "Network Investigations of cyber attacks: the limits of digital evidence," *Crime, Law and Social Change*, Vol. 46, No. 4-5, 2006, pp. 239-256.
164 Cyberdeterrence and Cyberwar, op. cit., p. 43.

intimate knowledge of the IT security system of the organization.[165]

Thus, cyber attacks have become a very annoying global problem because they are low-risk, low-cost,[166] highly effective, and easily deployable globally. The cost to develop this new class of weapons is within reach of many countries, extremist or terrorist groups, and even of individuals. The raw materials needed to construct cyber weapons are not restricted and widely available. Apart from states, there are also cybercrime organizations that are known to develop cyber weapons. Among the most notorious is the Russian Business Network, commonly known as RBN, which originated as an Internet service provider for child pornography, phishing, spam, and malware distribution in St. Petersburg. By 2007, it developed partner and affiliate marketing techniques in many countries to provide a method for organized crime to target victims internationally.[167] It is specializing in, and in some cases monopolizing, personal identity theft for resale, and is the originator of MPack and alleged operator of the Storm botnet. RBN has been described by VeriSign as 'the badest of the bad.'[168] It is not a registered company, and its domains are registered to anonymous addresses. Its owners are known only by nicknames. It does not advertise, and trades only in untraceable electronic transactions.

RBN and their support units provide scripts and executables to make cyber weapons undetectable by anti-virus software. Every time a copy of the cyber weapon is generated, it looks different to the anti-virus engines, and it goes ever more often undetected. The modularization of delivery platform and malicious instruction is a growing design in cyber weapons. RBN's cyber weapons are very popular and powerful. In June 2007, one was used by a single person to attack and compromise over 10,000 websites in a single assault.[169]

Cyber Weapons

A missile is comprised of three basic elements: (1) a *delivery vehicle*, the rocket engine, (2) a *navigations system* which tells it how to get to the target, and (3) the *payload* – the components that cause harm. The same three elements appear in the design of a cyber weapon. There are numerous methods of delivering cyber weapons to their targets. Emails with malicious code embedded or attached is one mechanism of delivery. Another is websites that have malicious links and downloads. Or it can be done by wireless code insertion transmitted over radio or radar frequencies.[170] Hacking is a *manual delivery vehicle* that allows placing the malicious payload on a target computer, system or network. Counterfeit hardware, software, and electronic com-

165 David Chaikin, "Network Investigations of cyber attacks: the limits of digital evidence," op. cit.
166 A stealth bomber costs $1.5 to 2 billion; a stealth fighter costs $80 to 120 million; a cruise missile costs $1 to 2 million, whereas a cyber weapon could cost $300 to $50,000 or more.
167 Brian Krebs, "Shadowy Russian Firm Seen as Conduit for Cybercrime," *Washington Post*, 13 October 2007.
168 "A walk on the dark side," *The Economist*, 30 August 2007, at: http://economist.com/displaystory.cfm?story_id=9723768
169 Kevin G. Coleman, *Preparing for a Cyber Attack. Countdown to eDay!*, McMurray, The Technolytics Institute, no date.
170 Clarke & Knake, op. cit., p. 7. And: David A. Fulghum, "Searching for Ways to Trace Cyber Attackers," *Aviation Week and Space Technology*, 20 May 2011.

ponents can also be used as delivery vehicles. Just as the navigation system guides a missile, it allows the malicious payload to reach a specific point inside a computer, system or network. System vulnerabilities are the primary navigation systems used in cyber weapons. Vulnerabilities in software and computer system configurations provide entry points for the payload. These security exposures in operating systems or other software or applications allow for exploitation and compromise. This enables unauthorized remote access and control over the system.[171]

The payload of a missile is the warhead which is packed with some type of 'explosive.' In a cyber weapon, the payload could be a program that copies information off of the computer and sends it to an external source. It can also be a program that is altering and manipulating information stored on the system. Finally, it can enable remote access so that the computer can be controlled or directed over the Internet. A 'bot'– a component of a botnet – is a good example of a payload that makes possible the remote use of an IT system by an unauthorized individual or organization.[172] The three-element architecture demonstrates how advanced and sophisticated cyber weapons are becoming. The architecture creates reusability and reconfiguration of all three components. As software or system vulnerability is discovered, reported, and patched, that component can be removed and replaced while the other two components are still viable. This not only creates flexibility, but also significantly increases the productivity of the developers of cyber weapons.

Nations are becoming increasingly vulnerable to cyber attacks that could have catastrophic effects on critical infrastructures as well as severely damage national economies. Massive cyber attacks even in only a segment of the system are difficult to control, and their consequences could be incalculable. There is a built-in tendency for unleashing chain reactions even from modest incidents.[173] They could decisively alter the power equations, the stability of the entire digital environment on which society depends, much beyond the parties to a conflict. The interest in the maintenance of transnational networks and information structures is an interest shared by all international actors. Thus, priority must be given to the maintenance or early restoration of a stable digital environment. That *clearly places the emphasis on defense*. Resilient IT infrastructures discourage attacks. Resilience includes several elements, among which are the self-healing quality of systems, the availability of warning systems, built-in redundancies, but also trained behavioral modes like the exploration of areas of cooperation within the stakeholder community, and encouragements to practice it.

171 Kevin G. Coleman, *Preparing for a Cyber Attack. Countdown to eDay!,* McMurray, The Technolytics Institute, no date.
172 Ibid.
173 "The international community needs to be aware that a small cyber skirmish could be the precursor to a major cyber conflict that potentially will spark a regional kinetic engagement that will have international repercussions." John Bumgarner, Chief Technology Officer, US Cyber Consequences Unit, *Jane's Defence Weekly*, 29 September 2010.

5. Major Issues, Ambiguities, and Problems of Cyberwar

Cyber attack as a mode of conflict raises many operational issues and, due to inherent ambiguities, some other problems. Among these is the *'use of force'* and *'act of war' conundrum*. Problems also derive from the *legal framework governing cyber attacks*. Then, there is the *problem of deterrence in cyberspace* that is affecting retaliation, preemption, and conflict escalation. *Networked forces*, the most recent military innovation, hold the promise of fighting more effectively, but they also create more uncertainties. In order to *effectively manage cyber conflicts*, these may have to be categorized into various levels, depending on their intensity and impact on war. In addition, there is the still unresolved problem of *destructiveness of cyber attacks*. And connected with this is the problem of *what effects newest malware* like Stuxnet *might have on the mode of future conflict*.

'Use of Force' and 'Acts of War'

Cyber attack refers to deliberate action to alter, disrupt, deceive, degrade, or destroy computer systems and networks or the information and/or programs resident in or transiting these systems or networks. Thus, it is not correct to call every bad thing that happens in cyberspace and on the Internet *war* or *attack*. War is the *use of force* to cause damage, destruction or casualties for political effect by states or groups. A cyber attack may be an act intended to cause damage or destruction. There is a grey area, of course, that consists of disruption of data and services *below the level of use of force*. The threshold should be high for calling a disruptive activity *an act of war* or *an attack*. An act of war involves the use of force for political purposes by or against a state.[174] Force involves violence or intimidation by the threat of use of force. If there is no violence, it is not an attack. If there is no threat of violence, it is not the use of force. And here too is a grey area consisting of clandestine or covert activities. But if an opponent intends for a cyber exploit to remain undetected, and if the exploit does not inflict physical damage or destruction, it is not intimidation, not the use of force, nor is it an attack.

What is the legal framework governing cyber attacks? The *Rules of Armed Conflict* that guides traditional wars is derived from international treaties, such as the Geneva Conventions, International Humanitarian Law, and the practices that nations consider *customary international law*. Among them is the UN Charter that was designed, in essence, to ban 'war' from the lexicon of nations.[175]Article 2(4) of the Charter

174 In 1999, a professor published a framework for determining what constitutes an act of force or war, which would warrant a retaliatory response of some kind. See: Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,* Colorado Springs, Institute for Information Technology, 1999, p. 17.

175 Charter of the United Nations and Statute of the International Court of Justice, San Francisco, United Nations, 1945.

demands that nations "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[176] Despite the reference to territorial integrity and political independence, it is now widely understood that the prohibition applies to *any use of force not otherwise permitted by the terms of the Charter*. It sanctions only *two exceptions* to this prohibition on the *use of force*: (1) when the UN Security Council authorizes force, and (2) when a nation acts in self-defense.

As to *self-defense*, Article 51 says that nothing in the Charter shall "impair the inherent right of individual or collective self-defense if an armed conflict occurs" against a UN Member. Though International Humanitarian Law does not specifically mention cyber operations, the absence of specific references to cyberwar does not mean that cyber operations are not subject to the rules of international law. The essence of an armed operation is the causation, or risk thereof, of death or injury to persons and damage to or destruction of property and other tangible objects.[177] If the means and methods of cyberwar produce the same effects in the real world as conventional weapons, such as destruction, disruption, damage, injury or death, they are governed by the same rules as conventional weapons.

Of all the legal issues bedeviling cyberwar, the issue of when a cyber event amounts to an *act of war* captures most interest.[178] The *threshold* for regarding a cyber incident as the use of force is the most *important ambiguity in cyberwar*. The right of self-defense is triggered by the use of force. This makes the question of the threshold between an act that justifies the use of force and an act that does not central in cyberwar. When cyber attacks are persistent and insidious, they could arguably pose a risk to national security if they are detrimental to industry and society as a whole; consequently affect the security and stability of the state.[179] However, only large scale cyber attacks on critical infrastructures that result in significant physical damage or human losses comparable to those of an armed attack with conventional weapons would entitle the victim state to invoke self-defense under Article 51 of the UN Charter. While Article 2 prohibits all threats and uses of force, Article 51 allows the use of force *only* in response to an *armed attack*. But not all uses of force qualify as *armed attacks* that are a prerequisite to an *armed response*. Thus, a nation may become victim of cyber force being applied against it but cannot respond in kind because the force it suffered did not amount to an *armed attack*.

Basically, threatening destructive cyber attacks against another state's military infrastructure if that state mounts unlawful cross-border operations would not breach the norm. But threats of destructive cyber operations against another state's critical infrastructure would do so – unless that state cedes territory. However, the prohibition applies only to an explicit or implied communication of a threat. It does not

176 Ibid., p. 3.
177 Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, National Academies Press, 2010, p. 163.
178 Anna Mulrine, "When is a Cyberattack an Act of War?", *Christian Science Monitor*, 18 October 2010.
179 *On Cyber Warfare*, op. cit., p. 9.

reach actions which simply threaten the security of the target state, but which are not communicative in nature. Hence, the introduction into a state's cyber systems of vulnerabilities which *are capable of destructive activation at some later date* would not constitute *a threat of the use of force*, unless their presence is known to the target state, and the originating state exploits them for some coercive purpose.[180]

There is consensus based on international practice that propaganda, harassment, hacktivism, and crime *do not justify the use of force in response*. But other areas are less clear. For example, when does *intelligence collection* or *cyber reconnaissance* become an act of war? Such activities are usually not considered sufficient justification. Nondestructive computer methodologies employed for cyber espionage may violate the domestic law of the victim nation-state *but are not contrary to international law.*[181] However, intelligence collection that involves the theft of terabytes[182] of classified information – as happened with the attacks on the US Department of Defense and the US Central Command in 2008, leaving behind great damage – may eventually be interpreted as an act of war.[183] Ultimately, however, the decision as to whether something is an act of war is a political decision. "At the end of the day, the answer to whether a particular attack is an act of war comes down to this: Is it in your interest to declare it so?"[184]

Violation of sovereignty is an equally imprecise guide for deciding what an *act of war* in cyberspace is. Spies, criminals, and hackers routinely send packets across borders with malicious intent. These activities are violations of sovereignty, but individually, they do not qualify as *acts of war*. Inserting spies, whether physically or digitally, would not generally be regarded as a use of force justifying a forceful response – unless the violation could be portrayed as an attempt at coercion or intimidation. It could be argued that massive and repeated violations of sovereignty by cyber intrusions could be interpreted as an act of war. But it would be incumbent upon the target nation to first notify the attacker that further intrusions would be regarded as an act of war. The failure of any nation to make such a notification or complaint so far in the face of massive cyber intrusions over the last decade means that the opportunity has been missed to create such a threshold or constraint in cyber conflict.[185]

The interpretive dilemma of whether cyber operations constitute a *use of force* is that the drafters of the Charter took a cognitive short cut by framing the treaty's prohibition in terms of the *instruments of coercion employed – force*. Yet, it is seldom the instruments employed, but instead the *consequences* suffered, that matter to states. At

180 See Michael N. Schmitt, Cyber Operations as a "Use of Force" in *Proceedings of a Workshop on Deterring Cyberattacks, Informing Strategies and Developing Options for U.S. Policy*, The National Academies Press, 2010, p. 153.
181 Walter Gary Sharp, *Cyberspace and the Use of Force*, San Antonio, Aegis Research Corp., 1999, pp. 123-32.
182 Equivalent to what is stored in papers and books in the US Library of Congress, which amounts to some 12 terabytes.
183 See: http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml. Also: "Pentagon cyber security role expands," *Oxford Analytica: Global Strategic Analysis*, 2 July 2010.
184 *Cyberdeterrence and Cyberwar*, op. cit., Annex A: What Constitutes an Act of War in Cyberspace? p. 180.
185 In May 2011, the Pentagon has decided that cyber attacks constitute an act of war. In a classified document it concluded that the US may respond to cyber attacks from foreign countries with traditional military force. While some say the policy is in keeping with the times, others worry that it could lead the country into war more easily. See: John Hudson, *Reuters*, 31 May 2011.

the time the Charter was drafted an instrument based-approach made sense, for prior to the advent of cyber operations the consequences that states sought to avoid usually comported with instrument-based categories. But cyber operations do not fit neatly into this paradigm because, although they may be 'non-forceful' or 'non-kinetic,' their consequences can range from mere annoyance to death. Resultantly, as the present Commander of US Cyber Command noted during his confirmation hearings, policy-makers must understand that "there is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force."[186]

Hence, discomfort among cyber warriors in the armed forces relying on existing law of armed conflict norms is understandable since most of the international agreements and practices of nation-states that comprise the law of armed conflict predate the cyber era. Thus, there is an urgent need for seeking international consensus, not only on the *right to response by the military*, but also *on rules of engagement for cyberwar*, including how nations might use private-sector networks to reroute traffic and shut down attacks. Some experts like Bruce Schneier warn that the time is running out to put in place *a cyber treaty* that could, as he advocates, "stipulate a no first use policy, outlaw unaimed weapons, or mandate weapons that self-destruct at the end of hostilities."[187] While many legal tools for dealing with coordinated attacks already exist, nations need to develop *the policies* to allow *countermeasures*, such as mutual aid agreements and cyber security policies, and, foremost, *for governance of cyberwar*.

While agreements that might expedite cyber law enforcement efforts are possible, it is not likely that any new international treaty governing cyberwar or cyber weaponry will be forthcoming in the foreseeable future. Although most people cheer international treaties that have banned chemical and biological weapons, some experts see them as unintentionally inhibiting the development of nonlethal and low-lethality weaponry.[188] Even the US government, while emphasizing the need for 'building the rule of law through international norms and processes' in its latest International Strategy for Cyberspace,[189] perhaps the first national 'foreign policy' for the Internet, seems guarded with respect to *cyber arms agreements*. Writing in a recent issue of *Foreign Affairs*, Deputy Secretary of Defense William Lynn observed that "traditional arms control agreements would likely fail to deter cyber attacks because of the challenges of attribution, which make the verification of compliance almost impossible."[190] Attribution stubbornly permeates every aspect of cyber operation; it is, indeed, the 'single greatest challenge to the application of the law of armed conflict to cyber activity.'[191]

186 Unclassified Senate Testimony by Lt Gen Keith Alexander, Nominee for Commander US Cyber Command, 15 April 1010.
187 See "Time for a Treaty," *Defense News*, 18 October 2010, and Bruce Schneier, "It will soon be too late to stop cyberwar," *Financial Times*, 2 December 2010.
188 See John B. Alexander, "Optional Lethality: Evolving Attitudes towards Nonlethal Weaponry," *Harvard International Review*, 7 May 2006.
189 White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, May 2011.
190 William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs,* 89, No. 5, September/October 2010.
191 Todd C. Huntley, "Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Con-

Essentially, however, this is a technical issue, not a legal one. Nonetheless, the identity of the attacker may well determine if *a state of war* exists.

For more than a decade the potential threat and opportunity of cyberwar has confronted military planners, while the international community has yet to reach consensus on the application of International Humanitarian Law. This lack of consensus may be due to a variety of reasons, from holding that the current framework of International Humanitarian Law can be applied to cyberwarfare *by analogy* to the realization that the vast growth and fluidity of technology would render potential international agreement quickly obsolete.

The absence of prohibition of cyberwar in the law of armed conflict is significant because, as a general rule, that what is not prohibited is permitted.[192] But the absence is not dispositive, because even where international law does not purport to address particular methods, weapons or technologies of cyberwar, the general principles of International Humanitarian Law do apply to cyberwar – *with limitations*.

What are the Limitations that International Humanitarian Law imposes on Cyberwar?

Once a state has entered into a conflict, the use of force is governed by *jus in bello*, which is largely derived from the Hague Conventions,[193] the Geneva Conventions,[194] and their associated protocols, much of which is considered customary international law. Even states that have the lawful right to use force still have limitations in how they use force. The restraints on how a state conducts its use of force are not contingent on the weaponry used. So transposing the principles of international humanitarian law to the use of cyber attacks is not only possible, but appropriate given its growing popularity as a coercive tactic. This requires a look at the principles that derive from the traditional schema of *use in bello* in relation to cyberwar: *military necessity*, *distinction*, *proportionality*, *perfidy*, *neutrality*, and *unnecessary suffering*.

The ***principle of military necessity***: When a cyber attacker is party to a conflict, international humani-tarian law restricts the use of force to targets that will accomplish valid military objectives. Lawful targets are limited to "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization offers a definite military advantage."[195] Article 23 of the 4th Hague Convention forbids destruction or seizure of property, "unless such destruction or seizure be imperatively demanded by

flict During a Time of Fundamental Change in the Nature of Warfare," *Naval Law Review*, Vol. 60, 23 November 2010, pp. 1-40.

192 See: *Legality of the Threat or Use of Nuclear Weapons;* Advisory Opinion, International Court of Justice, 8 July 1996.

193 Hague Convention IV Respecting the Laws and Customs of War on Land, Annex, 18 October 1907.

194 See e.g. The Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949.

195 Article 52 of the 1977 Additional Protocol to the Geneva Conventions.

the necessities of war." A violation of the principle of military necessity is considered a 'war crime' in the Rome Statute of the International Criminal Court.[196]

A cyber attack that targets an adversary's military computer systems satisfies the condition of military necessity by virtue of their exclusive military association. There are many opportunities for cyber attacks within the computer systems of modern armed forces, which use computer systems within every facet of their operations. A deeper shade of grey occurs, however, when determining whether a target creates a '*definite military advantage*.' Presumably, this limits cyber attacks whose military advantages are indeterminate. The complexity of computer systems makes such a calculation a challenge. The value of a cyber weapon often lies in its cascade effect on systems that rely upon the initial target. Most cyber attackers *do not have sufficient information to predict the indirect effects of an attack*. An attacker that indirectly targets a military computer system might be unsuccessful. An attacker that penetrates into computer systems of an electrical generator might gain a military advantage, but the system may have unforeseen layers that prevent such an advantage from occurring. In these circumstances, the military advantage is not definite enough to satisfy the condition of military necessity. Moreover, military necessity is weighed against other limiting principles, including the principle of distinction.

The principle of distinction: In order to ensure respect for and protection of the civilian population and civilian objects, the parties to a conflict are required to "at all times distinguish between the civilian population and combatants, and between civilian objects and military objectives." [197] And attackers are required to ensure that "the civilian population and individual civilians … enjoy general protection against dangers arising from military operations" and "not be object of attacks."[198] Attackers must direct their operations only against military objectives. Four rules follow from this principle:

- The ***obligation to direct attacks only against 'military objectives***,' as defined by the 1977 Additional Protocol I of the Geneva Conventions. The definition comprises two conditions: first, it must make an effective contribution to the military action of the adversary, and secondly, in the circumstances ruling at the time, the attack must offer a definitive advantage to the attacker. Whenever these two conditions are *simultaneously present*, there is a military objective in the sense of extant international humanitarian law.

- The ***prohibition of indiscriminate attacks***. According to Article 51 of the 1977 Additional Protocol I of the Geneva Conventions, an indiscriminate attack is one which is not carefully aimed at a specific military objective, either through carelessness or use of weapons that are by their nature not capable of being so directed, or because the effects of an attack on the military objective are uncontrollable and

196 Rome Statute of the International Criminal Court, Article 8(2)(a)(iv),1998.
197 Article 48 of the 1977 Additional Protocol I to the Geneva Convention.
198 Article 51 of the 1977 Additional Protocol I to the Geneva Convention.

unpredictable.

- The need to minimize collateral civilian damage and to abstain from attacks if such damage is likely to be disproportionate to the value of the military objective to be attacked. An attack against a military objective with lawful means or methods of warfare causing collateral civilian damage or injury only becomes illegal if it violates the rule of proportionality. This would be an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relations to the concrete and direct military advantage anticipated.[199]

- The ***needs to take the necessary precautions*** to ensure that the above three rules are respected.[200]

The ***principle of proportionality***, similar to distinction, is concerned with the consequences of an attack on civilians and civilian objects as it relates to the achievement of a military goal. Proportionality governs the degree and kind of force used to achieve a military objective by comparing the expected military advantage gained to the expected incidental damage to civilians and property. It applies to both whether a given level of force is appropriate in response to a particular grievance, as part of the law of the use of force, or *jus ad bellum*,[201] and whether a given action is appropriate in light of its objectives and the casualties that will result, as part of the law of armed conflict, or *jus in bello*.[202] Commanders must minimize civilian casualties, subject to the need to accomplish a particular military mission, and they must weigh the cost of civilian lives against the benefit to be gained by the mission.

Proportionality applies to the ***indirect effects of an attack as well***. Some objects have such dangerous indirect effects that targeting them is outright prohibited. "Works or installations containing dangerous forces, namely dams, dykes, and nuclear electrical generating stations, shall not be the object of an attack, even where those objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."[203] The Rome Statute incorporates proportionality within its enumeration of particular crimes.[204]

The prohibition on perfidious conduct – arising from the desire to restore peace without completely destroying the adversary. Cyberwar creates new opportunities for practicing *ruses of war*. Since Computer Network Exploitation is likely to be an important tool for intelligence collection, the parties to a conflict will be tempted to plant misinformation deliberately with a view to confuse the adversary. Such misinformation about military plans is perfectly lawful and is no different in principle to

199 Wording used in Article 51(5)(b) of the 1977 Additional Protocol I of the Geneva Conventions.
200 These rules are defined in Article 57 of the 1977 Additional Protocol I of the Geneva Conventions.
201 Judith Gail Gardam, "Proportionality and Force in International Law," *American Journal of International Law*, 1993, p. 396.
202 Ibid., p. 391.
203 As stated in Article 56 of the1977 Additional Protocol I of the Geneva Conventions.
International Telecommunications Convention, Art. 35.
204 Rome Statute of the International Criminal Court, Article 8(2)(b)(iv).

any other vehicle for misinformation. But with all ruses of war, the parties to a conflict must ensure that they *do not cross the line into perfidy.*[205] For example, causing enemy forces to believe that combat vehicles of the opponent were medical vehicles or those of neutrals would be perfidious. Another example of prohibited perfidious conduct would be if an adversary raises the flag of surrender with the implicit promise to lay down their arms, and once the armed forces that they are fighting expose themselves from cover, the adversary begins firing on them.

The ***principle of neutrality*** permits a state to declare itself neutral to a conflict, and thereby protects the neutral state from attack or trespass by belligerents. Neutral states remain protected as long as they do not militarily participate or contribute to belligerent states or allow their territory to be used for such military purposes.[206] Notwithstanding these restrictions, a neutral state may maintain its relations with belligerents during hostilities.

To retain the title of neutrality, a state may not allow belligerents to move troops, munitions of war or supplies through neutral territory. An attack through a network that crosses neutral territory, or uses a neutral country's satellites, computers, or networks, would infringe upon that neutral's territory. The attack would thus be considered illegal and, perhaps, an act of war against a neutral.[207] Conversely, a neutral's failure to resist the use of its networks for attacks against another country may make it a legitimate target for reprisals by the country that is the ultimate target of the attacks. There is one exception to the inviolability of a neutral state's territory. Under Article 8, a nation need not "forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals" as long as the neutral state permits the use of its telecommunications infrastructure impartially.[208]

In addition, any attack involving networks and telecommunications may implicate the International Telecommunication Union (ITU) and its underlying charter, the International Telecommunication Convention (ITC), which apply to international wire and radiofrequency communications. The ITU, and the regulations promulgated under it, do have some applicability to cyberwar and information warfare attacks that use the electromagnetic spectrum or international telecommunication networks. First, broadcasting stations from one nation may not interfere with broadcasts of another states' services on their authorized frequencies.[209] The International Frequency Regulation Board of the ITU allocates the electromagnetic spectrum to prevent interference. Even military installations must observe the noninterference requirement.[210] Additionally, offshore radio stations are banned, and states may not carry out transmission of false or misleading signals. However, even where cyberwar and information

205 See definition in Article 37 of the 1977 Additional Protocol I of the Geneva Conventions.
206 Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land.
207 See: United Nations Manual on the Prevention and Control of Computer-Related Crime, 1993, pp. 261-164.
208 Idem., Article 8.
209 International Telecommunications Convention, Art. 35.
210 Ibid., Art. 22.

warfare activities do violate ITU regulations, mere violations are more likely to be considered *breaches of contractual obligations* under treaty than *acts of war* justifying forceful responses.[211]

The ***prohibition on unnecessary suffering*** restricts what arsenal is available to a state when it chooses to use force. The principle prohibits the use of weapons designed to cause unnecessary suffering. International Humanitarian Law recognizes that "the rights of belligerents to adopt means of injuring the enemy are not unlimited."[212] As noted in the *Nuclear Weapons Advisory Opinion*, "states do not have unlimited freedom of choice of means in the weapons they use."[213] The International Court of Justice based its finding on the principle that "it is prohibited to use weapons causing them such harm or uselessly aggravating their suffering."[214] This prohibition encourages states to use the appropriate level of force to achieve their military ends. The basic idea is that harm should be no greater than is necessary to achieve legitimate military objectives. Under this principle, indiscriminate weapons, such as biological or chemical weapons, are unlawful. But cyber attacks are often difficult to control, and thus indiscriminate in their effects. A cyber weapon that employs the use of a worm can unintentionally infect millions of computers in its efforts to activate on a single targeted network. But whether the cyber weapon violates the prohibition of unnecessary suffering is often a case-by-case determination that examines all relevant factors. A good rule of thumb is that a cyber attack is unlawful if its consequences are similar to a kinetic attack that violates the prohibition on unnecessary suffering.

Discussions are ongoing on how to classify *state cyber attacks* within an international legal framework. Overall, the *jus ad bellum* question has been addressed: cyberwar occurs when the 'level of damage inflicted is similar to an armed attack.' Exactly what this means, however, still remains a point of contention. As far as cyber *jus in bellum* is concerned, it is increasingly accepted that any cyber attack would have to conform to the major principles of the Law of Armed Conflict and International Humanitarian Law. Cyber attacks should be conducted with a distinction between military and civilian targets, consider the proportionality principle as well as the possibility of secondary and tertiary effects. But what ICT infrastructure could be considered purely civilian and what dual-use still remains subject of vigorous debate. A number of other issues, foremost the responsibility of nation-states to prevent third-party cyber attacks from being carried out from 'their' cyberspace, and particularly by non-state actors, is currently the major issue of discussions. Most Western countries consider that addressing this issue would represent *a principle step in decreasing the potential for interstate cyberwar*.

A different view on how de-escalation can be achieved is advanced by Russia and China. These countries would prefer to talk about state cyber weapons, and to treat

211 Sean P. Kanuck, "Recent Development, Information Warfare: New Challenges for Public International Law," *Harvard Inter-national Law Journal*, 289, 1996.
212 Hague Convention IV, Article 22.
213 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, International Court of Justice Reports, sec. 39, 8 July 1996.
214 Ibid.

these negotiations as an arms-control issue, with treaties banning the 'development and deployment of cyber weapons.' Western nations have traditionally considered such a treaty to be hardly enforceable and open to abuse, and have favored instead the ratification of the Council of Europe Convention on Cybercrime as an important step to limit cyber attacks and state-affiliated cyber espionage. The great increase of cyber espionage attacks against governments in the last years has prompted a compromise position, culminating in deliberations on the 'Rules of Behavior' in Cyberspace.[215] A number of different organizations are now engaged in diplomatic discussions on how this could best be achieved.

The Problem of Deterrence

Cyberwarfare, a great equalizer and like terrorism a new form of asymmetrical warfare, is a tempting option to take. But the problem with the tempting option is that cyber deterrence does not work as well as nuclear deterrence; this already because the *ambiguities of cyber deterrence* contrast starkly with the clarities of nuclear deterrence. It was the incredible power of nuclear weapons that gave birth to deterrence – a strategy in which the purpose of armies shifted from winning wars to preventing them. Nothing compares to the destructive power of nuclear weapons. Nonetheless, cyber attacks loom on the horizon as a threat that is best understood as an extraordinary means to a wide variety of political and military ends, many of which can have serious national security ramifications. For example, computer hacking can be used to steal offensive weapons technologies, including weapons of mass destruction technology. Or it could be used to render adversary defenses inoperable during a conventional military attack.[216] As long as secure passive cyber defense is impossible, deterrence seems the only feasible path. In that light, attempting proactively to *deter cyber attacks* may become an essential part of national strategy. However, deterrence is pointless without attribution. Attribution means knowing who is attacking you, and being able to respond appropriately against the actual place that the attack is originating from.[217] Attribution as it relates to cyber warfare is also defined as "determining the identity or location of an attacker or an attacker's intermediary."[218] In the case of a cyber attack, an attacker's identity may be a name or an account number, and a location may be a physical address or a virtual location such as an IP address.[219] *But if retaliation does not hit the attacker, he will not be deterred.* And it is of legal importance as well. Retaliation against the wrong actor is unjust and a crime of war. Thus attribution is a necessary condition for the law of war. An attacker has to be identified and, to make it an armed attack and not just a criminal act, the attacker has to be a state actor or those acting on behalf of a state.

215 One of these initiatives is currently developed at the NATO CCD COE and entitled "10 Rules of Behavior for Cybersecurity."
216 David A. Fulghum, Robert Wall & Amy Butler, "Cyber-Combat's First Shot," *Aviation Week & Space Technology*, 167, 26 November 2007, pp. 28-31.
217 Dan Morrill, *Cyber Conflict Attribution and the Law*, Toolbox for IT, 7 August 2006, Knowledge Management Blogs.
218 David A. Wheeler & Gregory N. Larsen, *Techniques for Cyber Attack Attribution*. Institute for Defense Analyses, Alexandria, 2007.
219 Ibid.

At the level of the nation-state, there are two possible deterrence strategies: *denial* and *punishment*. Both have three basic requirements: *capability*, *communication*, and *credibility*. But in cyberspace, both strategies suffer from a lack of credibility. *Denial* is unlikely to work due to the ease with which cyber attack technology can be acquired, the immaturity of international legal frameworks, the absence of an inspection regime, and the perception that cyber attacks are not dangerous enough to merit deterrence in the first place. *Punishment* is a real option, but this strategy also lacks credibility due to the daunting challenges of *cyber attack attribution* and *asymmetry.* At a minimum, attribution must improve before a cyber attacker may feel deterred. If cyber attacks can be conducted with impunity, attackers have no reason to stop undertaking attacks.

Deterrence is a state of mind. It is the concept of one state influencing another state to choose *not* to do something that would conflict with the interests of the influencing state. Deterred states decide not to take certain actions because they perceive or fear that such action would produce intolerable consequences.[220] The idea of influencing states' decisions assumes that states are rational actors willing to weigh the perceived costs of an action against the perceived benefits, and to choose a course of action logically based on some "reasonable cost-benefit ratio."[221]

The *efficacy of cyber deterrence* relies on the ability to impose or raise costs, and to deny or lower benefits related to cyber attack in a state's decision making calculus. Credible cyber deterrence is equally dependent on a state's willingness to use these abilities, and a potential aggressor's awareness that these abilities, and the will to use them, exist.

For cyber deterrence to really work effectively, it will have to consist of a comprehensive scheme of *offensive* and *defensive* cyber capabilities, supported by a robust international legal framework. *Offensive capabilities* are the primary tools to impose or raise the costs in deterrence because they provide a state the *means and ways for retaliation*, and enhance the perceived probability that aggressors will pay severely for their actions. The more robust the capability, the more will it translate to a credible imposition of costs. *Defensive capabilities* play an equally critical role in deterring cyber attacks. They not only ensure that essential services and functions of society continue unabated, they also deny or lower the benefits an attacker may obtain via cyber attacks. Defensive cyber capabilities increase a state's resistance to attacks, reduce the consequences, enable the state to strengthen the security of potential targets, and limit or eliminate an aggressor's ability to threaten the state through cyberspace. Ultimately, they reduce the probability of success that an aggressor will achieve his goals.

Over and above offensive and defensive capabilities, a robust *international legal framework* that addresses cyber aggression *is the most critical component of a compre-*

220 Colin S. Gray, "Deterrence and the Nature of Strategy," in *Deterrence in the 21st Century*, Max G. Manwaring, ed., London, Frank Cass, 2001, p. 18.
221 Robert H. Dorff & Joseph R. Cerami, "Deterrence and Competitive Strategies: A New Look at an Old Concept," in *Deterrence in the 21st Century*, Max G. Manwaring, ed., London, Frank Cass, 2001, p. 111.

hensive approach to deterrence. International law and norms are fundamental to deterrence because states share an interest in adopting or codifying common standards for the conduct of international transactions, and in promoting or banning specific kinds of behavior by states.[222] Multilateral agreements provide the most efficient way of realizing these shared interests. The common acceptance of norms moderates state interaction and makes state behavior more predictable, which leads states to combine to insist on respect for specific norms of conduct by those who violate their consensus.[223] In this way, international law builds the framework that guides how and when states employ offensive and defensive cyber capabilities, and forms the foundation of cyber deterrence. It adds certainty to punitive actions and amplifies the costs of cyber attack by engendering a negative response from the international community, not just from the attacked state. Moreover, it adds *credibility* to the *threat of reprisal* by providing legitimacy to retaliatory actions and by increasing the potential to isolate aggressive states. In addition, international law also provides a measure of protection to states that lack defensive and offensive capabilities, and serves as their first and possibly only line of deterrence.

Unfortunately, there is currently "no binding international law on cyber security expressing the common will of countries."[224] In fact, the lack of international norms, laws, and definitions to govern state action in cyberspace has led to a grey area that can be exploited by aggressive states as long as their actions skirt the imprecise thresholds contained in the UN Charter.[225] For example, in response to the accusations of state-sponsored cyberwar against Estonia, the head of the Russian Military Forecasting Centre stated that "the attacks against Estonia had not violated any international agreements because no such agreements exist," suggesting that even if Russia's complicity could be proved, Estonia's options for reprisal were limited.[226] Such an environment thwarts deterrence because it lowers the probability "of reprisal even if the attacker's identity is suspected," and reduces an attacker's potential costs of pursuing cyber attack.[227]

The basic fact is that *deterrence in cyberspace* is undermined by *the problem of accurate attribution of cyber attacks*, which poses problems both for retaliation and law enforcement. The threat of offensive cyber capabilities will not deter aggression because if you cannot identify the perpetrators, you cannot threaten them. And there is no way to enforce the law because unidentifiable perpetrators cannot be held accountable. Likewise, deterrence falters if the UN Security Council cannot identify whom to target with sanctions. With blame being the main problem in cyber attacks, then any quick reaction is excluded. In fact, deterrence is partly based on *reaction speed* or *anticipation*. Either, one acts first to stop the opponents action, or one must be in a position to react before being struck by attacks of the opponent. If days, weeks or months are

222 Charles W. Freeman, *Diplomatic Strategy and Tactics*, Washington D.C., US Institute for Peace, 1997, p. 84..
223 Ibid., p. 38.
224 Ministry of Defence, Estonia, *Cyber Security Strategy*, Tallinn, 2008, p. 17.
225 Eneken Tikk, Kadri Kaska, Kristel Runnimeri, et al, „Georgian Cyber Attacks: Legal Lessons Identified," Tallinn, NATO Co-operative Cyber Defence Centre of Excellence, 2008, p. 7.
226 Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala*, Vol. 8, No. 1, October 2008, p. 51.
227 Tikk et al, op. cit., p. 22.

needed to be sure of the blame, then deterrence as well as dissuasion no longer work.

The key problem with deterrence is that we are still too early in the cyber age to know with any precision how much damage states or other actors can do by cyber attacks on their own or linked to other military attacks. We do not know how good attackers' abilities to ward off retaliation are either. For practicing deterrence, relevant information is lacking about how much damage a potential attacker would consider unacceptable. There is too much secrecy about existing cyber attack capabilities and their survivability for purposes of *retaliation*. The US, China, and Russia are widely perceived to have the best capabilities, but very little is available about how robust they would be after a major attack. Thus, discussions about how a conflict would go, and what it will take to deter, are largely *hypothetical.*

Preemption is equally difficult. It is easy to see troops massing on a border. However, in the digital realm we do not even know all the attacks we have suffered, just those we have managed to discover. Without any tangible basis for an attack, preemption is risky. And if we cannot prove we were about to be attacked, we risk being seen by the international community as the aggressor, not the aggrieved.[228] Finally, given the ability to use wage-ranging diffused networks of enslaved computers to launch an attack, *it is highly unlikely that a preemptive attack would eliminate the threat.*[229]

And there is the *question whether retaliators can hold assets at risk*. While it is possible to understand the target's architecture and test attack software in vivo, one might still not understand how the target will behave or respond under attack. Undiscovered system processes may detect and override errant operations or alert human operators. How long a system malfunctions, and thus how costly the attack is, will depend on how well its systems administrators understand what went wrong and can respond to the problem.[230] Moreover, there is no guarantee that attackers will have assets that can be put at risk through cyberspace.

As to the *questions whether cyber attacks can disarm cyber attackers*, and whether the vexing *challenge of escalation* can be avoided: the answers to both are clearly no. In a world of cheap computing, ubiquitous networking, and hackers who could be anywhere, *disarming cyber attackers is not possible*. Equally impossible is *avoidance of escalation*. Even if retaliation is in kind, counterretaliation may not be. This means that a fight that begins in cyberspace may result in spill-over into the real world, possibly with grievous consequences."[231]

Responses to cyber attacks must weigh many factors since, in many ways, *cyberwar is the manipulation of ambiguity*. Not only do successful cyber attacks threaten the credibility of untouched systems (who knows that they have not been corrupted?), but the entire enterprise is beset with ambiguities. Questions arise in cyberspace that

228 Eugene E. Habiger, *Cyberwarfare and Cyberterrorism*, White Paper, The Cyber Secure Institute, 1 February 2010, p. 3.
229 Cyberwar and Cyberdeterrence, op cit., p. xvii.
230 Ibid., p. xviii.
231 Ibid., p. xvii.

have few counterparts in other media. What was the attacker trying to achieve? What should the target reveal about the attack? How should states respond to freelance attacks? And should deterrence be extended to allies?[232]

Advantages and Risks of the most recent Military Innovation: Networked Forces

Today, "Bombs are guided by GPS satellites; drones are piloted remotely from across the world; fighter planes and warships are now huge data-processing centers; even the ordinary foot-soldier is being wired up."[233] With this wiring up, the Internet has enabled the most recent military innovation: *networked forces*. A networked force enables the expansion, acceleration, and qualitative improvement of command and control, and helps to improve situational awareness that can reduce uncertainty. It may change the way how wars are fought. A networked force is more effective than a non-networked one of comparable size. Networked air defense is much more combat effective than an aggregation of individual air-defense units. Ships, aircraft, and fighting vehicles connected by data links hold the promise to fight more effectively than non-networked units who rely solely on radio/voice communications. This increase in effectiveness makes military networks clearly a valuable and legitimate target for attack.

The use of network technologies and exploitation of cyberspace for intelligence collection, surveillance, reconnaissance, targeting, and attack has become a normal part of military activity. Cyberwarfare aims at disruption of crucial network services and data, damage to critical infrastructure, and *creation of uncertainty* and *doubt* among opposing commanders and political leaders. Cyber attacks can be directed at targets over very long strike distances using relatively inexpensive tools. However, cyber attacks seem generally not very likely to be decisive in the sense that the engagement of strategic weapons or a main force conventional attack can be. No one will likely win a victory or war using *only cyber attacks*.[234] But cyber attacks do offer *advantages*. And cyber attacks will certainly be part of future military conflict since "We know with a sad certainty that war has a healthy future. What we do not know with confidence are the forms that warfare will take."[235]

The amount of advantage provided by cyber attack will depend in part on the scope and length of a conflict. Cyber attacks may well be more valuable in short conflicts. In a conflict limited in time and scope, the disruption created by cyber attacks in services and logistics may provide an initial advantage. But the longer the conflict lasts, the probability increases that the utility of this advantage will decline as an opponent adjusts. In contrast, attacks against command and control, such as those

232 Ibid., p. xviii.
233 "Cyberwar: War in the fifth domain." *The Economist*, 1 July 2010, at: http://www.economist.com/sites/default/files/images/images-magazine/2010/27/fb/201027fbd001.jpg
234 Libicki dixit.
235 Colin Gray, *Another Bloody Century*, London, Weidenfeld & Nicolson, 2005, p. 24.

that disrupt data and undermine confidence in the own information, could have a sustained cumulative effect, and increasingly hamper an opponent's ability to resist. Cyber attacks thus introduce a *new dimension in the ability to create uncertainty* in the mind of opposing commanders. Uncertainty does not only create a large part of what Clausewitz called the 'fog and friction of war': it slows decision making, amplifies caution and timidity, and increases the chance of errors. Misleading an opposing commander has always been part of warfare. But cyber attacks provide a new and more intimate capacity to undertake this, and potentially offer a significant advantage for *deception*, and thus for *undermining confidence*.

A similar kind of *uncertainty and indecision* can be produced by *manipulation of data* in a cyber attack. Beyond scrambling data to deny an opponent access to it, a more difficult and damaging attack consists of manipulating data in order to make it misleading or incorrect. A cyber exploit that surreptitiously manipulated data in ways unfavorable to the opposing commander provides new promises for cyber conflict. In addition, it also provides possibilities to sabotage targeting and weapon systems, to take over control of missiles, Unmanned Aerial Vehicles (UAV),[236] robots, and radars, or to mislead or disrupt the controls even of jet fighters. Data manipulation could also create havoc with *operational planning*. And it is not hard to imagine cyber attacks that effectively interfere with logistics plans and chains: by giving false locations of depots, by rerouting supplies or making it appear that there are shortages or surpluses when the opposite is the case.[237]

Weapon systems are ever more dependent on software, computer hardware, and battlespace networking. While the security of these weapon systems advances in step with the development and implementation of cyber technology, they can be increasingly affected by cyber attacks. Aircraft are a good example. In the past, 100 percent of an aircraft's performance and capabilities were defined by hardware – the physical makeup of the aircraft. In more recent advanced aircraft, 75 percent or more of its performance and capability is dependent on software. Without software, some aircraft would not be controllable. For instance, the F-16 is unstable below Mach one, and uncontrollable without its software-based flight control system. The Boeing 777 and the Airbus 330 have software flight control systems without any manual backup. Through software, aircraft performance is gaining some independence from physical configuration, and therefore *software dependence* and *hardware independence* are growing. But even fifth generation multirole fighters like the F-22 and F-35 are not closed systems; external information systems can update and integrate information for combat operations during the flight. Through these external connections, not just the information systems, but the basic software and hardware systems of these fighters can be attacked.[238] Vulnerabilities increase in proportion of the number of code

236 Already in 2009, Iraqi insurgents, using off-the-shelf software costing $26, hacked into downlinks of US UAVs costing $4.5 million each in order to monitor their video feeds. Siobhan Gorman, Yochi J. Dreazen & August Cole, "Insurgents Hack US Drones," *Wall Street Journal*, 17 December 2009. The Israeli Air Force is now equipping all its UAVs with encrypted communications to prevent video monitoring by Hezbollah and Hamas.
237 *On Cyber Warfare*, op. cit., p.13.
238 Lionel D. Alford, "Cyber Warfare: The Threat to Weapon Systems," *The WSTIAC Quarterly*, Vol. 9, No. 4, 2010.

lines deployed.[239]

The doctrine of *network-centric warfare*, a cornerstone in the ongoing transformation efforts of a number of Western armed forces, seeks to translate an information advantage, enabled in part by IT, into a competitive advantage through the *robust networking* of well informed geographically dispersed forces.[240] It draws its guidance from the concept of *team warfare*, and the *integration* and *synchronization* of all appropriate capabilities across the various services, which is part of *the principle of joint warfare*. This networking, combined with changes in technology, organization, processes, and people, may allow new forms of organizational behavior. Specifically, the theory of network-centric warfare contains the following tenets: (1) A robustly networked force improves information sharing; (2) Information sharing and collaboration enhance the quality of information and shared situational awareness; (3) Shared situational awareness enables self-synchronization; and (4) these, in turn, dramatically increase mission effectiveness. There is no doubt that the effectiveness of network-centric warfare has greatly improved. US forces engaged in *Operation Desert Storm*, involving more than 500,000 troops, were supported with 100 Mbit/s of bandwidth. The forces in *Operation Iraqi Freedom*, with some 350,000 warfighters, had more than 3'000 Mbit/s of satellite bandwidth, which is 30 times more bandwidth for a force 45 percent smaller. US troops essentially used the same weapon platforms used in *Operation Desert Storm* but with significantly increased effectiveness.[241] And good C4ISTAR systems are at the heart of successful military operations.[242]

However, in view of the many architectural and design challenges, it is not yet clear whether the vision of network-centric warfare is soon realizable. Since network-centric warfare focuses so much on distributed information, the armed forces must be wary of the effects of false, misleading, or misinterpreted information entering the system, be it through enemy deception or simple error. Just as the usefulness of *correct information can be amplified, so can the repercussions of incorrect data entering the system achieve much greater non-positive outcomes*. In addition to this, there are potential issues arising from the very nature of any complex, rapidly-developed artificial systems arising from *complexity theory*, which implies the possibility of failure modes such as congestion collapse or cascading failure.

239 Joseph Henrotin estimates that the software of the F-22 counts around 2 million lines of code, versus 8 million for the F-35. See: "Intelligence, the First Defense? Information Warfare and Strategic Surprise," in *Cyberwar and Information Warfare*, Daniel Ventre, ed., op. cit., footnote p. 104.
240 Department of Defense, *The Implementation of Network-Centric Warfare*, Washington D.C., 2005, p. 7.
241 Lt Gen Harry D. Raduege Jr., "Net-Centric Warfare is Changing the Battlefield Environment," Defense Information Systems Agency, *CrossTalk The Journal of Defense Software Engineering*, January 2004, and Deloitte LLP, "An interview with Harry D. Raduege, Jr., Chairman, Deloitte Center for Cyber Innovation," July 2011.
242 *Visiongain* calculated that in 2011 the global market for C2/C4ISR systems will amount to $70.3 billion, which constitutes 5 percent of global defense spending. See: *The C2/C4ISR Systems Market 2011-2021 Defense Report*, London, 21 January 2011.

Categorizing Cyber Conflicts according to their Scope, Intensity, and Impact on War

Cyber attacks have *tactical*, *operational*, and *strategic* applications. They can be used against *deployed forces* or against *strategic targets* in an opponent's homeland, for instance, against those that contribute to the ability to wage war. Their range is practically unlimited, and targets can be attacked anywhere the global network extends. Cyber attacks have a variety of delivery options: over *networks* or from *dedicated ground*, *sea*, *air*, and *space* platforms. The tools are relatively cheap. But cyber attacks may become more expensive as they depend ever more *on time and effort for reconnaissance of network targets to find vulnerabilities*. And this reconnaissance must be periodically refreshed as networks change and new equipment or software is added or reconfigured. While the preparation for a cyber attack may be lengthy, the speed of the actual attack is measured in seconds irrespective of the distance from the target. And *surprise* and *stealth* are normal attributes of cyber attacks.[243]

Different levels of cyberwar can be imagined, of which three stand out: (1) cyberwar as an *adjunct to military operations*; (2) *limited cyberwar*; and (3) *unrestricted cyberwar*. When modern armed forces are involved in military hostilities, a key objective is to achieve information superiority or information dominance in the battlespace. This requires suppressing enemy air defenses, jamming or destroying radar, and the like. The aim is to increase the 'fog of war' for the enemy and to reduce it for one's own forces. This can be achieved through strikes and attacks designed to degrade the enemy's information-processing systems, communications and C4ISTAR systems, or by attacking the systems internally to achieve, not denial of service, but denial of capability.[244] In effect, this form of cyberwarfare can be focused almost exclusively on military cyber targets.

In *limited cyberwar*, the information infrastructure is the medium, target, and weapon of attack, with little or no real-world action accompanying the attack. As a medium of attack, the information infrastructure forms the vector by which the cyber attack is delivered to the target – sometimes through interconnections between the enemy and its allies, using links for sharing resources or data, or through wide-area network connections.[245] Alternatively, insiders might place malware directly on the opponent's networks or IT systems.

As a target of attack, infrastructures are the means by which the effectiveness of the enemy force can be reduced. "Networks facilitate organizational missions. Degrading network capacity inhibits or prevents operations that depend on the network. Degrading the level of service on the network could force the enemy to resort to backup

243 Surprise due to the speed of attack, which is close to the speed of light, and because of the fact that cyberattacks theoretically can impact the entire spectrum of the cyberspace domain simultaneously. Stealth because the weapons and effects are unknown.
244 Thimothy Shimeall, Phil Williams & Casey Dunlevy, "Countering cyber war," *NATO Review*, Vol. 49, No. 4, Winter 2001/02, p.17.
245 Idem.

means for some operations, which might expose additional vulnerabilities."[246] In addition, degrading data on a network might force the enemy to question the quality of the information to make decisions. And as the weapon of attack, infrastructures could even be perverted to attack themselves, either via implantation of multiple pieces of malware, or via deliberate actions that exploit existing weaknesses. *Limited cyberwar* could either be used to slow an opponent's preparation for military intervention, as part of an economic warfare campaign, or as part of the maneuvering that typically accompanies a crisis or confrontation between states.

Unrestricted cyberwar would certainly be more serious, since it is a form of warfare that has three major characteristics: (1) It is comprehensive in scope and target coverage, with little or no distinctions between military and civilian targets or between the home front and the fighting front. (2) Unrestricted cyberwar can have physical consequences and may cause casualties, some of which would result from attacks deliberately intend to create mayhem and destruction. And some of which would result from the erosion of civilian command and control capabilities in areas such as air-traffic control, emergency-service management, water resource management, and power generation. (3) The economic and social impact could be profound, in addition to damage and loss of life.[247] Ultimately, unrestricted cyberwar may have the potential to result in economic and social degradation of a state. The great unknown and thus danger of unrestricted cyberwar is the unintended secondary and tertiary consequences an attack may have on uninvolved third parties, or even for the attacker.

Cyber attacks on hospitals, for example, could produce casualties by manipulating data, through erasing, replacing, or adding ones and zeros; by changing prescriptions or turning off life-support and other critical systems; by causing radiation overdose, etc. While terrorists may find such attacks attractive, for states they would be a violation of the laws of war. Moreover, putting non-combatants in harm's way is not likely to produce a military advantage. But an opponent still might do it. Attacks on critical national infrastructures, for example the electric power grid, might also disrupt medical services and produce casualties, but would not necessarily be contrary to the laws of war if there would have been some prior considerations as to whether the value of the target outweighed the risk of non-combatant casualties. This fact alone might constitute an additional reason calling for adaptation of the Geneva Conventions.

To effectively manage a cyber conflict, it may have to be categorized into various levels of intensity. A *low intensity cyber conflict* involves the legitimate use of cyber resources to undermine the adversary. Examples are psychological or information warfare, a usual preamble of an armed conflict. A *medium intensity cyber conflict* comprises low intensity conflict and sporadic *cyber attacks*, as well as intrusions to gather intelligence or to harass or destabilize the adversary. A high *intensity cyber conflict* consists of conflicts of low and medium intensity, plus cyber attacks resulting in the

246 Idem.
247 Idem.

destruction or damage to infrastructure, injuries and even the loss of human lives.[248]

Critical national infrastructures are normal targets for military planners with the mission of gaining a strategic advantage. Soviet and Warsaw Pact planning of the strategic offensive against Western Europe targeted air bases, telecommunications services, fuel pipelines, electric power grids, transportation hubs, and government centers. Disabling these targets, combined with preemptive assaults on bridges, tunnels, and harbors, would have contributed to the speed and success of the offensive.[249] Cyber attacks could potentially produce the same disruptions, and possibly at lesser cost to any later occupation force. This is different from strategic attacks against manufacturing or other critical infrastructures where the intent is not to gain immediate operational advantage, but to benefit from the *degradation of the opponent's capacity for sustained resistance.* In this erosion of the capability to resist, the utility of cyber attacks may be open to question. But the ability to interfere with communications and logistics for operational or tactical advantage is not. Thus, for a number of conflict scenarios, an opponent could reasonably be expected to use cyber attacks to interfere with efforts to move, deploy, and supply forces.

On the still unresolved Problem of Destructiveness of Cyber Attacks

Compared to some other weapons, cyber attacks seem not likely to be very destructive. Such attacks have difficulties to produce a lot of casualties, and the possibility of causing damage, destruction, and death with cyber attacks seems rather low.[250] In its physical consequences a cyber attack is more like sabotage carried out by guerillas or Special Forces. For all practical purposes a cyber weapon is intangible: tiny electrical pulses whose lethality comes not from their own innate destructive capacity, but from the ability to instruct other tangible systems to malfunction.[251] Given their limited capacity for damage, successful cyber attacks may thus depend more on speed and surprise to achieve an optimal effect.

As to the *kinetic effect of cyber weapons*, however, cyber attacks have a certain ability to inflict *physical damage.* Evidence is the Aurora test at the American Idaho National Laboratories, where a remotely transmitted command of a 21-line software code caused a 27 tons $1 million diesel-electric generator to self-destruct.[252] And to destroy a refinery, a code can be sent that causes crucial components to overheat. The first thing is to turn the system to manual controls to avoid protection by automatic

248 Ahmad Ghazali Abu-Hassan, *Managing Cyber Conflict*, Cyber Security Malaysia Awards, Conference and Exhibition, Kuala Lumpur Convention Centre, 25-29 October 2010,
249 Phillip A. Petersen & John G. Hines, "The Soviet Conventional Offensive in Europe," *Defense Intelligence Report DDB-2622-4-83,* May 1983, and "The Conventional Offensive in Soviet Theater Strategy," *Current News*, Special Edition, Department of Defense, 12 April 1984. Also: *Employment of Warsaw Pact Forces Against NATO*, Director of Central Intelligence, Interagency Memorandum NI IIM 83-10002, 1 April 1983. Phillip A. Petersen & Notra Trulock III, "Soviet Views and Policies toward Theater War in Europe," in *The USSR and the Western Alliance,* edited by Robbin F. Laird & Susan L. Clark, Boston, Unwin Hyman, 1989.
250 Cyberdeterrence and Cyberwar, op. cit., p. xv.
251 James A. Lewis, *Thresholds for Cyberwar*, Center for Strategic and International Studies, September 2010, p. 3.
252 See: *The Aurora Power Grid Vulnerability*, A White Paper, at: http://unix.nocdesigns.com/aurora_white_paper.htm.

controls. The main targets would be the heating element and the recirculation pump. If both malfunction, an explosion is caused.[253] There are also examples where accidental programming errors produced physical damage.[254]

There is also the possibility of potentially catastrophic single cyber-related events, the occurrence of which cannot be fully excluded. One includes a successful attack on one of the underlying technical protocols upon which the Internet depends, such as the *Border Gateway Protocol*, which determines routing between Internet Service Providers.[255] Another could be a very large-scale solar flare which physically destroys key communications components such as satellites, cellular base stations, and switches.[256] Such catastrophic single cyber-related events, as well as conventional or natural catastrophes, bear the danger that the supportive information infrastructures become overloaded, crash, and inhibit recovery. But the cyber infrastructure, while providing a potential vector for propagating and magnifying an original triggering event, may also be the means of mitigating the effects. If appropriate contingency plans are in place, information systems can support the management of other systemic risks. They can provide alternate means of delivering essential services, disseminating the latest news and advice on catastrophic events, reassuring citizens and hence dampening the potential for social discontent and unrest – since from the public's point of view, the absence of a clear government response may trigger panic if there appears to be no route back to normalcy.

On the Effects Newest Malware might have on the Mode of Future Conflicts

There is the recent Stuxnet worm, the arrival of which was a watershed in the security world.[257] Some consider it to be the most sophisticated malware ever publicly disclosed. Stuxnet contains malware aimed at the programmable logic controllers (PLCs), designed to destroy SCADA networks: those that run factories, the electric power grid, refineries, pipelines, utilities, and nuclear power plants.[258] Most industrial systems are run on computers which use Microsoft's Windows 7 operating system. Hackers constantly probe software for what are known as *zero day* vulnerabilities: weak points in the code never foreseen by the original programmers. On a sophisticated and ubiquitous piece of software such as Windows XP, which counts around

253 See: http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml
254 Accidental threats relate to errors and omissions. Errors may sometimes be a threat (for example, programming error causing system to crash) or may create vulnerability (for example, a computer screen left unattended may be exploited by an unauthorized user). These threats can result in incorrect decisions being made, disruption of business functions, loss of public confidence or image, financial loss, legal liabilities and breakdown of duty of care, all with additional costs being incurred.
255 However, there is also what CERN in Geneva is doing, which could again change the world. In a decade, we may see an entirely different, vastly more powerful, faster, and more internationally distributed network. The Grid, designed for computational support of CERN's ambitious search for the Higgs boson, among other quantum theoretical particles, could make current cyberwarfare concerns either quaint or obsolete. Hopefully the latter.
256 "Reducing Systemic Cybersecurity Risk," op. cit., p. 5.
257 James P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival,* Vol. 53, No. 1, February-March 2011.
258 "Les attaques cybernétiques contre l'Iran ont commencé, " *Le Temps*, 25 Novembre 2010, p. 5.

35 million lines of code, discovering even a single *zero day* vulnerability is extremely uncommon. The makers of Stuxnet found, and utilized, four of them. No one in cyber security had ever seen anything like it. It targeted a specific component: the frequency converters made by the German equipment manufacturer Siemens that regulate the speed of the many thousands of spinning centrifuges used in the Iranian uranium enrichment process. The worm then took control of the speed at which the centrifuges spun, making them turn so fast in a quick burst that they would be damaged but not totally destroyed. At the same time, the worm masked that change in speed from being discovered at the control panel – with a rootkit piece of code that intercepts security queries and sends back false 'safe' messages, indicating that the worm is innocuous.

The *New York Times* published an article 25 January 2011, detailing the cooperation between the US and Israel in developing the Stuxnet worm. Creating it involved three major components, which require major state resources: technical intelligence on the technology used in Iran's nuclear facilities; programming and testing capabilities; and human access to the facilities. The report only details some of the first and second components.[259] The worm is said to have gained initial access to a system through a 'blue rubber-clad swivel-style USB drive.' In a rare moment of openness from Iran, its president confirmed on 29 November 2010 that the centrifuges had been damaged by Stuxnet. And the Busher nuclear power plant that was scheduled to go operational on 21 August 2010 did not. If Stuxnet managed to severely damage the steam turbine in the Busher plant, repairing or replacing it may cost a significant amount of money – up to several million dollars. Presently, it looks like more than 5,084 out of 8,856 centrifuges have been taken offline at the Natanz facility, with unknown damage in Fordow and other centrifuge plants.[260] All this translates to another multi-million dollar damage.[261]

According to David Sanger from the New York Times, an Israeli military official had estimated that an air strike against the Iranian nuclear program would cause a delay of two or three years. So it looks like Stuxnet achieved pretty much what air strikes would have achieved, only at much less cost, without known fatalities, and without a full-blown war in the Middle East. It seems to have been successful in temporarily disabling the epicenter of Iranian nuclear research. A sophisticated half-megabyte of computer code apparently accomplished what a half-decade of UN Security Council resolutions could not. The cost of development of Stuxnet has been estimated to be around $10 million. The cost of air strikes would have been multiple, only counting material, not fatalities and injuries. Assuming that only one fighter jet would have been lost in a military campaign against Iran is certainly naïve; there would have been several. And there would have been many dead and many injured, significant destruction by Iranian missiles fired in retaliation and a huge amount of collateral damage just by the oil price jumping. All this did not happen with Stuxnet. Thus, in military terms, it was a bargain. If the alternative is conventional military strikes with

259 See: "The US-Israeli Stuxnet Alliance," Austin, *STRATFOR Global Intelligence*, 17 January 2011.
260 Michael Martine, "Bits before bombs: How Stuxnet crippled Iran's nuclear dreams," *Sapphire*, 3 December 2010.
261 Ralph Lagner, *The Short Path from Cyber Missiles to Dirty Digital Bombs*, Travis, politicalforum, 26 December 2010.

explosives or maybe even weapons of mass destruction, cyber strikes might be the better deal, not only for the attacker, but especially for the attacked.[262]

Hence, Stuxnet may represent the opening of a new chapter in the use of cyberspace to achieve the strategic effect of neutralizing a potent international threat, suggesting that cyber attacks can be seen as another long-range strike weapon – faster than missiles or aircraft, not as destructive, but cheaper and possibly covert.[263] This sophisticated SCADA attack, now seen as a 'game changer,' demonstrated the potential of future cyber attacks and cyberwarfare.[264] It is also an excellent example demonstrating that political and strategic effect can be achieved without the need for armed conflict.

Stuxnet has shown that the strategic utility of cyber weapons is their ability to disrupt, deny, and deceive an adversary's strategic intentions. While it certainly damaged the Iranian program and confused its technicians, the attack's overall effect seems to have been less impressive. Iran has replaced all of its damaged centrifuges and has resumed enriching uranium. This is significant, as it suggests that cyber-weapons are not the 'silver bullet' replacement for more-traditional military instruments that they have been purported to be. It has not coerced the Iranian regime into abandoning that program. Stuxnet also shows that effective cyber attacks require large, complex operations, and entail a massive intelligence burden. It now seems that the Iranian nuclear facilities are under a renewed attack with a worm called 'Stars,'[265] and more recently with a Trojan called 'Duqu.'[266]

There are clear limitations and disadvantages of such attacks, however. This, not least brought about by the porous borders of cyberspace, which, as exemplified in the case of Stuxnet, led to the infection of thousands of additional computers both in Iran and beyond.[267] As of yet, there exists no ascertained ability to estimate or forecast the scope of unintended consequences and collateral damage of cyber attacks. For attacks that disable networks, there could be unpredictable damage not only to the target, but also to non-combatants, neutrals, allies, or even the attacker, depending on the interconnections of the target network or the systems attacked. This makes the political risk of collateral damage and unintended second and third order consequences unpredictable, and carries with it the risk of escalating a conflict.

262 Ibid., at: http://www.mail-archive.com/politicalforum@googlegroups.com/msg65062.html
263 If Stuxnet was aimed specifically at the Iranian nuclear reactor in Busher or the Natanz uranium enrichment plant, it exhibited one of the weaknesses of cyber attacks: they are difficult to target and also to contain. India and China were reportedly harder hit than Iran, and the worm could easily have spread in a different direction, and may have even hit the originator. Hence, the very openness of the Internet serves as a deterrent against the use of cyber weapons.
264 Paul K. Kerr, John Rollins & Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, Washington D.C., CRS Report for Congress, Congressional Research Service, 7-5700, R41524, 9 December 2010. And: Richard Adhikari, "Stuxnet Suspicions Rise: Has a Cyberwar Started?," *TecNewsWorld*, 4 November 2010.
265 Serge Dumont, "Comment Israël déstabilise ses ennemies? Par ses usines à virus, Israël renforce sa cyberguerre contre l'Iran," *Le Temps*, 28 avril 2011, pp. 1 & 6.
266 "Iran says it has 'controlled' Duqu malware attack," *BBC News Technology*, 14 November 2011.
267 "A worm in the centrifuge," *The Economist*, 2 October 2010. And: "The meaning of Stuxnet," *The Economist*, 30 September 2010.

While strikes on deployed forces may create unease and concern over potential escalation, striking civilian targets and critical national infrastructures in an opponent's homeland will likely be considered a major escalation of conflict. The reaction of the enemy's leadership to attacks on civilian targets could be pronounced. Even if an attack may be intended to be limited, the opponent may not perceive or believe the limitation. Uncertainties about the scope of collateral damage, and problems with attribution of an attack with sufficient certainty, create political risk for a decision to use cyber attacks. For an attacker as well as for a retaliator, unintended consequences and unexpected collateral damage could weaken international support, produce negative domestic reactions, and stiffen resistance in the target country.

And there is another problem. Cyber weapons can be copied and their proliferation cannot be controlled. Stuxnet-inspired weapons and technology may soon be in the hands of rogue nation-states, terrorists, organized crime, and hackers. And these weapons may soon look different from the original. Stuxnet was precisely designed for surgical attacks on distinct targets. But there is no reason to assume that follow-up attackers will follow the same philosophy. It is much more likely that we are going to see 'dirty' digital bombs in the wake of Stuxnet, which is a cyber weapon that inflicts low to medium damage to a large number of random targets. And to make these weapons does not require experts.

The governance problem

A more important problem is that in all states both the decision making apparatus for cyber attack and the oversight mechanisms for it are inadequate today. Cyber attack is a relatively new addition to the menu of options that policymakers may exercise, and there are few precedents and hardly any history to guide them. The infrastructure and resources needed to conduct such activities, and the activities themselves, are by their nature less visible than those associated with more traditional military, intelligence, or law enforcement activities. Nor do they fit into standard categories. The weapons may initially act in a non-lethal manner, though they subsequently may well have destructive or lethal effects. The activities for which they are suited go far beyond surveillance or covert action. Moreover, the weapons are shrouded in secrecy. In most cases, budgets to acquire cyber attack capabilities are likely small compared to budgets for major acquisition programs of conventional weapons.[268] The technical knowledge needed to conduct informed oversight is limited. The importance of cyber attack as a possible option for policymakers is not widely appreciated. And procedures for informing potentially relevant policymakers in both the executive and the legislative branches appear to be minimal or non-existent.

With all these factors in play, an adequate organizational structure for decision making and exercising oversight has yet to emerge, and much of the information

268 In the US, for example, a major defense acquisition program is one designated as such by the Secretary of Defense and estimated to require a total expenditure for research, development, test, and evaluation of more than $300,000,000 or a total expenditure for procurement of more than $1,800,000,000 (based on fiscal year 1990 constant dollars).

relevant to conducting informed oversight is unavailable. As a result, government and society at large are neither organized nor in any way prepared to think about the implications of cyber attack as an instrument of national policy, let alone to make informed decisions about them. In addition, a major element missing and conspicuous in its absence is the role Parliament should play in decisions related to cyber attacks. Thus, resulting is a governance problem that needs to be solved.

In sum

- Cyber threats pose critical national and economic security concerns due to the rapid advances in, and increasing dependency on, ICT that is underpinning ever more aspects of modern society and life. Data collection, processing, storage, and transmission capabilities are growing exponentially, and mobile, wireless, and cloud computing bring the full power of the globally-connected Internet to myriad personal devices and critical infrastructures. Because of market incentives, innovation in functionality is outpacing innovation in cyber security. And neither the public nor the private sector has been successful at fully implementing existing best practices.

- The impact of this evolution can be seen not only in the increasing scope of cyber security incidents, but also in the expanding range of actors and targets. Breadth and sophistication of computer network operations by both state and non-state actors have increased markedly in the last years. However, by far not all such cyber security incidents qualify as cyber attacks. Cyber attack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems and networks.

- Cyberspace operations for the most part do not meet the criteria for 'use of force' or 'act of war' as currently defined by international law.[269] However, the issues raised by the acquisition and use of cyber attack capabilities are significant across a broad range of conflict scenarios, from small skirmishes with minor actors to all-out conflicts with major adversaries, a few of which may even be capable of employing weapons of mass destruction.

- The availability of cyber attack technologies for national purposes greatly expands the range of options available to national policymakers as well as those of other countries. However, it also means that their use may sometimes result in unanticipated, unforeseen, or unintended consequences.

- The consequences of a cyber attack may be both direct and indirect, and in some cases of interest, the indirect consequences can far outweigh the direct consequences. Direct or immediate effects are those on IT systems or networks attacked.

269 Notions related to 'use of force' and 'armed attack' should be judged primarily by the effects of an action rather than its modality.

Indirect or follow-on effects are those on the systems and/or devices that the attacked IT system or network controls or interacts with, or on the people that use or rely on those.

- States which are highly dependent on the capabilities afforded by ubiquitous ICT in every sector, both military and civilian, have much to lose from unrestrained cyber attacks that proliferate worldwide. And for many IT infrastructure targets, the ease of cyber attack is increasing rather than decreasing. There is, therefore, room to explore an arms limitation approach to cyber security (including options for confidence and security-building measures). A priority would be to ensure that IHL is also observed in the cyber dimension of war.

- While doubts remain as to whether strategic cyberwar is feasible, it is unlikely that a war would be fought only with cyber weapons and purely within the cyber domain. The use of cyber capabilities in conjunction with a conventional military campaign seems to be the most likely feature of future warfare between states.[270]

- Like earlier technological innovations, these will be used to degrade enemy capabilities and to shape the battlespace, and perhaps reshape the ways wars will be fought.

Some of the issues, ambiguities, and problems identified will not be resolved until further and direct experience in cyberwar can be gained. In the interim, war games, simulation, and cyber security, cyber defense, and cyber attack exercises could provide more insights. Dialogue with allies and with potential opponents could help to clarify issues, ambiguities, and problems, and thus eventually also reduce the chances of miscalculation or misperception.

270 *On Cyber Warfare*, op. cit, p. 6.

Annex 1: In which Ways is Cyberwar different from the other Warfighting Domains?

Intrinsic Characteristics as a Unique Combat Domain

The advent of cyberwar brought the *emergence of cyberspace as a new domain of combat*, which, as such, is an exceedingly rare event. But in addition, cyberspace brought also new features that make it a *unique combat domain* with *five* critical distinguishing characteristics. *First*, cyberspace has become a 'global commons' *existing almost everywhere* and *open to anyone*, allowing users to move across it with ease and ever-increasing speeds. Because it is open to anyone, intruders can almost always gain access to a vulnerable system or network to exploit. And once in, they can be difficult to detect and to dislodge.[271] The *second* critical characteristic is that cyberspace provides a *greatly extended battlespace* with no real boundaries since real-world barriers have no counterparts in cyberspace. Nor would electronic barriers offer sanctuary. While defenders can and should build electronic 'firewalls,' such defenses can, in one way or another, be breached or bypassed. The *third* critical characteristic is that ICT has *demolished time and distance* in that greatly extended battlespace, which is no longer of a conventional type because it consists of the *convergence of technologies* and *infrastructures.* In this new domain of operations, *time* is more compressed than the fastest-moving kinetic capabilities. Because the Internet's reach renders physical distance largely irrelevant, intrusions and break-ins come at such high pace and speed that the own cyber defense forces have only seconds to respond. And this leads to the *fourth* critical characteristic: *cyberspace favors the attacker*. With no boundaries, attacks can come from anywhere. Ubiquitous access makes establishing a defense especially difficult because defenders must successfully parry every blow and must be always right, while the attacker must be right only once, and rarely has to face the consequences of his actions. Hackers can penetrate all network defenses at nominal cost compared to the great expenses for creating and maintaining network security. Moreover, cyberspace has yet to undergo any technological or organizational revolution that changes the dominance and inherent imbalance of offensive cyberwar, which today still continues to outpace defense. Finally, the *fifth* critical characteristic is the *kaleidoscopic change of the components of cyberspace*, which are under constant transformation through changes in usage and technology. These components are constantly being created, updated, moved or physically relocated, destroyed, lost, connected and disconnected, hidden and exposed. This is due partly to the pace of

271 The proliferation of wireless handheld devices that connect to the Internet opens millions of additional paths to cyberspace. The rapid pace of app development for mobile devices may accelerate the birth rate of software vulnerabilities. And techniques to exploit these vulnerabilities evolve just as rapidly.

innovation of ICT in general, which, in turn, drives the evolution of cyberspace. New products are appearing daily and receive regular updates. Because of this kaleidoscopic change, threats and vulnerabilities in cyberspace differ from those in the world of conventional combat.[272]

The upshot of the inherent nature of cyberspace is that, compared with the other warfighting domains, cyberspace constitutes a more difficult environment for security actors, one that is particularly difficult to defend. From a defensive perspective, it is difficult to defend a space that exists virtually everywhere, that lets anyone in, and that has no boundaries. Even so-called closed networks, such as those that are not connected to the Internet and those that are air-gapped, are still at risk from manual insertion of malware, for example, by means of portable storage devices, or by wireless code insertion transmitted over radio or radar frequencies.[273] And because the range of hostile or malicious action is much broader in cyberspace than in the other warfighting domains, and the identity of those who engage in these actions can be indeterminate, cyberspace has become the "wild west of the global commons."[274]

On the other hand, in terms of relevance to warfighting, the characteristics of cyberspace allow the own forces a broader span of effects, more precision, greater stealth, lower probability of detection, and a level of nonattribution not possible in other domains.

***Broader span of effects*:** Cyberspace offers the potential for nearly imperceptible system effects all the way through massive electronic means of *mass disruption*. As networked computer chips reach deeper into the devices that are used in daily life, the capacity to make minute changes in these systems offers the possibility of manipulating the perceptions of those they serve. These capabilities could be used, for example, to interrupt command and control of the armed forces, or to block communications to a terrorist leader at a critical moment in his operations, causing disarray, failure of an imminent attack, fomentation of mistrust and division among his supporters under the right conditions. Another strength of the cyber realm is the ability to achieve effects in some cases comparable to some kinetically generated effects but without or less international political and legal pitfalls.

***More precision*:** The cyber realm brings new meaning to precision. The precision inherent in cyber attacks goes beyond the ability to address specific targets. The cyber realm is capable of imposing effects upon certain characteristics or parts of targets. Everything from cutting off communications to feeding bad timing or location information to an adversary can manipulate the outcome of his operations and bring real tactical, operational, and even strategic advantage to the own forces. Depending

272 According to Shon Harris, a threat is a "potential danger to information systems," while a vulnerability is "a software, hardware, or procedural weakness that may provide an attacker an open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment." See: Shon Harris, *CISSP Exam Guide*, 4th ed., New York, McGraw-Hill, 2008, p. 61.

273 Clarke & Knake, op. cit., p. 7. And: David A. Fulghum, "Searching for Ways to Trace Cyber Attackers," *Aviation Week and Space Technology*, 20 May 2011.

274 Atlantic Council, *Protecting the global commons*, Dolce La Hulpe, Brussels, Security and Defense Agenda, SDA Report, 16 September 2010, p. 8.

on the circumstances, cyber capabilities can be used to produce effects such as delaying or even stopping an invasion, for example, by remotely immobilizing lead armored vehicles of a force on a bridge, thus thwarting the passage of other forces.

***Stealth and low probability of detection*:** Both stealth and low probabilities of detection are necessary conditions for effective operations in cyberspace and essential, particularly to conduct covert cyber ISR. Cyber attacks require a high level of access to adversary networks throughout all phases of conflict. Although cyber activities are characteristically stealthy and difficult to detect, care must still be taken to prevent their discovery. This, because discovery risks loss of target access, adversary knowledge of cyber capabilities readily countered or not easily replicated, and limitations of capabilities. Hence, research should focus on reducing the requirement for stealth so that cyber can provide better deterrent effects.

***Nonattribution and intraceability*:** The difficulty of detecting an adversary's cyber activities also makes these more challenging to trace and attribute. Embedded in some tools and methods, these capabilities frequently require manual actions such as log manipulations. Such characteristics prove invaluable to national security because they reduce the likelihood of counterattacks and preserve military operations below the level of war. They also reduce the probability of negative international political and legal effects when cyber capabilities are employed since they are not subject to the same sorts of international political consequences as are many traditional capabilities with comparable effects. In this way, the effects attainable in and through cyberspace can also be used to aid other elements of national power rather than hinder them.

Cyberspace, however, raises a number of difficult and complex issues, starting with the *unusually large array of threat actors* that are now in play, and the *ease with which they can undertake hostile actions*. Already the types of threats go beyond those that are canonical to the international system. "They jump over and render obsolete centuries of understandings about sovereignty and national borders."[275] Because it is a domain characterized by speed, automation, anonymity, and a rapid pace of technological advancement, cyberspace is indeed a very difficult environment for security actors. Yet the relatively low cost of a sophisticated attack makes it an asymmetric field. And the asymmetries enable a range of other actors, not just states, to use virtual means for their own hostile ends, sometimes even with psychological dimensions.

As to the Differences of Cyberwar at the Strategic and Operational Levels of Warfare

The *strategic purpose of the application of cyberpower* is obvious: it revolves around the ability in peace and war to manipulate perceptions of the strategic environment to one's advantage while at the same time degrading the ability of an adversary to comprehend that same environment. Transforming the effects of cyberpower into

275 *On Cyber War*, op. cit., p. 28.

policy objectives is the art and science of strategy, defined as "managing context for continuing advantage according to policy."[276] *Strategy* is concerned with the relationship between *ends*, *ways*, and *means*. While the relationship between ends, ways, and means is important and strategically applicable in the classical warfighting domains, this is not so to the same extent for war in the cyberspace domain. First, it is less clear what the *ends* of cyberwarfare are. The fact that it is almost impossible to discern the intent or even the identity of an aggressor in cyberspace with sufficient certainty makes it very difficult to see cyberwarfare as an action by a known party using certain resources in order to achieve specifiable goals. In the other warfighting domains attribution is not a problem as it is more or less self-evident who acts in a warlike manner, and for what reason. But without fast and accurate attribution, the identity and intent of an attacker in cyberspace might just not be knowable. Hence, deterrence will hardly work, and it will be more difficult for a defending government to know that its retaliatory response is both accurately targeted and proportionate to the damage caused.[277]

Second, the *ways* of cyberwarfare are even less clear. What can be expected of cyberwarfare as a method for achieving *strategic ends* is neither obvious, nor is there any method to estimate *how ambitious these ends can be*. The answer will depend upon the *degree of decisiveness* that can be attributed to cyberwar. And on this issue, only very controversially disputed opinions exist. The arguments range from seeing cyberwar merely as an ancillary function of *force multiplier*, to understanding it as a distinct domain alongside land, sea, air and space operations, to seeing it as nothing less than a new 21st century war in its totality, that is *displacing conventional military operations altogether*.[278] It is as common to find people convinced of the possibility of a *cyber Pearl Harbor*[279] or *cybergeddon* as it is to find vehement attempts to dismiss such possibilities as worst-case analysis and scaremongering.

Third, the *means* of cyberwarfare pose a wider variety of problems. Compared to kinetic weapons, cyber weapons have three distinguishing characteristics: (1) They are generally easier to use with a higher degree of anonymity and plausible deniability, making them well suited for covert operations and for instigating conflict between other parties. (2) Cyber attack means are more uncertain in the outcome they produce, making it more difficult to estimate deliberate and collateral damage. And (3) cyber attack means involve a larger range of options and possible outcomes, and may operate on time scales ranging from tenths of a second to years, and at spatial scales anywhere from 'next door' to globally dispersed.

Cyberspace offensive weapons have analogies with weapons of mass destruction and space forces. Their effects are global in nature and cannot really be contained

276 Everett C. Dolman, Pure Strategy: Power and Principle in the Space and Information Age, London, Frank Cass, 2005, p. 6.
277 *On Cyber War*, op. cit., p. 29.
278 "Marching off to cyberwar," *The Economist Technology Quarterly*, 6 December 2008, pp. 20-21.
279 Jason Ryan, "CIA Director Leon Panetta Warns of Possible Cyber Pearl Harbor," Top Intelligence-Security Officials Say Computer Attacks Increasing, 15 February 2011, at: http://crisisboom.com/2011/02/15/computer-cyber-hacking-increasing/

to a specific geographic theater. Offensive full-spectrum cyberspace weapons are strategic in nature: once used, they lose their deterrent value and effectiveness because knowledge of their specific capabilities may quickly spread across the Internet. Opponents can then adjust their defenses, and write and implement software patches against it. Attackers must give serious considerations to employing cyber munitions because it is not usually destroyed during an attack. Once released, such a weapon is relatively easy to capture. Cyber forces can then deconstruct and analyze its code to determine appropriate countermeasures for future attacks, and for use as a weapon against its sender.[280]

Cyber weapons are almost always dual-use, in the sense that they are lines of code and physical hardware that can be modified for other purposes. And cyber attack operations in cyberspace occur near the speed of light in real-time.[281] More important, they often can impact the entire spectrum of the cyberspace domain simultaneously without notice, intelligence warning or indications. This instantaneous nature, and the ability to attack the entire domain simultaneously, is a characteristic that makes cyberspace a more dangerous and at the same time also a more vulnerable domain.

The *means* can be more difficult to comprehend than those existing in the classical warfare domains. Constituting a new classification of capabilities designed to disrupt computer systems and networks, they include any instrument or instrumentality used in a manner to cause harm to computers, networks or electronic devices.[282] This is hardly surprising: for as long as there has been technology (the application of science and innovation) and strategy (the use of forces and resources to achieve political ends), there has been a relationship between these two activities.[283] But the technology of cyberwarfare challenges the established thinking about this relationship in at least three respects. First, the most distinctive feature of cyberwar is the rapidity with which threats can evolve in cyberspace. The extraordinary pace of change can be so abrupt as to render the conventional, action/reaction cycle of strategic evolution out of date before it has begun.[284] The second distinctive feature is that cyber technology is exploiting what in the classical domains is normality in a covert, if not invisible way, with the result that increasingly powerful and stealthy cyber weapons have become within reach of almost every actor in cyberspace. And third, as a *strategic means*, cyberwar has become 'democratized,' in the sense that technologies, which in the past would have been considered highly specialized, are now proliferating as widely available, cheap, and relatively easily useable *means of combat for everyone*.

Further enhancing the problems of cyberwar is the fact that also the weapon systems used in the other warfighting domains are increasingly vulnerable to

280 Eric D. Trias & Bryan M. Bell, "Cyber This, Cyber That…So What?," *Air & Space Journal*, Vol. XXIV, No. 1, Spring 2010.
281 A keystroke travels twice around the world in 300 milliseconds according to William J. Lynn, US Deputy Secretary of Defense.
282 An interesting point is that the number of viruses, worms, and Trojans currently in circulation has now topped the 1 million mark according to a security software provider.
283 For a discussion of this relationship see: Paul Cornish, "Technology, strategy and counterterrorism," *International Affairs*, Vol. 86, No. 4, July 2010.
284 *On Cyber Warfare,* op. cit., p. 29.

cyberwarfare as they become more automated and networked. Current and future weapon systems are being infused with technological advancements, many of which are electronic, including sensors, communication systems, and control systems.[285] Various systems are being networked to provide *augmented command and control ability*. This establishes an advantage for cyberwar, and even though the systems are embedded with highly advanced security, any time there is an opportunity for *interconnection* there is also *a vulnerability to foreign access*.

C4ISTAR systems – the command, control, communications, computers, intelligence, surveillance, target acquisition, and reconnaissance systems of the armed forces – are particularly vulnerable to cyber attacks because they interconnect. Moreover, computer processors, memory, and other hardware are ubiquitous. While scans can be run on software and hardware, there is also a potential for infiltration during development and manufacturing of these elements. Infiltrations can thus enable cyber attacks on many weapon systems. Cyberwarfare can affect the control of radars, missiles, communications, and software. It can potentially disable mobile targets like missiles or even redirect them to the launch site. And not only can cyberwar disable or disrupt wireless mobile communication systems, but also the global positioning system (GPS).[286]

Directed energy weapons are another class of weapons that create offensive, defensive, and preemptive capabilities. They have the ability to project or target energy at a specific hostile location or facility, and can be used to fry, melt, disrupt, and destroy electronic circuits used in computers and network switching components. These can be employed against all types of command and control systems as well as against stationary and mobile targets. Hence, dealing with the rapid proliferation of these kinds of new cyber weapons will be a key challenge to solve in the coming years.

The rapid growth in technology is the primary reason for the accelerating rise of threats in cyberspace. As has become obvious by now, maintaining a *defensive only posture* in cyber security is self-defeating in the long run. Because of its perceived lack of capability to prevent attacks completely, cyber security has to get out of the mindset of a purely defensive approach and combine it with offensive actions to ensure that a more solid defensive posture can ultimately be maintained. While neither a defensive strategy nor an offensive strategy *alone* can provide the needed protection, the combination of an enhanced defense-in-depth strategy with an offensive strategy may offer better ways to secure cyberspace.

Specifics of the type of offensive operations intended for use by the armed forces in cyberwar remain largely undefined due to sensitivity and classification. But they are intended to provide an offensive capability to target potential threats and ensure freedom of action for attaining national interests. These include, among others, intelligence gathering, disruption of enemy activities by altering their systems, and

285 "Cyber Warfare: The Threat to Weapon Systems," op. cit.
286 Lionel D. Alford, "Cyber Warfare: The Threat to Weapon Systems," WSTIAC, Weapon Systems Technology Information Analysis Center, New York, *WSTIAC Quarterly*, Vol. 9, No. 4, 2010.

undertaking activities to dissuade future use of the network as a tool for attack. These are not new military tasks, but having the capability to be launched from the cyber realm provides a more attractive and more promising approach.

The benefits of an offensive strategy are evident. Chief among these are risk and level of effort required in terms of resources. Clearly, a mechanism that provides a way to deliver the effects needed without placing military personnel in harm's way is of a very low risk. The fact that cyberspace weapons are primarily software tools, often integrated with only a minimal amount of hardware, is another attractive feature. Funding, timelines for procurement, and sustainment costs will be much lower than those incurred by conventional weapons systems such as tanks and aircraft. Looking at the dilemma some armed forces face today in replacing their aging fighter fleets, one can see how the ability to rapidly produce new cyber weapons for a fraction of the cost and effort of kinetic systems would be welcomed.

New offensive cyber weapons, designated 'CyberCraft' in the US, offer a shift in capabilities and forward deploy technology out in the network allowing *mobile defense*. These CyberCraft weapons are expected to sense targets and mitigate enemy threats prior to their use to exploit and penetrate networks. They have small signatures to avoid detection, are capable of being activated from within the network, contain control information, are remotely controlled, and have a self-destruct mechanism in case they are detected. Moreover, they consist of sophisticated computer programs delivering other advanced tech-nological capabilities to warfighters.[287] Thus, marrying the capabilities of CyberCraft weapons with defense-in-depth will allow for an *active defense strategy*. And such a marrying may provide the best possibility for stopping attacks at the source while ensuring that basic protection remains in place.

There is, however, another fact to consider: namely, that the life expectancy of any one cyber weapon is only as good as the life of the vulnerability that the cyber weapon is designed to exploit. Once a remote vulnerability or avenue of attack is closed, the cyber weapon created to capitalize on this may no longer be valid. Therefore a program that can continually develop newer and more sophisticated methods to exploit anticipated emerging vulnerabilities is needed.

These facts and the linked uncertainties render the cyberspace environment *strategically less stable* than the environments of the traditional warfighting domains. The rapidity of innovation in cyberspace tends to *amplify the dominance of the offensive*, which can create incentives for a first or preemptive strike. *Crisis instability* and *arms race instability* might ensue. Crisis instability can push governments to act first in a crisis, often earlier than may be necessary. In such high-pressure circumstances resulting in compressed decision cycles for cyberspace operations, cyber capabilities may be regarded in the way nuclear weapons were for a while in the early days of nuclear deterrence, when the choice seemed to be: *use them or lose them*. Arms race

287 See for example: Paul W. Phister, Dan Fayette & Emily Krzysiak, *CyberCraft: Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment*, AF Research Laboratory, Information Directorate, Rome, NY, June 2005.

instability, on the other hand, can encourage tit-for-tat escalation in capability, leading to an arms race in cyberspace. Governments then will wish to draw upon new sources of expertise and innovation in order to achieve a speedier response to the threat development. The danger here is that another lesson of the nuclear era might be lost: while innovation can address specific vulnerabilities, it can also make the system as a whole less stable.[288]

The uncertainties and yet-unsolved problems notwithstanding, the consequences of what was presented above are the following: Cyber attack can support military operations. For example, a cyber attack could disrupt adversary command, control, and communications; suppress air defenses; degrade smart munitions, missiles and platforms; or attack warfighting as well as warmaking infrastructure, such as the defense industrial base. Cyber attack might be used to enable or augment kinetic attack to succeed, or defend IT systems and network of the own forces by neutralizing the source of adversary cyber attack.

Cyber attack can also support covert action designed to influence governments, events, organizations, or personnel supporting foreign strategy and policy in a manner that is unlikely to be attributable to the own government. The range of possible cyber attack options is very large. Covert action might be used, for example, to instigate conflict between political factions, harass disfavored leaders and entities, or influence decision making or even such things like elections.

As to other Elements of Warfighting that the Advent of Cyberwar is Changing

Most warfare throughout the two centuries of the industrial era centered on one principal strategic objective: the physical occupation of territory. The possibility of occupying territory, or the threat of becoming occupied, forced nations to amass large standing armies, to maintain navies, and to procure aircraft in hopes of achieving superiority against their adversaries. Cyberwarfare changed this. Computer connections to various communications networks and the Internet, in particular, make it easier to execute attacks and *may render irrelevant the need to reach the target physically*. And the barriers to entry in the cyber domain are so low that non-state actors as well as small states can play more significant roles at much lower levels of cost.

Some elements of the cyberspace domain are common to the other warfighting domains. Land, sea, air, and space are all interactive and require cross-domain planning. Cyberspace is not different. Although theoretically, *dominance* in cyberspace will support freedom of action in all other domains and deny freedom of action to adversaries, as will, at least temporarily, *superiority* in the cyberspace domain: *dominance in cyberspace is elusive*, and *superiority would seem to be much harder to*

288 On Cyber Warfare, op. cit., p. 30.

achieve than in the traditional domains of warfighting. It is more predicated to successful conventional military operations.

In contrast to sea, air, and space, cyber shares three characteristics with land warfare in ever greater dimensions: (1) the number of players, (2) the ease of entry, and (3) the opportunity for concealment. On land, dominance is not a readily achievable criterion. While some larger states have greater capacity than others, it makes little sense to speak of dominance in cyberspace as in sea power or air power. If anything, dependence on complex IT systems and networks for support of military and economic activities creates new vulnerabilities in large states that can be exploited by smaller states and even by non-state actors.[289] Compared to the other warfighting domains, cyberwar has one advantage. *In military planning concepts, operations in cyberspace can be greatly accelerated*. They can move directly from shaping operations to seizing the initiative to instant, if temporary, superiority worldwide, with huge implications on strengths and vulnerabilities for states, aggressor nations, and non-state actors. But the other side of the coin of accelerated operations is, of course, more unpredictability, more fluidity, and less certainty of impact.

While clear distinctions can be drawn in the other domains between public and private sector attacks and responses, this is not the case in cyberspace, where the cost of entry for attacks is so low. Cyberwarfare differs significantly from warfare in the physical world, where military operations are shaped by relatively clear and well-understood political guidelines and constraints – which are still lacking for operations in cyberspace.[290]

The principal challenge in cyberwar is the question of how to respond to cyber attacks. This requires the development of a risk-mitigation architecture underpinned by a generally accepted understanding of what actually constitutes cyberwar and what price should be paid for preparing it. Without clear political and legal guidance, understood by all stakeholders, it will not be possible for certain operations to be undertaken. If they take place nonetheless, then only in the knowledge that legal action could ensue against those commissioning or carrying out the activity should its details become public knowledge. Neither of these are palatable options.

Cyberwar differs from past wars in other ways. Distinctions between soldiers and civilians are eroded. Threats are more diffuse, and the perpetrators of attacks are ever harder to locate. At the same time, existing paradigms for war and conflict cease to be appropriate. For example, a clear sense of the law of conflict in the information age is still lacking.[291] It took decades to establish the place of airpower in national defense strategies and international rules for conflict. With cyberspace, the challenges will be similarly large and onerous, if not more so. They range from mastering the forensic

289 Joseph S. Nye, *Cyber Power*, Cambridge, Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010, p. 4.
290 Ibid., p. 16.
291 Lt Gen Kenneth A. Minihan, Director NSA and previously Director DIA, and Air Force Gen Kevin P. Chilton, Commander US Strategic Command, in remarks to the Defense Writers Group, 4 March 2008.

tasks of attack attribution all the way to much broader questions about *proportionality of response* and *legitimacy* of certain *targets*.[292]

New ways will have to be found to solve difficulties such as the mismatching of domestic and inter-national law. Old concepts and standards of sovereignty do not function well in this cyber world, where the limits of national ownership and responsibilities are fuzzy, and cyber threats are transnational. The latter means, by definition, they are not confined by borders. This complicates the defensive task in a variety of ways; most notably it means that attackers and non-state actors can hide more easily. Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and impunity. The difficulties of attribution allow a larger degree of plausible deniability, which is in more plentiful supply in cyberspace. Perpetrators can cover their own tracks and implicate others, particularly when third-party servers and botnets in unrelated countries can be used to originate attacks and provide cover for the actual attacker. In contrast, the defender is confronted with the disadvantage to be forced to rely on others if he is to enforce actions across borders.[293] Thus, the key to successful cyberwar is attribution, which becomes increasingly difficult with current technology and present Internet network communications. While it is difficult to envision a major conventional land, sea, or air attack that cannot be attributed to a nation-state, it is practically impossible to achieve attribution of a nation-state cyberspace aggressor if he chose anonymity. And equally impossible can be attribution of responsibility for *state-sponsored operations by non-state actors*.

However, much of what is considered offensive cyberspace activity does not meet the criteria of *attack* in the other domains. Shutting down or massively corrupting data in critical financial, health or electrical power grid networks constitutes an attack on national sovereignty and may or may not justify a use-of-force response. A cyber attack on a SCADA system that results in casualties or in a regional electric blackout could be considered a kinetic effect to an offensive cyberspace operation. But at the lower end of the spectrum, actions such as pinging, browsing, or port scanning are often used simply for checking the effective functioning of networks. Thus, cyberspace operations may or may not have hostile intent. The vast majority of malware, botnets, and network intrusions are technically competitive measures, espionage, vandalism, or crimes that fall under the category of technical network defense responses or traditional law enforcement and counterintelligence functions. They are not attacks on a state's sovereignty. In many cases, these types of attacks would be better considered as network irritation than as network attacks.

While a major cyber attack may have the potential to destroy fundamental infrastructures on a massive scale, few hostile actions in cyberspace fall into this category. Hostile actors can make use of a wider range of techniques. One can, for example, envision *cyber protest* whereby a nuclear or other sensitive facility is attacked

292 Rebecca Grant, *Rise of Cyber War*, A Mitchell Institute Special Report, Air Force Association, November 2008, p. 5.
293 *On Cyber Warfare*, op. cit., p. 13.

for ecological or environmental reasons. Another example of cyber protest can be seen in the recent attacks on Visa, Mastercard, and PayPal that occurred in the wake of the WikiLeaks bonanza, the release of US diplomatic cables.[294] Such action may have the appearance of warlike activity. But in cyberspace, the distinction between what is and what is not warlike is often more blurred than in the other domains.

Further differences between cyberwar and other forms of cyber attack are apparent in terms of the political framework within which such actions are presented, and in terms of intent and attribution.[295] As noted by the Economist: "a cyber attack on a power station or on an emergency-services call center could be an act of war or an act of terrorism, depending on who carries it out and what their motives are."[296] Such difficulties tend to be more numerous in cyberspace and thus are another manifestation of what makes cyberwarfare different from the other warfighting domains.

Finally, unlike in the other warfigthing domains, victory and defeat will be less clearly recognizable in cyberwar, as these concepts have little traction in cyberspace, where political, ideological, religious, economic, and military combatants fight for varying reasons according to different timescales. These actors will bring their own code of conduct to the fight, resulting in a more discordant and more chaotic sphere of conflict in which it is not yet obvious that a common framework of ethics, norms, and value can apply.[297]

On the Difficulties of conceiving Military Doctrine and Rules of Engagement for Cyberwar

In theory, cyberwarfare might be a good thing for the world if it makes future conflicts shorter and costs fewer lives, which could facilitate economic recovery and post-war diplomacy. However, it may be more difficult to conceive *a military doctrine* for many aspects of cyber conflict that are *truly revolutionary*. As examples of the many revolutionary aspects existing, the following ones can be listed to consider:[298]

- The Internet is an artificial environment that can be shaped in part according to national security requirements.
- The blinding proliferation of technology and hacker tools makes it impossible to be familiar with all of them.
- The proximity of adversaries is determined by connectivity and bandwidth, not terrestrial geography.

294 Jane Wakefield, "WikiLeaks' struggle to stay online," *BBCNews Technology*, 7 December 2010.
295 *On Cyber War*, op. cit., p. 11.
296 "Marching off to cyberwar," *Economist Technology Quarterly*, 6 December 2008, pp. 20-21.
297 *On Cyber Warfare*, op. cit., p. 37.
298 Kenneth Geers, "The Art of Cyberwar," *Internet Evolution*, 24 January 2012.

- Software updates and network reconfigurations increase the unpredictability of the battlespace of cyber conflict with little or no warning.

- Contrary to our historical understanding of war, cyber conflict favors the attacker.

- Cyber attacks are flexible enough to be effective for information warfare and propaganda, espionage, and the destruction of critical infrastructure.

- The difficulty of obtaining reliable attack attribution lessens the credibility of deterrence, retaliation, and prosecution.

- The 'quiet' nature of cyber conflict means a significant battle could take place with only the direct participants knowing about it.

- The dearth of expertise and evidence can make victory, defeat, and battle damage assessments a highly subjective undertaking.

- There are few moral inhibitions to cyber attacks, because they relate primarily to the use and abuse of data and computer code. So far, there is little perceived human suffering.

Top military thinkers can help the armed forces to fill the holes in their cyber defenses. But it will take many years to incorporate all the revolutionary aspects of cyber conflict into military doctrine. The same is true for rules of engagement (ROEs). Developing appropriate rules for the use of cyber weapons is very difficult. ROEs are supposed to be developed prior to the need for use of these weapons, so that warfighters have proper guidance under operational circumstances. That means that various contingencies must be anticipated in advance. However, it is difficult to imagine all possible contingencies before any of them happen. As examples of some of the problems to be solved, the following ones can be listed to consider:

- ROEs must be developed to cope with the fact that several dimensions of cyber attacks span a wider range than those encountered in the classical warfighting domains.

- Cyber attacks may range from being non-lethal to destructive on a society-wide scale.

- The impacts of cyber attacks may be easily predicted in some cases, but may have a higher uncertainty than the impacts of kinetic weapons in other cases.

- The set of potential targets that may be adversely affected by cyber attacks is likely larger than the corresponding set of potential targets for other weapons.

- A cyber attack conducted for offensive purposes may well require authorization from higher levels of command than would a technically similar cyber attack conducted for defensive purposes.

- The adversary might not react at all to a cyber attack, or might even react with weapons of mass destruction.

- The adversary may range from being an individual hacker to a well-funded nation-state.

It is thus unrealistic to try to craft a single ROE that attempts to cover all uses of cyber attack. Rather, it will be necessary to tailor an array of ROEs that are applicable to specific kinds of cyber attack and for likely specific circumstances. And it will be more difficult to craft ROEs for missions involving cyber attacks than for missions involving other kinds of weapons. The following issues illustrate the complexity of developing ROEs in advance by just looking at the question under what circumstances governed by what authority a retaliatory cyber attack might be launched to neutralize an immediate or ongoing threat:

- Who should influence and who should develop ROEs for active threat neutralization?

- What level of impact must an incoming cyber attack have to justify active threat neutralization?

- How far are the intent and the identity of a cyber attacker relevant?

- How does the proportionality principle apply to active threat neutralization?

- How far down the chain of command should delegation of authority for neutralization be carried?

- How should the scope, duration, and intensity of a neutralization action be calibrated?

A further level of complication in developing ROEs is that the factors above cannot be assessed independently.

While cyber attack is an important capability for states to maintain, the acquisition and use of such capabilities raise questions which either do not exist or pose more difficult problems to solve than in the traditional warfighting domains. Such questions show other differences existing at the operational and tactical level between cyberwar and traditional warfighting. Some countries have undertaken studies on what differentiates cyber attacks from the use of other weapons, and on

the implications of their acquisition of cyber weapons.[299] The findings of these studies may serve as an indicator of many other differences existing between cyberwar and traditional warfighting.

299 See the exemplary study done for the US by the Committee on Offensive Information Warfare, Computer Science and Tele-communication Board, Division on Engineering and Physical Sciences of the National Research Council: William A. Owens, Kenneth W. Dam & Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington D.C., National Academy of Sciences, The National Academies Press, 2009, 360 p.

Annex 2: Summary of major Incidents of Cyber Conflict

United States 1982

In 1982, US President Reagan approved a plan of the CIA to transfer software used to run pipeline pumps, turbines, and valves to the Soviet Union. The software, subsequently stolen by Russians in Canada, had embedded features – a logic bomb – designed to cause pump speeds and valve settings to malfunction. "The result was the most monumental non-nuclear explosion and fire ever seen from space," noted former US Air Force Secretary and former Director of the National Reconnaissance Office, Thomas C. Reed, in his book 'At the Abyss: An Insider's History of the Cold War.' The attack had an enormous economic and psychological impact on the Soviet Union and is credited with helping to end the Cold War.[300]

United States 1991

The US used cyberwarfare means and methods when it invaded Iraq in 1991. Phase I of Operation Desert Storm opened with a strategic air campaign and strikes against Iraq's air defenses, aircraft and airfields, command and control systems, telecommunications facilities, and key elements of the national infra-structure, such as critical electric grids.[301] The US also used its extensive communication and satellite systems to support the operation.[302]

Chechnya 1994 and 1997-2001

Chechnya in 1994 is another case of cyberwarfare, where pro Chechen and pro-Russian forces have waged a virtual war on the Internet, simultaneous to their conflict on the ground. The Chechen separatist movement in particular is considered a pioneer in the use of the Web as a tool for delivering powerful PR messages. The skillful placement of propaganda and other information, such as the number to a war funds bank account in Sacramento, California, helped to unite the Chechen Diaspora.[303]

During the second Chechen war, 1997-2001, in which the Russian military invaded the breakaway region of Chechnya to reinstall a Moscow-friendly regime, both sides used cyberspace to engage in information operations to control and shape

300 David E. Hoffman, "CIA slipped bugs to Soviets," *Washington Post*, 27 February 2004.
301 *Operation Desert Storm: Evaluation of the Air Campaign*, U.S. Government Accountability Office, Letter Report, GAO/NSIAD-97-134, 12 June 1997, Appendix V.
302 Jon Trux, "Desert Storm: A space-age war," *NewScientist*, 27 July 1991.
303 Timothy L. Thomas, "Information Warfare in the Second Chechen War: Motivator for Military Reform?", Foreign Military Studies Office, Fort Leavenworth, Kansas, 2002.

public perception. The most effective information, however, was not pro-Chechen, but anti-Russian. Digital images of bloody corpses served to turn public opinion against perceived Russian military excesses. In 1999, just as Kremlin officials were denying an incident in which a Chechen bus was attacked and many passengers killed, images of the incident appeared on the Web. As technology progressed, Internet surfers watched videos of favorable Chechen military activity, such as ambushes on Russian military convoys.

Russian officials were accused of escalating the cyber conflict by hacking into Chechen websites. The timing and sophistication of at least some of the attacks suggested nation-state involvement. Even after the war officially ended, the Russian Federal Security Service (FSB) was reportedly responsible for knocking out two Chechen websites kavkaz.org – hosted in the US – simultaneous to the storming by Russian Spetsnaz Special Forces of a Moscow theater under siege by Chechen terrorists on 26 October 2002.[304]

Kosovo 1999

Just as Vietnam was the world's first TV war, Kosovo in 1999 proved to become the first broad-scale Internet war. As NATO planes began to bomb Serbia, numerous pro Serbian or anti-Western hacker groups, such as the 'Black Hand,' began to attack NATO Internet infrastructure. It is unknown whether any of the hackers worked directly for the Yugoslav military. But their stated goal was to disrupt NATO military operations.[305] US armed forces hacked into Serbia's air defense control to facilitate the bombing of Serbian targets. Later, in May 1999, NATO accidentally bombed the Chinese embassy in Belgrade, spawning a wave of cyber attacks from China against US government websites.

The Israeli-Palestinian Cyberconflict July 1999 to April 2002

In September 2000, Israeli teenage hackers created a website to jam Hezbollah and Hamas websites in Lebanon. The teenagers launched a sustained DDoS attack that effectively jammed 6 websites of the Hezbollah and Hamas organizations in Lebanon and of the Palestinian National Authority. This seemingly minor attack sparked a cyberwar that quickly escalated into an international incident. Palestinian and other supporting Islamic organizations called for a cyber Holy War.[306] Hackers struck 3 high-profile Israeli sites belonging to the Israeli Parliament, the Ministry of Foreign Affairs, and the Israeli Defense Force information site. Later, they also hit the Israeli Prime Minister's Office, the Bank of Israel, and the Tel Aviv Stock Exchange.

304 Oliver Bullough, "Russians Wage Cyber War on Chechen Websites", *Reuters*, 15 November 2002.
305 "Yugoslavia: Serb Hackers Reportedly Disrupt US Military Computer", *Bosnian Serb News Agency SRNA*, 28 March 1999.
306 "Cyber War Also Rages in MidEast," *The Associated Press*, 28 October 2000.

By January 2001, the conflict had struck more than 160 Israeli and 35 Palestinian sites. 548 Israeli domain websites were defaced out of 2,295 in the Middle East. The main types of attacks were website defacement and DDoS attacks. Attacks were also made against companies providing telecommunications infrastructure. Palestinian hackers defaced an Internet Service Provider and left a message claiming that they could shut down the Israeli ISP NetVision, which hosts almost 70 percent of all the country's Internet traffic.

The Cyber Attack on Estonia April-May 2007

Estonia, with a population of 1.3 million people, has become a marvel in terms of widespread access to ICT. As one of the most electronically advanced countries, the Estonian government has shifted its operations since November 2005 to the virtual domain. Cabinet-level meetings are conducted online and documents are signed with e-signatures. Estonian citizens could cast their votes in national elections via their PCs.[307] In 2007, Estonia was ranked 23rd in e-readiness ratings. 61 percent of the population enjoys online access to bank accounts, and 95 percent of banking transactions are electronic.[308] Such over-whelming reliance on the Internet was bound to attract the interest of Russian hackers, who were waiting for a pretext to test Estonia's cyber defenses.

That pretext came with the Estonian government's decision to relocate the monument commemorating the sacrifice of Soviet armed forces in liberating Estonia from the Nazi yoke during World War II. On 27 April 2007, the seemingly innocuous act of relocating the monument from the center of the Estonian capital Tallinn to a military cemetery outside the city sparked protests and riots among Estonia's Russian minority. These protests were then followed by a barrage of DDoS attacks ranging from single individuals using various low-tech methods like ping floods to expensive rentals of botnets from all around the world usually used for spam distribution which clogged Estonia's Internet network. A call for action, complete with specific instructions on how to participate in the DDoS attacks, quickly spread through Russian online chat rooms. Soon Estonian "government websites that normally receive 1,000 visits a day reportedly were receiving 2,000 visits every second."[309] The government network was designed to handle 2 million megabits per second; the servers were flooded with nearly 200 million megabits per second of traffic. The longest attack lasted over 10 hours and created over 90 million megabits per second of data on the targets. As a result, the websites of the Ministries of Foreign Affairs and Justice had to shut down, while Prime Minister Andrus Ansip's Reform Party's website was defaced with digital graffiti of a Hitler-style moustache scrawled across the Prime Minister's photo. On 3 May, the botnets began attacking private sites and servers. Banks in Estonia were shut down, save a few, but it came at great monetary costs and affected also international banking. The climax of the attacks happened on 9 May, the Russian anniversary of the end of WWII. To cope with the increased traffic, the government quadrupled the amount of traffic it can handle from 2 to 8 gigabits a second.

307 Cyrus Farivar, "Cyberwar I. What the Attacks on Estonia Have Taught Us About Online Combat," *Slate*, May 22, 2007.
308 Johnny Ryan, "iWar: A New Threat, Its Convenience – and Our Increasing Vulnerability," *NATO Review*, Winter 2007.
309 Clay Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Service Report for Congress, January 29, 2008.

During the following days the attacks subsided, with a new spike happening on 15 May. The Russian hacktivists also managed to briefly disable the national emergency toll-free phone number 112. Moscow denied any involvement in the attacks, but Estonian officials have reiterated their certainty that the Kremlin was behind the attacks.[310]

Both the US and NATO sent teams of computer security experts to help the Estonian authorities cope with the massive wave of DDoS attacks that paralyzed the country's government websites, banking industry, and media outlets. What struck many network security experts as unusual about the cyber attacks was that they lasted weeks, and their intensity was extremely high. Some botnets employed in the DDoS attacks on Estonian websites included up to 100,000 'zombie' PCs. The concerted efforts by its allies eventually stabilized Estonia's situation, but intermittent cyber attacks on national government websites, including the State Chancellery and Federal Electoral Committee, continued well into the middle of May 2007.

The cyber attack on Estonia led NATO to establish the Cooperative Cyber Defense Center of Excellence (CCD COE) in Estonia in May 2008. The Center, with a staff of 30 specialists, became operational in August of that year, and is part of a NATO network of 13 accredited Centers of Excellence dedicated to training representatives from alliance member countries "on technically sophisticated aspects of NATO operations." The CCD COE focus is on coordinating cyber defense and establishing policy for aiding allies during cross-jurisdictional attacks.

From the point of view of international law, the attack on Estonia can be described as an 'unjust' cyber attack. Seen from the perspective of *jus ad bellum*, the attack lacked a sufficient just cause and was not undertaken in any meaningful sense as a last resort. From the perspective of the just conduct of hostilities – *jus in bello* – the attack was utterly indiscriminate, and disproportionate in its threat of harm, at least, when compared either to the harm Russia or its citizens allegedly were suffering, or any legitimate military objective that might have otherwise been under consideration.

Chinese attacks against European government networks in August 2007

The British Security Service, the French Prime Minister's Office, and the Office of German Chancellor Angela Merkel, all complained to China about intrusions of their government networks. Merkel even raised the matter with China's President Hu Jintao.

So far no official source in China has admitted complicity in these cases.

Israeli disruption of Syrian air defense networks 6 September 2007

Operation *Orchard* was an Israeli airstrike with F-15, F-16, and an ELINT aircraft on a target in the Dayr az-Zawr region carried out just after midnight on 6 September 2007 that destroyed the Al Kibar complex with AGM-65 Maverick missiles and laser-

310 Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations*, Tallinn, Cooperative Cyber Defense Centre of Excellence (CCD COE); 2010, pp. 15-34.

guided 500 kg bombs.[311] The target had been a nuclear reactor under construction by North Korean technicians built to process plutonium. One report stated that a team of elite Israeli Shaldag Special Forces commandos arrived at the site the day before so that they could highlight the target with lasers, while a later report had Sayeret Matkal special commandos involved. US industry and military sources speculated that the Israelis may have used technology similar to America's Suter airborne network attack system to allow the aircrafts to pass undetected by radar into Syria. This would make it possible to feed enemy radar emitters with false targets, and even directly manipulate enemy sensors. In May 2008, a report in IEEE Spectrum cited European sources claiming that the Syrian air defense network had been deactivated by a secret built-in switch activated by the Israelis.[312] Aviation Week and Space Technology later reported that Israeli aircraft actually engaged a Syrian radar site in Tall al-Abuad with conventional precision bombs, electronic attack, and brute force jamming. In a November 2009 report, the IAEA stated that its investigations had been stymied due to Syria's failure to cooperate. The following February, under the new leadership of Yukiya Amano, the IAEA stated that "the presence of such uranium particles points to the possibility of nuclear-related activities at the site and adds to questions concerning the nature of the destroyed building … Syria has yet to provide a satisfactory explanation for the origin and presence of these particles."[313] Syria disputed these allegations.

Although the operational details are murky, and formal attribution has never been made or acknowledged, from the point of view of international law, the attack on an adversary's illicit military installation was justified. A strike had been continuously threatened in the event that Syria pursued development of a nuclear weapons program. Both the cyber and conventional military actions were undertaken only after reasonable diplomatic efforts, including embargoes of illegal shipments of materials from North Korea, had failed to halt Syrian collaboration with North Korean agents. The preemptive cyber strikes were directed against military targets: radar and Russian-made air defense systems, much as a conventional attack might have been, enabling Israeli fighters to penetrate deeply into Syrian airspace with little resistance. Unlike the conventional attacks that followed, the cyber attack attained the military objective of rendering defensive forces helpless, without widespread destruction of property or loss of life on either side.[314]

Lithuania June-July 2008

On 17 June 2008, the Lithuanian Parliament adopted an amendment to the Law on Meetings that regulated the implementation of freedom of speech and freedom of assembly. Public display of Soviet and Nazi German insignia, such as the hammer and sickle, the red star, and the swastika, as well as playing of the Soviet and Nazi anthems at public gatherings were prohibited. Following the passage of the amendment, the Russian Federation expressed their discontent with the decision, with both the

311 *Operation Orchard*, Wikipedia, at: http://en.wikipedia.org/wiki/Operation_Orchard Also: Hans Rühle: "Wie Iran Syriens Nuklearbe-waffnung vorgetrieben hat," *Neue Zürcher Zeitung*, 19 März 2009.
312 Sally Adee, "The Hunt for the Kill Switch," *IEEE Spectrum*, May 2008.
313 Mark Heinrich, "IAEA suspects Syrian nuclear activity at bombed site," *Reuters*, 18 February 2010.
314 Uzi Mahnaimi & Sarah Baster, "Israelis seized Nuclear Material in Syrian Raid," *The Sunday Times*, 23 September 2007, and David A. Fulghum, Robert Wall & Amy Butler, "Israel Shows Electronic Prowess," *Aviation Week*, 25 November 2007.

President and Parliament issuing condemning statements. On 22 June, the Russian and the Belarusian Presidents jointly denounced the new law as a "politicized approach to history," and condemned what they described as "attempts to rewrite wartime history." Coinciding with the adoption of the amendment on 28 June, hundreds of government and corporate websites in Lithuania were hacked, and some were covered in digital Soviet-era graffiti, implicating Russian nationalist hackers.[315]

The Russia-Georgia War August 2008

The cyber campaign against Georgia in August 2008 is the first example of cyberattacks that coincided directly with a land, sea, and air invasion by one state against another, and is probably the best example of how to properly employ computer network attacks in a modern battlespace. Russia invaded Georgia in response to Georgia's attack against the separatists in South Ossetia.[316] The highly coordinated cyber campaign utilized vetted target lists of Georgian government websites and other strategically valuable sites, including the US and British embassies. Russians and Russian sympathizers also disrupted key Georgian media sites with botnets and command and control systems through DDoS attacks, electronic warfare jamming technique, website postings and defacement. Each site was vetted in terms of whether it could be attacked from Russian or Lithuanian IP addresses. Attack vectors included DDoS, SQL injection, and cross-site scripting XSS.[317] Main targets were government websites, financial and educational institutions, business associations, and news media websites, among them BBC and CNN, probably because they were providing useful information.[318]

The speed of action and the multidirectional nature of these cyber strikes adhered to a classical military swarming technique, overwhelming the cyber defenses of the Georgian targets. The attacking forces were highly decentralized, but were able to synchronize and concentrate their operations in a way that made any Georgian defense response nearly impossible. The primary objective of this cyber campaign was to support the Russian invasion of Georgia, and the cyber attacks fit neatly into a military-style invasion plan. Many of these cyber strikes were clearly designed to make it harder for the Georgians to determine what was happening. The inability of the Georgians to keep their websites up and running was instantly damaging to national morale. These attacks also served to delay any international response to the kinetic conflict unfolding in the South Ossetia region.

Probably the most important strategic lesson learned from the cyber campaign against Georgia is that cyber attacks are a viable military option on the battlespace.

315 Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations*, Tallinn, Cooperative Cyber Defense Centre of Excellence (CCD COE); 2010, pp. 51-64.
316 Jeffrey Carr, Inside Cyber Warfare, op. cit., p. 3. And: International Cyber Incidents: Legal Considerations, op. cit., pp. 66-89.
317 Jeffrey Carr, *Inside Cyber Warfare*, Cambridge, O'Reilly, 2010, p. 3.
318 See also: "Timeline of the Russian-Georgian conflict," OSW, EastWeek, Centre for Eastern Studies, 20 August 2008,

Another lesson is that cyber attacks can be launched from safe remote locations, in this case from several different countries and aided by Russian-organized crime syndicates. Yet another lesson is that these operations can be employed in cases where limiting the physical damage to the target is a strategic concern for the theater commander.

Even though the cyber campaign was tactically successful, there are several disadvantages to using offensive cyber attacks against an adversary's IT systems in place of more traditional attacks such as air strikes or direct action missions by Special Forces. One of these disadvantages is that cyber attacks do not produce quantifiable results as consistently as kinetic strikes do. This is due to the fact that specific cyber attacks can often be rendered useless by routine modifications in the target system – e.g. application-level patches. In military engagements involving equals, the tactical advantage for most offensive cyber attacks may go to the defender, because it is easier and faster to implement defenses than it is to develop offensive cyber attack techniques.[319]

From the point of view of international law, the cyber attacks on Georgia were part of a legitimate political disagreement between two sovereign nations over control of territory deemed important to both, conventionally taken to be a legitimate cause for the use of force when attempts at diplomatic solutions are unsuccessful. Moreover, the cyber attacks were aimed primarily at disabling the military capacities of command and control of the opposing government. Neither explicitly civilian infrastructure nor civilians themselves were deliberately targeted. Hence, the attack seems to be a justifiable use of cyber weapons in accordance with the constraints of the law of armed conflict as conventionally understood.

Kyrgyzstan January 2009

The attack against Kyrgyzstan is another successful cyberattack against a country. The attackers focused on three of the four Internet Service Providers (ISP). The DDoS attack quickly overwhelmed the three ISPs and disrupted all Internet communications. The IP traffic was traced back to Russian-based servers primarily known for cybercrime activities. Multiple sources have blamed the attack on the Russian cyber militia and the Russian Business Network (RBN) suspected to control the world's largest botnet with between 150 and 180 million nodes. One significant difference in this case is that most of the DDoS traffic was generated in Russia and may have implicitly involved the Kremlin, despite official denials. It could have been related to tensions between the administration and either the Russian government or an opposition party critical of the nation's policies. It could also have been an attack by Russian sympathizers over a dispute with Kyrgyzstan regarding US access to the Manas air base in that country.

319 John Bumgarner & Scott Borg, Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008, *A US-CCU Special Report*, August 2009. Also: John Bumgamer, "Computers as Weapons of War," *IO Journal*, May 2010, pp. 4-8.

Coordinated South Korean-US attacks July 2009

Beginning on 4 July 2009, a series of DDoS attacks began to strike first South Korean and then both South Korean and US government and commercial websites.[320] Sites targeted included the Korean Assembly, the US and South Korean presidents' websites, the US State Department, the public websites for the US stock exchanges NYSE, and NASDAQ, the popular sites in South Korea such as 'naver.com.' Investigations revealed a botnet that was apparently build using a variant of the MyDoom worm from early 2004 together with rudimentary DDoS attacks such as HTTP request floods, UDP, and ICMP floods.[321] The attacks continued from 4 until 10 July, when the infected PCs were reprogrammed to encrypt files and render them unbootable. South Korea's National Intelligence Agency told lawmakers that the cyberattacks that caused a wave of Websites outages in the US and the ROK were carried out by using 86 IP addresses in 16 countries.

The targets, the US and South Korea, together with the timing between a North Korean missile test launch on 4 July and the 15th anniversary of North Korea's Kim Il Sung's death on 8 July led some to suggest that North Korea was behind the attacks. To date, there is no evidence of this. The real motivations for these attacks remains a mystery, but it is widely considered a political attack.[322]

Cyber attacks against Iranian nuclear facilities from 2009 to 2010

A cyber worm called 'Stuxnet'[323] of unknown origin, developed and released in a number of countries in 2009, has damaged cascades of centrifuges, illegally obtained and operated in a highly protected site at Natanz, in Iran, in explicit violation of the 1970 nuclear non-proliferation treaty. The damage sustained within Iran to its clandestine and internationally-denounced nuclear program was subsequently deemed as 'substantial,' and thought to have put the nuclear weapons development program off track for some years.[324] Stuxnet is a sophisticated weapon. It attacks and disables nuclear centrifuges that operate with a SCADA system of the Siemens type, overriding the proprietary software and overloading the centrifuges. The latter so cleverly, that it disguises the damage in progress from operators and overseers until too late to reverse. Estimates are that it must have been many months, if not years in development, with large teams of experts and access to highly restricted and classified information and equipment. An endeavor with investment in time, resources, and

320 Steven Adair, Korean/US DDoS Attacks – Perplexing, Disruptive, and Destructive, Shadow Server Foundation Calendar blog, 10 July 2009.
321 James A. Lewis, *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, Center for Strategic and International Studies CSIS, October 2009.
322 Jose Nazario, Politically Motivated Denial of Service Attacks, Arbor Networks, 2009.
323 A nickname coined by Microsoft security experts, an amalgam of two files found in the worm's code.
324 That optimism has vanished, however, a year later as a report from the IAEA, released in November 2011, showed the nuclear weapons program back on track and recovered from the cyber damage.

expertise only of a well-positioned state or coalition, and clearly beyond what a terrorist group or a well-funded criminal organization could have undertaken.

From the international law point of view, there was a good and justifiable reason, reluctantly sanctioned in the international community, to undertake military action against the Iranian nuclear weapons program. Diplomatic efforts and other non-military measures have been undertaken for years without success. It was a preventive attack on a military target with damage confined to the target identified. There was not collateral damage of any significant sort to lives or property, and civilian personnel and infrastructure were neither targeted nor affected. Thus, Stuxnet was an effective and morally justified military cyber attack. It demonstrated that cyberwar can be a good alternative to conventional war, when less drastic forms of conflict resolution have been tried in good faith, and have failed. Stuxnet also showed that cyber weapons can be designed to be effective, discriminate, and to inflict proportionate damage on their targets – more so than attacks with conventional weapons can.

Glossary

Application (or App) – Computer software designed to help a user perform a certain function on the computer, whether word processing, drawing a picture, charting the blood pressure, etc.

Backdoor – A remote access to an IT system or network and method of bypassing normal authentication, in order to obtain access to plaintext while remaining undetected.

Bit – A single digit. In computer code, it would either be represented as a "0" or a "1".

Bot – Short for "robot," a computer that has been joined to an illicit network under outside control.

Botnet – A network of bots, or robot computers.

Byte – A unit of information in computer language that usually consists of eight digits, or bits.

Corruption – Takes place when data and algorithms of an IT system are changed in unauthorized ways, usually to the detriment of the correct functioning of the IT system.

Disruption – Takes place when IT systems are tricked into performing operations that make them shut down, work at a fraction of their capacity, commit obvious errors, or interfere with the operation of other systems.

DoS or **DDoS Attack** – A Denial-of-Service attack or a Distributed or Dedicated Denial-of-Service attack, overwhelming a targeted server, or website, with such a flood of requests for response that it can force it to crash.

Domain – An address on the Internet, rendered in letters or numbers. The actual address of the website consists of strings of ones and zeroes. The Domain Name is meant in most cases to make the owner easily recognizable to a human being – e.g. *google.com* or *amazon.com*. Domain Names are sold by Registries, who assign and protect them, making sure that no one but the paying customer can use them. Most Domains are represented on the Internet by websites, but not all.

Domain Name Algorithm (DNA) – The mathematical equation used by the worm to generate seemingly random lists of Domain Names, a technique to hide the location of the botnet's controller.

Dynamic Link Library (DLL) – This is the method Microsoft programmers employ to enable computers to exchange data.

Exploit – A program designed to break into an operating system by exploiting a flaw in its programming code. Increasingly, exploits have become vehicles for malware. They are marketed openly, and used by criminals to insert whatever malware they wish into targeted computers.

Firewall – Software that blocks unauthorized access to a computer or network while permitting authorized communications.

GeoIP – A service provided by *maxmind.com* which tells you where specific IP addresses are located in the real world.

Hash Algorithm – A carefully-defined mathematical method of detecting content modification. It will detect a single alteration of a binary message written in ones and zeroes, even if the message contains trillions of bits.

Honeynet – A network of virtual computers created by researchers to snare and study malware.

Honeypot – A computer, usually virtual, without any security safeguards, in other words, *designed* to be infected by malware.

HTTP – HyperText Transfer Protocol, the foundation of data communication for the World Wide Web.

ICT – Information and Communication Technology.

Interface Manager – A layer of software between the operating system and an application that enables the user to move easily between functions, or run more than one simultaneously. Windows is an Interface Manager.

Intrusion – The entering of malware in an IT system or network enabled by vulnerability. Intrusion can lead to disruption or corruption.

IP Address – Short for "Internet Protocol Address," the ID number assigned to a specific computer in a network. Under the original IP Version 4, it consists of a 32-bit number. The newest version, IP Version 6, being implemented gradually to accommodate the phenomenal growth of the Internet, uses a 128-bit number.

IP spoofing – The creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computer system.

IRC Channel – Internet Relay Chat Channel, one of the oldest ways of setting up a forum on the Internet, where members of a group can communicate with each other either directly or broadcast messages to the entire group. IRC Channels were the first employed to create and control botnets.

ISP – Internet Service Provider, a computer or machine that connects individual computers or networks to the Internet.

IT – Information Technology.

IDN – Short for Internet Domain Name.

Kernel – The innermost core of a computer operating system.

Keystroke logging (or key logging) – The action of tracking the keys struck on a keyboard in a covert manner so that the person using the keyboard is unaware that his actions are being monitored. There are numerous methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis.

Logic bomb – A piece of software intentionally and maliciously inserted into a software system that will damage or destroy the system's functionality when a specific condition occurs (e.g. a certain date or time is reached) or by command.

Malware – Short for "malicious software," any program designed to illicitly enter a computer and disable, damage or hijack its operations.

Object Code – The most basic language for computers, composed exclusively of the ones and zeroes of binary communications.

Payload – A term used to describe the damage that can be done once a vulnerability has been exploited. For example, if a software agent, such as a virus, has entered a given IT system, it can be programmed to reproduce and retransmit itself, or destroy or alter files in the system. Payloads can have multiple programmable capabilities and can be remotely updated.

Peer-to-Peer Protocol (P2P) – Software that enables individual computers on a network to communicate and share data directly, without routing it through a central location.

Port Mirror – A network configuration that automatically copies all data traffic at a particular port to a monitoring station, allowing security technicians to watch for intrusions.

Patch – A security update that fixes a flaw in the operating system that, in effect, plugs a newly-discovered hole in the computer's defenses.

Registrar – An ICANN accredited company or organization that is authorized to provide registration services for the top-level domains such as *.com*, *.org* and *.net*. Registrars have contractual agreements with their customers. A Registrar submits all newly registered domains into the Registry.

Registry – A company or organization that maintains a centralized registry data-base for the Top-Level Domains. Currently there is only one Registry for every Top-Level domain, *.com*, *.org* and *.net*. NSI Registry maintains this Registry.

Remote Thread – Hidden code that executes itself within the virtual address space of an existing, legitimate process, in other words, a program that runs concurrent with another, so that it is not easily recognized even by a skilled technician looking for it.

Rootkit – Software that enables continued privileged access to an IT system while actively hiding its presence from administrators by subverting standard operating systems functionality or other applications.

Root Server – Computers that function as trunk lines for the Internet, managing traffic flow worldwide. There are 13 of them; labeled A, B, C, D … to M. Ten are in the United States, one each in Great Britain, Japan, and Sweden.

RPC (Remote Procedure Call) – A technology that allows a computer program to cause a subroutine or procedure to execute in another address space, usually on another computer or on a shared network, without the programmer explicitly coding the details for this remote interaction.

Server – A computer program designed to coordinate the flow of data within linked computers, or between networks, such as connecting a corporate website or individual computer to the Internet.

Service Pack Two – The 2004 Microsoft update that substantially changed the character of the operating system to regard any incoming data as a threat. A milestone in protecting computers from malware.

Source Code – Any of the various computer languages designed to render object code, the basic computer language of ones and zeroes, into something more intelligible.

Supervisory Control and Data Acquisition Systems (SCADA) – Software-based industrial control systems used to monitor the smooth, reliable, and continuous operation of infrastructure. With these systems, service providers use cyberspace to communicate and control sensitive processes, such as the opening and closing of valves; regulating temperatures; controlling the flow of oil, gas, water and waste water; balancing levels of chlorination in water; regulating power generation plants as well as power supply via the electric grid; controlling ground transportation and air traffic, etc.

Top Level Domain (TLD) – A broad category for Domain Names – e.g. *.com*, *.edu*, etc. – that serve as a primary routing service for the Internet traffic.

Trojan horse – A software that appears to perform a desirable function for the user prior to run or install, but steals information or harms the system.

Unpack – To break through or strip away the deceptive coding that compresses and protects a malicious program.

Virtual computer – An operating system inside a large computer designed to function as a singular smaller one.

Virus – A harmful software program secretly introduced into an IT system, able to generate and distribute multiple copies of it, thereby spreading throughout the system. Each virus has a destructive payload that is activated under certain conditions. When activated, it can corrupt, alter, or destroy data, generate bogus transactions, and transfer information

Website – A user-friendly platform designed to serve as a visible and interactive Internet platform, or a virtual headquarters, for a Domain.

World Wide Web – A system of interlinked hypertext documents (documents embedded with links to other, related content) accessed via the Internet.

Worm – A form of malware that spreads by itself; it does not require the computer user to do anything.

Select Bibliography

Official Documents

International Telecommunications Union (ITU)

Hamadoun I. Touré and the Permanent Monitoring Panel on Information Security, World Federation of Scientists, *The Quest for Cyber Peace*, Geneva, ITU, January 2011.

Measuring the Information Society 2010, Report, Geneva, ITU, 2010.

ITU Global Cybersecurity Agenda: High-Level Experts Group Chairman's Report, ITU, Geneva, 2008.

Cybersecurity guide for developing countries, ITU, Geneva, 2006.

NATO:

Draft NATO Cyber Defence Concept, 4 October 2007.

NATO in the Cyber Commons, Final Report from the fifth ACT workshop, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 19 October 2010.

Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, adopted in Lisbon on 20 November 2010.

NATO in the Global Commons: Global Perspective, Washington D.C., 3 February 2011.

"NATO 2020: Assured Security; Dynamic Engagement: Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO," 17 May 2010.

The NATO Cyber War Agreement, 1 May 2010.

NATO and Cyber Defence, NATO Parliamentary Assembly, NATO, 2009.

Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia 2010.

MajGen Mark Barrett, Dick Bedford, Elizabeth Skinner & Eva Vergles, "Assured Access to the Global Commons," Supreme Allied Command Transformation, NATO, Norfolk, Virginia, 3 April 2011.

European Commission

Protecting Europe from Large-Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security, and Resilience, European Commission, COM (2009) 149, Brussels, 2009.

OECD:

Reducing Systemic Cybersecurity Risk, OECD/IFP Project on "Future Global Shocks," Organisation for Economic Co-operation and Development, OECD, 2011.

Rethinking e-Government Services, User-Centred Approaches, OECD, 19 October 2009.

Australia:

Australian Government, *Cyber Security Strategy*, Commonwealth of Australia, 23 November 2009.

Australian Government, *Cyber Storm II*, *National Cyber Security Exercise*, Final Report, Attorney-General's Department, Security and Critical Infrastructure Division, August 2008.

Canada:

Government of Canada, *Canada's Cyber Security Strategy for a stronger and more prosperous Canada*, Her Majesty the Queen in Right of Canada, Cat. No: PS4-102/2010E, 2010.

Estonia:

Ministry of Defence, *Cyber Security Strategy*, Cyber Security Strategy Committee, Tallinn 2008.

France:

République Française, *Défense et sécurité des systèmes d'information, Stratégie de la France*, Paris, Agence nationale de la sécurité des systèmes d'information, Février 2011.

Germany:

Cyber Security Strategy for Germany, Berlin, Federal Ministry of the Interior, February 2011.

The IT Security Situation in Germany in 2009, Federal Office for Information Security, 2009.

Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI), Bundesministerium des Innern, Berlin, Juli 2005.

Netherlands:

Dutch Cabinet, The National Cyber Security Strategy (NCSS) Success through cooperation, 2011.

United Kingdom:

Cabinet Office, Cyber Security Strategy of the United Kingdom, safety, security and resilience in cyber space. Presented to Parliament by the Prime Minister, by Command of Her Majesty, Cm 7642, June 2009. HM Government, A Strong Britain in an Age of Uncertainty, The National Security Strategy, The Stationary Office Limited, 2010.

Cabinet Office, *The National Security Strategy of the United Kingdom, Security in an interdependent world,* Presented to Parliament by the Prime Minister, by command of Her Majesty, Cm 7291, March 2008.

United States:

The White House, International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World, May 2011.

The White House, The Comprehensive National Cybersecurity Initiative (CNCI), Partially declassified, 3 March 2010.

The White House, The Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009.

The National Military Strategy for Cyberspace Operations, The US Joint Chiefs of Staff, Washington D.C., 2006.

National Cybersecurity Strategy, Key Improvements Are Needed to Strengthen the Nation's Posture, Testimony Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives, US Government Accountability Office, GAO-09-432T, 10 March 2009.

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed, US Government Accountability Office, July 2010.

Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience, US Government Accountability Office, July 2010.

Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative, US Government Accountability Office, GAO-10-338, March 2010.

Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats, US Government Accountability Office, 2010.

Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, Committee on Deterring Cyberattacks, National Research Council, 2010.

Cyberspace Operations, Air Force Doctrine Document 3-12, US Air Force, LeMay Center,15 July 2010.

Cyberspace Operations Concept Capability Plan 2016-2028, US Army, TRADOC Phamphlet 525-7-8, 22 February 2010.

Department of Defense Strategy for Operating in Cyberspace, July 2011.

Information Warfare

John Arquilla & David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy*, Vol. 12, 1993.

Huba Wass de Czege, "Netwar – Winning in the Cyberelectromagnetic Dimension of 'Full Spectrum Operations', " *Military Review*, March-April 2010, pp. 20-32.

Col Michael J. Dominique, *Information Operations: The Military's Role in Gaining Information Superiority*, Strategy Research Project, US Army War College, Carlisle Barracks, 2009.

Martin C. Libicki, "Information Dominance" in *Strategic Forum*, Nr. 132, Washington D.C., National Defense University, Institute for Strategic Studies, November 1997.

NATO Allied Joint Publication (AJP) 3.10, *Allied Joint Doctrine for Information Operations*, 23 November 2009.

Joint Publication 3-13 Information Operations, Joint Staff, US Department of Defense, 13 February 2006.

Campaign Execution. Joint Doctrine Publication 3-00,(JDP 3-00), 3rd edition, Shrivenham, MoD, The Development, Concepts and Doctrine Centre, October 2009.

Carlo Kopp, "Fundamentals of Information Warfare," NCW 101 Part 14, *Defence Today*, pp. 71-73.

Brandon Himes & Patricia A. Joseph, *Information Warfare*, Proc ISECON 2005, Vol. 22, 8 October 1005.

David J. Lonsdale, The Nature of War in the Information Age: Clausewitzian Future, London and New York, Frank Cass, 2004.

Walter E. Richter, "The Future of Information Operations," *Military Review*, January-February 2009, pp. 103-113.

Cyberwar:

Robert K. Ackerman, "Network Situational Awareness Looms Large in Cyberspace," *Signal Magazine*, May 2010.

Richard Adhikari, "Stuxnet Suspicions Rise: Has a Cyberwar Started?," *TecNewsWorld*, 4 November 2010.

Lionel D. Alford, "Cyber Warfare: The Threat to Weapon Systems," *The WSTIAC Quarterly*, Vol. 9, No. 4, 2010.

Stewart Baker, Shaun Waterman & George Ivanov, *In the Crossfire – Critical Infrastructure in the Age of Cyber War*, A global report on the threats facing key industries, McAfee Inc., Santa Clara, 2009.

John Bumgarner & Scott Borg, Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008, *A US-CCU Special Report*, August 2009.

John Bumgarner, "Computers as Weapons of War," *IO Journal*, May 2010.

Kevin G. Coleman, Cyber Warfare Doctrine – Addressing the most significant threat of the 21st century, McMurray, The Technolytics Institute, 2008.

Kevin G. Coleman, *Preparing for a Cyber Attack. Countdown to eDay!*, McMurray, The Technolytics Institute, no date.

Paul Cornish, David Livingstone, Dave Clemente & Claire Yorke, *On Cyber Warfare*, London, A Chatham House Report, The Royal Institute of International Affairs, November 2010.

Paul Cornish, Rex Hughes & David Livingstone, *Cyberspace and the National Security of the United Kingdom: Threats and Responses*, A Chatham House Report, The Royal Institute of International Affairs, March 2009.

Matthew D. Crosston, "World Gone Cyber MAD – How "Mutually Assured Debilitation" Is the Best Hope for Cyber Deterrence," *Strategic Studies Quarterly*, Spring 2011.

Ronald Deibert, *China's Cyberspace Control Strategy: An Overview and Consideration of Issues for Canadian Policy*, Canadian International Council, China Papers No. 7, Centre of International Relations, Vancouver, The University of British Columbia, February 2010.

Chris Demchak, "Evolutions in Asymmetric Cyberpower," Cyberwar Real and Imagined, *World Politics Review*, Feature Report, 19 April 2011.

Ian Dudgeon, "Targeting Information Infrastructures," Chapter 4 in *Australia and Cyber-warfare*, Canberra Papers on Strategy and Defence No. 168, Australia National University, pp. 60-83.

Myriam Dunn Cavelty, *Cyberwar: Concept, Status Quo, and Limitations*, Zürich, CSS Analysis in Security Policy, Center for Security Studies (CSS), ETH, No. 71, April 2010.

James P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival,* Vol. 53, No. 1, February-March 2011.

Patricia Moloney Figliola, *Spyware: Background and Policy Issues for Congress*, Washington D.C.,CRS Report for Congress, Congressional Research Service, 7-5700, RL32706, 9 December 2009.

Franz-Stefan Gady & Greg Austin, *Russia, the United States, and Cyber Diplomacy – Operning the Doors*, New York, EastWest Institute, 2010.

Kenneth Geers, *The Challenge of Cyber Attack Deterrence*, Tallinn, Estonia, Cooperative Cyber Defence Centre of Excellence (CCD COE), no date.

Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?," *Strategic Studies Quarterly*, Fall 2010.

Patrick Gorman, "The Road to Cyberpower: Seizing Opportunity While Managing Risk in the Digital Age," Booz Allen Hamilton, 11 February 2010.

Rebecca Grant, *Rise of Cyber War*, A Mitchell Institute Special Report, Air Force Association, November 2008.

Clement Guitton, *An Analysis of the Cyber-Strategies of the US, China and Russia*, Geneva, Geneva School of Diplomacy & International Relations, University Institute, March 2011.

Eugene E. Habiger, *Cyberwarfare and Cyberterrorism*, White Paper, The Cyber Secure Institute, 1 February 2010.

Seymour M. Hersh, "The Online Threat", *The New Yorker*, 1 November 2010.

Rex Hughes, *Towards a Global Regime for Cyber Warfare*, London, Chatham House, Cyber Security Project, 2009.

Jeffrey Hunker, Bob Hutchinson & Jonathan Margulies, *Role and Challenges for Sufficient Cyber-Attack Attribution*, Institute for Information Infrastructure Protection, Dartmouth College, January 2008.

Lech Janczewski & Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism*, Hershey, Idea Group Inc., 2007.

Paul K. Kerr, John Rollins & Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, Washington D.C., CRS Report for Congress, Congressional Research Service, 7-5700, R41524, 9 December 2010.

Eleanor Keymer, "The cyber-war," *Jane's Defence Weekly*, No. 39, 29 September 2010.

Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Prepared for the US-China Economic and Security Review Commission, McLean, Northrop Grumman Corporation, 9 October 2009.

Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in Franklin D. Kramer, Stuart Starr & Larry K. Wentz, eds., *Cyberpower and National Security*, Washington D.C., National Defense University Press, Potomac Books, 2009.

Ralph Lagner, *The Short Path from Cyber Missiles to Dirty Digital Bombs*, Travis, politicalforum, 26 December 2010.

James A. Lewis & Katrina Timlin, *Cybersecurity and Cyberwarfare*, Preliminary Assessment of National Doctrine and Organization, Washington D.C., Center for Strategic and International Studies (CSIS), UNIDIR Resources, 2011.

James A. Lewis, *Thresholds for Cyberwar*, Center for Strategic and International Studies, September 2010.

Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, RAND Corporation, Project Air Force, 2009.

Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly*, Spring 2011, pp. 132-146.

Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy*, Vol. 4, 2010.

John Markoff, "Cyberwar: Old Trick Threatens the Newest Weapons," *New York Times*, 26 October 2009.

John Markoff, "Webs Anonymity Makes Cyberattack Hard to Trace," *New York Times*, 17 July 2009.

Michael Martine, "Bits before bombs: How Stuxnet crippled Iran's nuclear dreams," *Sapphire*, 3 December 2010.

Andrew Nagorski, ed., Global Cyber Deterrence – Views from China, the US, Russia, India, and Norway, New York, EastWest Institute, April 2010.

Joseph S. Nye, *Cyber Power*, Cambridge, Harvard Kennedy School, Belfer Center for Science and Inter-national Affairs, May 2010.

Marco Roscini, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force," in: A. von Bogdandy & R. Wolfrum, eds., *Max Planck Yearbook of United Nations Law*, Vol. 14, Koninklijke Brill N.V., 2010, pp. 85-130.

Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Colorado Springs, Institute for Information Technology, 1999.

John B. Sheldon, "Lessons Learned: Stuxnet and Cyberpower in War," *World Politics Review*, Cyberwar, Real and Imagined, 19 April 2011.

Shadows in the Cloud: Investigating Cyber Espionage 2.0, Joint Report JR03-2010, Information Warfare Monitor, Shadowserver Foundation, 6 April 2010.

Eric D. Trias & Bryan M. Bell, "Cyber This, Cyber That…So What?," *Air & Space Journal*, Vol. XXIV, No. 1, Spring 2010.

Jody R. Westby, Henning Wegener & William Barletta, *Rights and Responsibilities in Cyberspace – Balancing the Need for Security and Liberty*, New York, EastWest Institute, and Geneva, World Federation of Scientists, 2010.

The Road to Cyberpower, Seizing Opportunity While Managing Risk in the Digital Age, BA10-339, McLean, Booz/Allen/Hamilton, 2010.

"Cyberwar: war in the fifth domain." *The Economist*, 1 July 2010.

"A worm in the centrifuge," *The Economist*, 2 October 2010.

"The meaning of Stuxnet," *The Economist*, 30 September 2010.

"Marching off to cyberwar," *The Economist Technology Quarterly*, 6 December 2008.

Cyber Security

Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models, Arlington, Intelligence and National Security Alliance INSA, November 2009.

Kamlesh Bajaj, The Cybersecurity Agenda – Mobilizing for International Action, New York, EastWest Institute, 2010.

Heiko Borchert & Felix Juhl, Securing Cyberspace – Building Blocks for a Public-Private Cooperation Agenda, Lucerne, Sandfire AG, 2011.

John Blackburn & Gary Waters, *Optimising Australia's Response to the Cyber Challenge*, The Kokoda Foundation, No. 14, February 2011.

David Chaikin, "Network Investigations of cyber attacks: the limits of digital evidence," *Crime, Law and Social Change*, Vol. 46, No. 4-5, 2006.

Georgia Tech Information Security Center (GTISC), Security Summit 2010, Atlanta, *Emerging {Cyber Threats} Report 2011.*

Symantec Global Internet Security Threat Report, Trends for 2009, Mountain View, Vol. XV, Published April 2010.

Sophos security threat report 2011, Sophos Ltd. and Sophos Group, February 2011.

"Pentagon cyber security role expands," *Oxford Analytica: Global Strategic Analysis*, 2 July 2010.

David Shelly, Randy Marchany & Joseph Tront, *Losing the Gap: Analyzing the Limitations of Web Application Vulnerability Scanners*, The OWASP Foundation, Virginia Polytechnic Institute and State University, 8 November 2010.

Peter Sommer & Ian Brown, "Reducing Systemic Cybersecurity Risks," *OECD*, OECD/IFP Project on "Future Global Shocks," 14 January 2011.

Meeting the Cybersecurity Challenge: Empowering Stakeholders and Ensuring Coordination, IBM Corp., U.S. Federal White Paper, Somers, February 2010.

Verizon Business Risk Team, 2009 Data Breach Investigation Report 11, 2009.

Books

John Arquilla & David Ronfeldt, *Networks and Netwars*, Santa Monica, National Defense Research Institute, RAND, 2001.

Mark Bowden, *Worm – The First Digital World War*, London, Grove Press UK, 2011.

Jeffrey Carr, *Inside Cyber Warfare*, O'Reilly Media, Inc., Sebastopol, December 2009.

Richard A. Clarke & Robert K. Knake, *Cyber War – The Next Threat to National Security and What to Do About It,* New York, Harper Collins Publishers, 2010.

James F. Dunnigan, The Next War Zone: Confronting the Global Threat of Cyberterrorism, New York, Citadel Press, 2002.

Edward Yourdon, Byte Wars – The Impact of September 11 on Information Technology, Upper Saddle River, Prentice Hall PTR, 2002.

Daniel Ventre, et al, ed., *Cyberwar and Information Warfare*, London & Hoboken, NJ, ISTE Ltd and John Wiley & Sons, Inc., 2011.

About the series

We will be obliged in the years to come to broaden our analytical horizons way beyond current SSR and SSG approaches. There is a growing urgency to move beyond the first revolution in this area that led to the "whole of government" approach towards a second revolution, one that leads to a fully integrated security sector approach that reaches beyond established state structures to include select private companies – and thus permit, what we might call, a "whole of issues" approach.

Horizon 2015 working papers provide a short introductions to live issues on the SSG/SSR agenda. The papers, of course, do not seek to solve the issues they address but rather to provide a platform for further work and enquiry. As such, they ask many more questions than they answer. In addition to these working papers, the project has published an occasional paper – *Trends and Challenges in International Security: An Inventory* – that seeks to describe the current security landscape and provide a background to the project's work as a whole.

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) is one of the world's leading institutions in the areas of security sector reform and security sector governance. DCAF provides in-country advisory support and practical assistance programmes, develops and promotes appropriate democratic norms at the international and national levels, advocates good practices and conducts policy-related research to ensure effective democratic governance of the security sector.

Visit us at: www.dcaf.ch

DCAF Geneva
P.O. Box 1360
1211 Geneva 1
Switzerland

Tel: +41 (22) 741 77 00
Fax: +41 (22) 741 77 05

DCAF Brussels
Place du Congrès 1
1000 Brussels
Belgium

Tel: +32 (2) 229 39 66
Fax: +32 (2) 229 00 35

DCAF Ljubljana
Dunajska cesta 104
1000 Ljubljana
Slovenia

Tel: +386 (1) 5609 300
Fax: +386 (1) 5609 303

DCAF Ramallah
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank, Palestine

Tel: +972 (2) 295 6297
Fax: +972 (2) 295 6295

DCAF Beirut
P.O. Box 113 - 6041
Beirut
Lebanon

Tel: +961 (1) 738 401
Fax: +961 (1) 738 402