CHAPTER

4

Cyber Doctrine

INFORMATION IN THIS CHAPTER

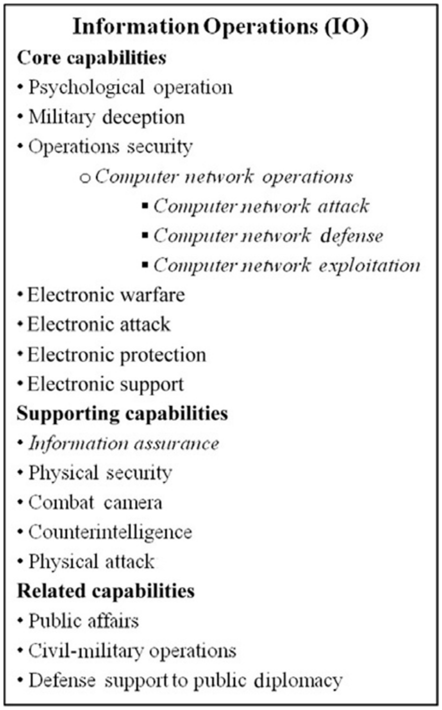
- Current U.S. Doctrine
- Sample Doctrine/Strategy from Around the World
- Key Military Principles That Must Be Adapted to Cyber Warfare
- Guidance and Directives
- Operations and Exercises

Doctrine is the fundamental principle by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application [1]. Doctrine is what militaries base their plans on and it is influenced by tradition, guides, and tactics, techniques, and procedures (TTPs). We will cover what doctrine exists today, what doctrine needs to be translated to cyberspace, what adjacent guidance exists in non-military agencies, and, finally, what exercises are being conducted to develop doctrine.

CURRENT U.S. DOCTRINE

The U.S. military does not have a definition for cyber warfare today. Over time this capability has been called computer security, Information Security (InfoSec), Net Centric Warfare, Information Assurance (IA), Information Warfare, Cybersecurity, and now Cyber Warfare. These terms generally focused on the defense; today when military planners use the term cyber they include offensive capabilities as well. Cyber is generally understood to be Computer Network Operations (CNO). There are three functions under CNO: Computer Network Exploitation (CNE), Computer Network Attack (CNA), and Computer Network Defense (CND). These functions map to traditional doctrinal terms: CNE is not what most security professionals think of as exploiting a system by compromising it but is focused on

http://dx.doi.org/10.1016/B978-0-12-416672-1.00004-0



Information Operations (IO)

Core capabilities

- Psychological operation
- Military deception
- Operations security
    - *Computer network operations*
        - *Computer network attack*
        - *Computer network defense*
        - *Computer network exploitation*
- Electronic warfare
- Electronic attack
- Electronic protection
- Electronic support

Supporting capabilities

- *Information assurance*
- Physical security
- Combat camera
- Counterintelligence
- Physical attack

Related capabilities

- Public affairs
- Civil-military operations
- Defense support to public diplomacy

FIGURE 4.1 Information operations framework.

reconnaissance or espionage and will be covered in Chapter 9, CNA is offense and is covered in Chapter 10, and CND is defensive operations, which are examined in Chapter 11.

CNO falls under Information Operations (IO) which has a set of core, supporting, and related capabilities (see Figure 4.1 for details). There are two areas that overlap: CNO and Information Assurance (IA). CNO is defined by the three functions listed above while IA is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities [1]. So we can think of IA as building and maintaining the networks while CNO is planning and conducting battle on them, much like the difference between maintaining the Tanks in an Armor Battalion and using them to fight a battle.

There are some concerns with how cyber doctrine is being developed today. The key Joint doctrine for cyber (JP 3-13) was published in 2006. Doctrine is not normally updated quickly, so when we have the environment operating under Moore's Law (capabilities doubling every 18 months) there is concern that the doctrine will quickly become out of date. Another potential issue is that the services do not follow the same terminology; for example the Army and the Air Force have different definitions of Information Operations. Then there is the challenge of having much of the doctrine classified. This leads to different groups having access to different information and basing decisions on only the information they have access to. Finally there is the problem with basic attitude on the importance of cyber as part of combat operations with some leaders' belief that cyberspace is only a supporting function for administrative activities, while others feel cyberspace is embedded in everything from today's command and control systems to the weapons systems and it is the critical center of gravity for the nation (often this division runs along the lines of techies and luddites).

U.S. Forces

The White House released its International Strategy for Cyberspace in May 2011 with focus on prosperity, security, and openness in a networked world. "The United States will pursue an international cyberspace policy that empowers the innovation that drives our economy and improves lives here and abroad. In all this work, we are grounded in principles essential not just to American foreign policy, but to the future of the Internet itself. Focus on freedom of information and privacy" [1]. It has an overall goal with key diplomatic and defensive objectives:

- *Goal*: the United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace.
- *Diplomatic Objective*: the United States will work to create incentives for, and build consensus around an international environment in which states—recognizing the intrinsic value of an open, interoperable, secure, and reliable cyberspace—work together and act as responsible stakeholders.
- *Defense Objective*: the United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these vital national assets as necessary and appropriate.

The Department of Defense (DoD) Strategy for Operating in Cyberspace was released in July 2011 and has five initiatives:

- Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.
- Strategic Initiative 2: Employ new defense operating concepts to protect DoD networks and systems.
- Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.
- Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity.
- Strategic Initiative 5: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

U.S. Cyber Command (CYBERCOM) has been given responsibility for cyberspace operations and must execute the strategies listed above. In a memo signed 23 June 2009, the U.S. Secretary of Defense established the new command [2]. General Keith Alexander (who is also the current director of the NSA) is its first Commander and in 2010 statement to Congress said, "The Department of Defense networks that we defend are probed roughly

250,000 times an hour" [2]. As early as 2006 the Department determined that 10-20 TB of data had been remotely exfiltrated from NIPRNet [2]. General Alexander then quoted Deputy Secretary William Lynn's 2010 comment that the key function for CYBERCOM is its "linking of intelligence, offense, and defense under one roof" [2]. The National Security Agency (NSA) contributes essential expertise to accomplish this. General Alexander further explained to Congress in his 2010 statement, "U.S. Cyber Command has three main lines of operation. We direct the operations and defense of the Global Information Grid so the Department of Defense can perform its missions, we stand ready to execute full-spectrum cyber operations on command, and we stay prepared to defend our U.S. nation's freedom of action in cyberspace" [2]. Cyber Command will use five principles for the Department's strategy in cyberspace: remember that cyberspace is a defensible domain; make our U.S. defenses active; extend protection to our critical infrastructure; foster collective defenses; and leverage U.S. technological advantages [3]. This focus on bringing cyber doctrine and policy to the highest level of command in the military shows how much emphasis the leadership is placing on this new warfighting domain. There is not a lot of money to make this happen until the new Command catches up with the DoD Program Objective Memorandum (POM) budgeting cycle, so DoD has had to reallocate funds, but they are making this happen now because they feel it is vital to the future success of the military. With sequestration and continuous resolutions in the U.S. it is not clear when they will be part of the annual budget cycle.

While this command has been stood up the Honorable W. "Mac" Thornberry Chairman of Subcommittee on Emerging Threats and Capabilities Committee on Armed Services House of Representatives has called out the fact "DOD does not yet have an overarching budget estimate for full-spectrum cyberspace operations including computer network attack, computer network exploitation, and classified funding. During February and March 2011, 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) that included different elements of DOD's cybersecurity efforts [4]. The three budget views are largely related to the Defense-wide Information Assurance Program and do not include all full-spectrum cyber operation costs, such as computer network exploitation and computer network attack, which are funded through classified programs from the national intelligence and military intelligence program budgets" [5].

NOTE

The key to understanding where the authority controlling cybersecurity is the same as any other function of the government: follow the money. A new command or presidential directive without funding is more posturing than executing a plan of action. Naming someone into a new position or declaring a new committee that does not have budget authority is more public relations than fixing a problem. When we look at a lot of the activity it is vital to see who controls the resources.

Joint Doctrine

The 2013 compendium of Key Joint Doctrine Publications noted that the pace at which Joint doctrine changes has accelerated in recent years. "One third of approved joint publications have been revised or new ones created in just the last two years ... Approximately 41% of the joint publications are under revision or in development." [6] Doctrine is still focused on joint and multinational integration of forces but now must deal with irregular warfare/counterinsurgency, U.S. Federal interagency coordination, counterterrorism, various humanitarian assistance and civil support operations, support to homeland security, national communications strategy and cyberspace operations.

Recent updates to Joint Pub 1 Doctrine for the Armed Forces of the United States published in 2013 have incorporated cyber into the two basic forms of warfare (traditional and irregular). A useful dichotomy for thinking about warfare is the distinction between traditional and irregular warfare (IW). Traditional warfare is characterized as a violent struggle for domination between nation-states or coalitions and alliances of nation-states. With the increasingly rare case of formally declared war, traditional warfare typically involves force-on-force military operations in which adversaries employ a variety of conventional forces and special operations forces against each other in all physical domains as well as the information environment (which includes cyberspace). IW is characterized as a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). In IW, a less powerful adversary seeks to disrupt or negate the military capabilities and advantages of a more powerful military force, which usually serves that nation's established government [7]. This formal recognition of cyber shows commanders are looking at cyberspace and cyber operations as part of both their operational environment and as a capability that can be employed.

Joint Publication 3-13 Information Operations published 27 November 2012 focuses on IO being a force multipliers to create a desired effect. There are many military capabilities that contribute to IO and should be taken into consideration during the planning process. These include: strategic communication, joint interagency coordination group, public affairs, civil-military operations, cyberspace operations (CO), information assurance, space operations, military information support operations (MISO), intelligence, military deception, operations security, special technical operations, joint electromagnetic spectrum operations, and key leader engagement. The two key aspects of cyber warfare, cyberspace operations and information assurance, are defined below [7]. It is important to note there is a move away from the current definition of Information Operations which includes Computer Network Operations (composed of Attack/Defend/Exploit) to cyberspace operations and information assurance.

- Cyberspace Operations (CO)
  a. Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. CO is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace capabilities, when in support of IO, deny or manipulate adversary or potential adversary decision making, through targeting an information medium (such as a wireless access point in the physical dimension), the message itself (for example, an encrypted message in the information dimension), or a cyber-persona (an online identity that facilitates communication, decision making, and the influencing of audiences in the cognitive dimension). When employed in support of IO, CO generally focuses on the integration of offensive and defensive capabilities exercised in and through cyberspace, in concert with other IRCs, and coordination across multiple lines of operation and lines of effort.

b. a process that integrates the employment of IRCs across multiple lines of effort and lines of operation to affect an adversary or potential adversary decision maker, IO can target either the medium (a component within the physical dimension such as a microwave tower) or the message itself (e.g., an encrypted message in the informational dimension). CO is one of several IRCs available to the commander.

- Information Assurance. IA is necessary to gain and maintain information superiority. The Joint Forces Commander relies on IA to protect infrastructure to ensure its availability, to position information for influence, and for delivery of information to the adversary. Furthermore, IA and CO are interrelated and rely on each other to support IO.

The inclusion of the cyberspace domain, cyber operations and evolution of doctrine at the strategic, operational and tactical level shows that the DoD is endeavoring to keep pace with military/doctrinal intricacies of the information age.

Finally a new addition to the doctrinal library is being published. “JP 3-12, Joint Cyberspace Operations, was initiated based on the National Military Strategy for Cyberspace Operations Implementation Plan, which directed USSTRATCOM to assess joint doctrine in support of operations in cyberspace and the five National Military Strategy Cyberspace Operations Ends. Initially a joint test publication (JTP), there was unanimous support by the joint doctrine development community to end development of the JTP and instead develop a Joint Publication (JP). This JP will address the uniqueness of military operations in cyberspace, clarify cyberspace operations-related command and operational interrelationships, and incorporate operational lessons learned” [7]. This will be a classified document.

The Joint Operational Access Concept (JOAC) of Jan 2012 envisions a greater degree and more flexible integration of space and cyberspace operations into the traditional air-sea-land battlespace than ever before. Three emerging trends in the operating environment promise to complicate the challenge of opposed access for U.S. joint forces: (1) The dramatic improvement and proliferation of weapons and other technologies capable of denying access to or freedom of action within an operational area, (2) the changing U.S. overseas defense posture, and (3) the emergence of space and cyberspace as increasingly important and contested domains [7]. As the U.S. military is predominantly a force projection capability they must ensure they address these new trends to ensure operational freedom.

NOTE

In February 2013 Defense Secretary Leon Panetta announced the creation of the Distinguished Warfare Medal, to recognize “extraordinary achievements that directly impact on combat operations, but do not involve acts of valor or physical risks that combat entails.” The medal will rank immediately below the Distinguished Flying Cross—higher than the Bronze Star—in order of precedence, according to a Defense Department chart. It can be awarded for any actions after September 11, 2001 [8]. This addition of a medal can be applicable to cyber warriors, and is a significant recognition of the importance of the domain.

One challenge the military faces is highlighted by Colonel U.S. Army Bryant David Glando in “Cyber Warfare —A New DoD Core Mission Area.” The new primary and current core mission areas do not adequately address cyberspace warfare as a way to shape the National

Security Strategy (NSS) of the United States. However, they subsume cyberspace capabilities as a service enabler across all the mission areas. This approach does not address the art of the possible, but limits the U.S. in its ability to develop a strategic approach using cyberspace capabilities as a means to achieve strategic objectives. Cyberspace warfare that uses cyberspace capabilities to conduct cyberspace operations could ensure the U.S. achieves its national security objectives. These issues are being addressed but highlights that most of the capabilities are service-specific.

U.S. Air Force

The first U.S. Air Force commander of 24th NAF Major General Richard E. Webber in 2010 told Congress his number one priority for 24th AF is developing and improving cyberspace situational awareness. The 24th has also established a Cyber Operations Liaison Element (COLE) to act as liaison officers (LNO) to facilitate the requisite exchange of expertise between mission planners and cyber planners [9]. The Air Force has made the earliest efforts to establish cyber operations integration into their forces. They were the first to move to stand up a cyber command unit, and have aggressively tried to take the lessons learned from developing doctrine and organizational structure for space and apply it to cyberspace.

United States Air Force published their Cyberspace Science and Technology Vision 2012-2025 in Dec 2012. It states, “Cyberspace is essential to all Air Force (AF) missions. It is the only service to not stand its subordinate command up at Fort Meade but collated with its key cyber units in San Antonio. It is a domain in which, from which, and through which AF operations are performed. Actions in cyberspace can have digital, kinetic, and human effects. Increasingly, the cyberspace domain is contested and/or denied. Yet our ability to address opportunities and threats is constrained by time, treasure, and talent.” and has the following recommendations:

- Assuring, empowering and enhancing mission system security standards, making more effective use of authorities (e.g., Title 10/50/32), synchronizing multi-domain effects, and increasing the cost of adversary cyberspace operations.
- Improving cyber accessions and education and developing Air Force Cyberspace Elite (ACE) forces.
- Requiring and designing-in security and securing weapon systems throughout their full life cycle.
- Rapid, open, and iterative acquisition that engages user and test communities early.
- Integrating cyber across all core functions, advancing partnerships, aligning funding, and orchestrating effort and effects across domains.
- Complexity reduction to ease verification and reduce life cycle cost, the development of trusted and self-healing networks and information, the creation of agile, resilient, disaggregated mission architectures, and the advancement of real-time cyber situational awareness/prediction and cyber S&T intelligence across all Air Force domains of operation.
- Using science and technology to improve foundations of trust, enhance human machine interactions, enhance agility and resilience, and assure and empower missions, in collaboration with the Air Force’s partners.

The Air Force also published Air Force Instruction 51-402 *Legal Reviews of Weapons and Cyber Capabilities* in 2011 which states the Judge Advocate General will "Ensure all weapons being developed, bought, built, modified, or otherwise being acquired by the Air Force that are not within a Special Access Program are reviewed for legality under Law of Armed Conflict (LOAC), domestic law and international law prior to their possible acquisition for use in a conflict or other military operation." This public statement shows the challenge faced by commanders in deploying their cyber weapons. This statement applies to the U.S. military which operates under U.S. title 10 codes for legal authority, the intelligence agencies operate under U.S. title 50 codes.

U.S. Navy

The U.S. Navy is moving out to develop their cyber capabilities as well. Retired Vice Admiral David J. "Jack" Dorsett, the first Deputy Chief of Naval Operations for Information Dominance (N2/N6) and Director of Naval Intelligence (DNI), in his Information Dominance and the U.S. Navy's Cyber Warfare Vision stated that the Navy is prominent and dominant in the fields of ISR, Cyber Warfare, C2, and Information & Knowledge Management, and as information becomes a Main Battery of U.S. Navy warfighting capability, warfighting wholeness will replace today sub-optimal stovepipes. The Navy will move from platform-centric to information-centric processes, into unmanned, machine autonomous technologies, and create a fully-integrated intel, C2, and Cyber & Networks Capability. Finally they will focus on the following principles: every platform is a sensor; every sensor is networked; build a little, test a lot; spiral development/acquisition; plug-n-play sensor payloads; reduce afloat/airborne manning; transition to remoted; automated; one operator controls multiple platforms; and emphasize UAS and autonomous platforms [10]. The Navy looked to its history and wanted to take lessons learned from standing up the 10th fleet during World War II to deal with the new submarine threat and apply that same methodology of innovation and focus on how new technology is impacting the battlespace. They have made some hard choices like reorganizing the staff functions to increase efficiencies and integration by joining the N2 (Intelligence) and N6 (Communications/Networks) functions into the Information Dominance directorate. These changes show the level of importance and time sensitivity the Navy is placing on the potential for cyber warfare. They do not want to be caught preparing to fight the last war.

The current Deputy Chief of Naval Operations for Information Dominance Director of Naval Intelligence Vice Admiral Kendall L. Card recently stated, "Whether characterized as cyber, intelligence, surveillance, reconnaissance, networks, communications, space, meteorology, oceanography, or electronic warfare, the Navy is inextricably and irreversibly dependent on information. In fact, I would argue that information lies at the core of the Navy's missions of sea control, power projection, deterrence and forward presence. The degree to which we master and control information will yield either a decisive operational advantage or an incapacitating weakness. Therefore, mastering the information domain is critical to the Navy's success. We refer to that mastery as information dominance—the advantage gained from fully integrating the Navy's information functions, capabilities and resources to optimize decision making and maximize war fighting effects" [11].

The Navy has also recently published their view of cyber in "Navy Cyber Power 2020 – Sustaining the US global leadership: priorities for 21st century defense" in Nov 2012. The Navy vision is that cyberspace operations provide Navy and Joint commanders with an operational advantage by [12]:

- Assuring access to cyberspace and confident C2. The Navy operates, defends, exploits, and engages in cyberspace effectively to ensure Navy forces retain access to cyberspace for all mission critical functions and to provide Navy and Joint commanders with resilient C2 capabilities.
- Preventing strategic surprise in cyberspace. The Navy effectively evaluates adversary actions in cyberspace through dedicated cyber intelligence collections and analysis and by fully integrating timely and relevant cyber information and threat warnings into the commander's operational picture.
- Delivering decisive cyber effects. The Navy delivers cyber effects at a time and place of its choosing across the full range of military operations in support of commanders' objectives.

U.S. Army

The U.S. Army's is formally addressing cyber doctrine development today. The primary Field Manual is FM 3-13 which was called Information Operations but was renamed Inform and Influence Activities in January 2013. This is based on the view that IO was looked at as a shaping operations. Army Doctrine Reference Publication (ADRP) 3-0 (which superseded FM 3-0) refined the elements of combat power so the mission command warfighting function includes two staff tasks—conduct inform and influence activities (IIA) and conduct cyber electromagnetic activities—as well as additional tasks of conducting military deception and information protection. The Army's concept of IIA is the integration of information-related capabilities that informs and influences audiences simultaneously. They view Cyber electromagnetic activities as the combination of electronic warfare, cyberspace operations and electromagnetic spectrum management operations [7].

The U.S. Army's key units are 1st Information Operations Command (Land), the 780th Military Intelligence Brigade at Fort Meade, the theater information operations groups, and supporting elements. The key officer skill is the Army functional area, 30 officers who are trained for the role of a joint information operations planner.

The U.S. Army Training and Doctrine Command (TRADOC) has coordinated concept development for cyber with stakeholders across the Army, and in January 2013 published a Cyberspace Operations Concept Capabilities Plan (CCP) which outlines the framework under which the Army expects to conduct cyber operations in the timeframe 2016-2028. They are focusing on three dimensions of cyber in the current operational environment: psychological contest of wills, strategic engagement, and the cyber-electromagnetic contest. Commanders seek to retain freedom of action in cyberspace and in the electromagnetic spectrum, while denying the same to adversaries at the time and place of their choosing; thereby enabling operational activities in and through cyberspace and consequently the other four domains. CyberOps encompass those actions to gain the advantage, protect that advantage, and place adversaries at a disadvantage in the cyber-electromagnetic contest. CyberOps

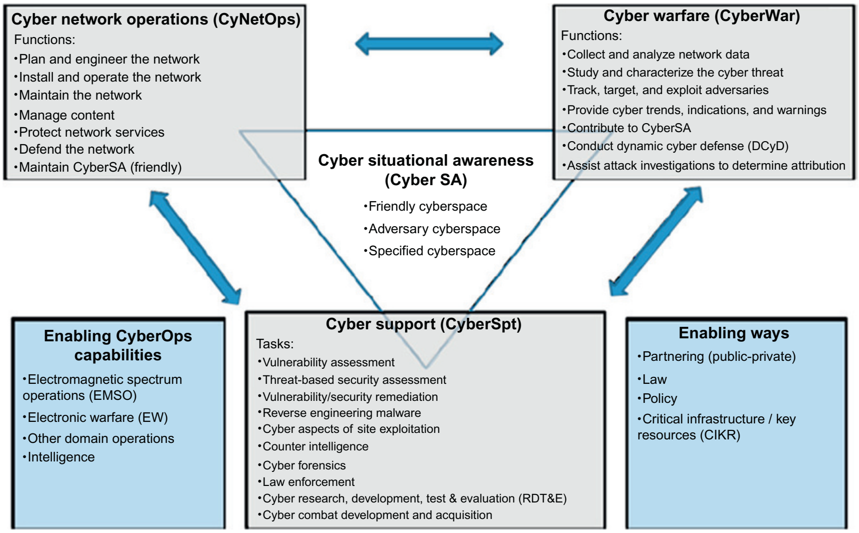

Cyber network operations (CyNetOps)
Functions:
•Plan and engineer the network
•Install and operate the network
•Maintain the network
•Manage content
•Protect network services
•Defend the network
•Maintain CyberSA (friendly)
Cyber warfare (CyberWar)
Functions:
•Collect and analyze network data
•Study and characterize the cyber threat
•Track, target, and exploit adversaries
•Provide cyber trends, indications, and warnings
•Contribute to CyberSA
•Conduct dynamic cyber defense (DCyD)
•Assist attack investigations to determine attribution
Cyber situational awareness (Cyber SA)
•Friendly cyberspace
•Adversary cyberspace
•Specified cyberspace
Enabling CyberOps capabilities
•Electromagnetic spectrum operations (EMSO)
•Electronic warfare (EW)
•Other domain operations
•Intelligence
Cyber support (CyberSpt)
Tasks:
•Vulnerability assessment
•Threat-based security assessment
•Vulnerability/security remediation
•Reverse engineering malware
•Cyber aspects of site exploitation
•Counter intelligence
•Cyber forensics
•Law enforcement
•Cyber research, development, test & evaluation (RDT&E)
•Cyber combat development and acquisition
Enabling ways
•Partnering (public-private)
•Law
•Policy
•Critical infrastructure / key resources (CIKR)

FIGURE 4.2 Cyber Net Ops.

are not an end to themselves, but rather an integral part of full spectrum operations and include activities prevalent in peacetime military engagement, which focus on winning the cyber-electromagnetic contest. CyberOps are continuous; engagements occur daily, most often without the commitment of additional forces. Consequently, the framework developed for Army Operations establishes four components for CyberOps: cyber warfare (CyberWar), cyber network operations (CyNetOps), cyber support (CyberSpt), and cyber situational awareness (CyberSA). See Figure 4.2 for how they interrelate [13]. The Army is the service that focuses the most on publishing doctrine. They integrate it in their school house curriculum (at every level) as a way to push new doctrine into the field. This is a different approach from the other services that are focused on reorganization; the Army wants to reeducate their force to understand the new environment.

DoD INFOCONs

The last thing we will cover in current U.S. military doctrine is Information Operations Condition (INFOCON) system procedures [14]. This is the guidance for all DoD systems to direct the state of the defensive posture the military networks must take when under attack. The INFOCON increases from 5 to 1 when under more severe attacks.

- INFOCON 5 (normal activity). This is the normal state of readiness of information systems and networks (i.e., "Routine" Network Operations (NetOps)) that can be sustained indefinitely. System and network administrators will create and maintain a snapshot of each server and workstation in a normal operational condition. This snapshot then becomes the normal operational baseline that can be compared against future changes to identify unauthorized activities.
- INFOCON 4 (increased vigilance procedures). System and network administrators will establish an operational rhythm to validate the known good image of an information

network against the current state and identify unauthorized changes. Additionally, user profiles and accounts are reviewed and checks are conducted for dormant accounts. Impact to end-users should be negligible.

- INFOCON 3 (enhanced readiness procedures). System and network administrators will further NetOps readiness by increasing the frequency of validation of the information network and its corresponding configuration. Impact to end-users should be minor.
- INFOCON 2 (greater readiness procedures). System and network administrators will increase the frequency of validation of NetOps readiness for the information network. Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.
- INFOCON 1 (maximum readiness procedures). This is the highest condition of NetOps readiness. This condition addresses intrusion techniques that cannot be identified or defeated at lower readiness levels. During INFOCON 1, System and Network Administrators may reload the operating system software on key infrastructure servers from an accurate baseline. Once baseline comparisons no longer indicate anomalous activities, INFOCON 1 would be terminated. Impact to end-users could be significant for short periods, which can be mitigated through training and scheduling.
- Tailored Readiness Options (TROs). TROs are supplemental measures to respond to specific intrusion characteristics. They are narrowly focused and meant to supplement the current INFOCON readiness level. TROs will document, in standard language, all supplemental INFOCON measures to ensure a common understanding of the level of readiness and mission impact of each measure.

There are some issues: these INFOCONs are not regularly exercised and there is some doubt as to the viability of the current IT staffs to be able to execute this intensive schedule. The good news is these are much better reaction guidelines than the old set which led to organizations disconnecting themselves during an attack causing a self denial of service. Any local commander can increase the level of INFOCON but may not lower the level of protection below the next higher command. Finally, a TRO is a unique reaction to a specific threat; the most recent example is the reaction to malware on thumb drives. DoD disallowed the use of thumb drives deciding that the operational impact of losing the capability was less than the threat of compromising their network.

WARNING

When dealing with an attack or intrusion, the normal response is to recover systems as soon as possible. This will often destroy evidence necessary to determine how the systems were compromised in the first place. If we do not do the forensic work before the reload, it will be impossible to figure out what we need to fix to prevent the threat from coming right back. The key is to ensure we have a process to preserve the evidence offline while the systems are recovered.

SAMPLE DOCTRINE/STRATEGY FROM AROUND THE WORLD

We will now review some of the cyber doctrine and strategies being developed by other nations. We will start with China and some of the other major Asian countries, and then cover

European countries. While Russia is a major player, most of their impact is in crime versus warfare so we will not call them out uniquely. Iran is active and trying to be a major player in cyber but there is not much open source information on what their national cyber strategy is. Finally, we will look at possibility of private or mercenary organizations. These countries are meant to be a sampling of cyber stratagems rather than a holistic representation of the cyber strategy landscape.

Background

There have been some studies that shed light on broad trends. The RAND Corporation's study "Cyber-security threat characterization: A rapid comparative analysis" prepared for the Center for Asymmetric Threat Studies (CATS), Swedish National Defence College, Stockholm does a great job breaking out the nations by focus [15]. Below are two of the many countries analyzed as an example of what the report covers:

Comparator	**Level of Prioritization**	**Characterization of Threat**	**Lead Responding Authority**
Russian Federation	Most prominent	Internal (crime and corruption)	Security Council of the Federation/Ministry of Defence
		External (state, terrorists, foreign competition)	National system of information protection and intelligence community
USA	Priority (one of four)	Criminal hackers Organized criminal groups Terrorist networks Advanced nation	Distributed across a number of organizations with inter-agency policy committee

The "*Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization*" report by the Center for Strategic and International Studies (CSIS) is a useful reference. Using open-source literature, CSIS reviewed policies and organizations in 133 states to determine how they are organized to deal with cybersecurity, whether they have a military command or doctrine for cyber activities, and whether they have or plan to acquire offensive cyber capabilities. There are clear limitations to open-source data. CSIS identified 33 states that include cyberwarfare in their military planning and organization. These range from states with very advanced statements of doctrine and military organizations employing hundreds or thousands of individuals to more basic arrangements that incorporate cyberattack and cyberwarfare into existing capabilities for electronic warfare. They also discuss another 36 states where there is no public discussion of a military role in cyberspace and where civilian agencies charged with internal security missions, computer security or law enforcement are responsible for cybersecurity [15]. This is a great reference for finding a half page summary of country doctrinal positions.

These and other studies show a continued trend toward public declarations of national cyber strategies, formal policy and doctrine, standing up of military and civilian agencies charged with cyber missions and ensuring all elements of national power are secure. Following are examples on some key countries and their doctrinal/strategic activities.

Chinese Doctrine

The first nation we will look at is China. As early as 1999, China was developing doctrine on how to compensate for military technological inferiority against the United States. Some of their senior strategists published a document called “Unrestricted Warfare.” It was insightful that they were thinking about the value of network warfare already, but statements like, “Technology is like ‘magic shoes’ on the feet of mankind, and after the spring has been wound tightly by commercial interests, people can only dance along with the shoes, whirling rapidly in time to the beat that they set” [16], shows how differently a culture can shape how doctrine is developed.

Taiwan watches Chinese strategies very closely, and published a good analytical review of new doctrine being considered by the People’s Liberation Army (PLA) [17]. The following is a list of the more pertinent concepts:

- Highly controlled war is a new form of warfare in which “the direct purpose is to control a political regime, and in which political, economic, diplomatic, and other resources are integrated effectively to control the scale, form, means, and results of the war, with the backing of absolute military superiority.”
- Acupuncture war establishes the examination of critical points in a network. Much like the pressure points in martial arts, when taken out, this type of war can shut down an entire system. Here, using Electronic Warfare (EW) can enable “the first battle being the final battle.”
- Strategic information war is the integration of political, economic, military, diplomatic, and other areas to produce an overall or comprehensive information victory. The targets of strategic Information Warfare (IW) include national political, monetary, communications, and other crucial sectors down to single weapon systems such as aircraft carriers.
- Work Web sites establish distant learning capabilities and databases for quick access to information not readily available in the past.
- Intangible war focuses on strategies, market competition, legal systems, and intellectual property rights.
- Net Force is a brand new type of “Grand War” scheme that combines high-tech knowledge with politics, economy, psychology, and information networks and that is “all people being soldiers, the integration of peace and warfare, and dual usage for the military and civilians.”
- Surgical warfare aims to attack the vulnerability of high-tech weapons systems to achieve final victory, namely, attacking one point to cripple the whole system.
- Space warfare capability puts the crowning touch on China’s asymmetric warfare capability: the ability to sabotage or destroy an enemy’s space systems.

The US-China Economic and Security Review Commission Report on the *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* states “The government of the People’s Republic of China (PRC) is a decade into a sweeping military modernization program that has fundamentally transformed its ability to fight high-tech wars. The Chinese military, using increasingly networked forces capable of communicating across service arms and among all echelons of command, is pushing beyond its traditional missions focused on Taiwan and toward a more regional defense posture. This modernization effort, known as informationization, is guided by the doctrine of fighting 'Local War Under Informationized Conditions,' which refers to the PLA's ongoing effort to develop a fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the electromagnetic spectrum" [18]. This open source study reveals how seriously China is modernizing their Cyber Forces for today's ongoing cyber war and the next integrated kinetic/non-kinetic war.

The Annual Report to Congress Military and Security Developments Involving the People's Republic of China 2011 states that China's development of capabilities for cyber warfare is consistent with authoritative PLA military writings. Two military doctrinal writings, Science of Strategy and Science of Campaigns identify information warfare (IW) as integral to achieving information superiority and an effective means for countering a stronger foe. Although neither document identifies the specific criteria for employing computer network attack against an adversary, both advocate developing capabilities to compete in this medium.

In a separate report it was pointed out that as few as 12 different Chinese groups, largely backed or directed by the government there, do the bulk of the China-based cyberattacks stealing critical data from U.S. companies and government agencies, according to U.S. cybersecurity analysts and experts. The aggressive, but stealthy attacks, which steal billions of dollars in intellectual property and data, often carry distinct signatures allowing U.S. officials to link them to certain hacker teams. And, analysts say the U.S. often gives the attackers unique names or numbers, and at times can tell where the hackers are and even who they may be [19]. This targeting can result in accusations and political posturing but to date no military action has been authorized. Much like the Cold War it is more about gathering information, but unlike the Cold War where military capabilities were displayed as part of a show of force but not used, today many of the cyber weapons are being actively used.

From WikiLeaks documents, and several other sources, the identity and location of the main Chinese Cyber War operation is now known. The Chinese Chengdu Province First Technical Reconnaissance Bureau (1st TRB) is a Chinese Army electronic warfare unit located in central China (Chengdu), and is the most frequent source of hacking attacks traced back to their source. The servers used by the 1st TRB came online over five years ago, and are still used. The Chinese government flatly refuses to even discuss the growing pile of evidence regarding operations like the 1st TRB [20]. So we can see China is using both civilian hackers and military Computer Network Attack units to engage in cyber operations.

TIP

The information being posted to WikiLeaks has changed the paradigm of insider threats. Both commercial and government organizations are now relooking at internal trust. With hackers breaking in and posting information to Wikileaks and insiders handing over large amounts of data that reporters can pour through, it is time for senior leaders to reevaluate their insider protections and risk acceptance.

What does all this focus on modernization and cyber doctrine mean? The level of effort and types of activities mentioned above show that China is preparing to fight the next war utilizing the electromagnetic spectrum and plans to deny access to its enemy. China understands how dependent the West has become on the IT infrastructure, and will attack that center of gravity. It is conducting reconnaissance today that will give it the advantage. China has the infrastructure to conduct denial of service attacks, and has talked about attacking the integrity of systems so an enemy cannot trust its command and control systems to give accurate reports. China is not alone in this level of cyber warfare doctrinal development but they are in the front of the pack.

The recent "APT1 Exposing One of China's Cyber Espionage Units" by Mandiant specifies that APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. The report estimates that Unit 61398 is staffed by hundreds, and perhaps thousands of people based on the size of Unit 61398's physical infrastructure [21].

Similarly, Bloomberg BusinessWeek magazine February 2013 also had a cover story on how Joe Stewart of Dell SecureWorks tracked down the specific individual responsible for the APT malware he was investigating. "There is a tremendous amount of manpower being thrown at this from their side," Joe says. Investigators at dozens of commercial security companies suspect many if not most of those hackers either are military or take their orders from some of China's many intelligence or surveillance organizations. In general, they say the attacks are too organized and the scope too vast to be the work of freelancers. Secret diplomatic cables published by WikiLeaks connected the well-publicized hack of Google to Politburo officials, and the U.S. government has long had classified intelligence tracing some of the attacks to hackers linked to the People's Liberation Army (PLA), according to former intelligence officials. None of that evidence is public, however, and China's authorities have for years denied any involvement [22]. These two examples of commercial companies that are uncovering espionage while protecting commercial companies show the level of activity that is going on today.

Other Asian Countries

Japan has placed their strategy under the Japanese Ministry of Defense (MoD) Self-Defense Forces National Information Security Center (NISC). In 2005, NISC was established following a surge in cyberattacks. The government-wide agency was set up to co-ordinate efforts to protect computer networks. In February 2009, the Japanese government adopted the Second National Strategy on Information Security (NSIS) for the years 2009-2011. The 3-year plan included four subjects: central and local governments, critical infrastructure, business entities, and individuals. As part of the NSIS process, the Japanese government adopted "Secure Japan 2009." One-fourth of its 212 policy items are aimed at the improvement of central and local governments. In the areas devoted to critical infrastructure and business entities, private enterprises serve as the subjects of its actions while the government provides support [23]. Japan is developing cyber doctrine with a broader government focus; they want to ensure the country is secure from attacks, and are willing to leverage their military capabilities to achieve it.

South Korea and North Korea: South Korea's Defense Security Command (DSC) and the Ministry of National Defense (MND) stated in December 2009 that hackers had accessed classified military plans drawn up by South Korea and the U.S. Details of "Operation Plan 5027," which outlines how South Korea would be defended in the event of war, were said to have been transferred to an internet protocol (IP) address in China but thought to be compromised. The reaction was to stand up a cyber warfare command to protect its military computer systems, the plans are part of the ministry's strategy known as "Defense Reform 2020" [24]. The Korea Internet & Security Agency (KISA) was also formed in 1996 to promote internet cooperation and security.

North Korea has built capabilities under Unit 121, which was stood up in 1998. The mission is to increase their military standing by advancing their asymmetric and cyber warfare capabilities through both offensive and espionage methods. This unit is trained by the Mirim Academy in Pyongyang. Their annual budget is estimated to be ~$56M [25]. With the struggle on the Korean peninsula still going on, it is easy to see why North Korea would carry the battle to cyberspace. This could give North Korea an advantage as it is not as dependent on IT infrastructure as most countries, but at the same time it will have to come a long way to overcome the lack of a computer workforce to draw from.

Terrorists have no formal published doctrine but they are very interested in understanding the doctrine of the countries that they want to attack. It would be important to know what a country's response to specific attacks would be in order to plan attacks that accomplish their objectives. They also have many locally developed doctrinal practices for reconnaissance, communication, and recruiting on the internet so they are leveraging the capabilities it offers. Finally, it should be assumed that they understand how many of the countries in the west depend on cyber so have actively sought out capabilities to exploit this vulnerability but to date no plans have been seen on how they would accomplish it.

European Countries

The Cooperative Cyber Defense Center of Excellence (CCD COE) located in Tallinn, Estonia, was formally established on the 14th of May, 2008, in order to enhance North Atlantic Treaty Organization's (NATO) cyber defense capabilities. The Center received full accreditation by NATO and attained the status of International Military Organization on the 28th of October, 2008. Its mission is to enhance the capability, cooperation, and information sharing among NATO, NATO nations, and Partners in cyber defense by virtue of education, research and development, lessons learned, and consultation [26]. This center is designed to allow NATO to integrate cyber doctrine. There are political, legal, doctrinal, and technical issues that must be worked out when operating in a multi-national task force. It has taken years to develop the processes to do this in the real world and NATO is moving to establish the same functionality in the virtual world.

The United Kingdom is developing strategies and doctrine for cyber as well. The "Cybersecurity Strategy of the United Kingdom safety—security and resilience in cyber space" was published in June 2009 by UK Office of Cybersecurity and UK Cybersecurity Operations

Center. This document states there is an ongoing and broad debate regarding what "cyber warfare" might entail, but it is a point of consensus that with a growing dependence upon cyberspace, the defense and exploitation of information systems are increasingly important issues for national security. It recognizes the need to develop military and civil capabilities, both nationally and with allies, to ensure we can defend against attack, and take steps against adversaries where necessary. Furthermore, these include criminals, terrorists, and states, whether for reasons of espionage, influence or even warfare [27]. This acknowledgement that cyber war is a distinct possibility and they are preparing for it is a clear statement that the UK is treating this as a matter of national security. They expanded the scope of cyber battle space to include criminals and espionage but treat them as separate from warfare; this inclusion in the statement shows the overlap that is one of the challenges in cyber doctrine.

France's government published a white paper on defense and national security which says cyber war is a major concern. The white paper develops a two-pronged strategy: (1) a new concept of cyber defense, organized in depth and coordinated by a new Security of Information Systems Agency under the purview of the General Secretariat for Defense and National Security; (2) the establishment of an offensive cyber war capability, part of which will come under the Joint Staff and the other part will be developed within specialized services [28]. Though not a national strategy, this white paper does call out France's belief that cyber is a military problem with the need for offensive capabilities under their special services units. They have followed the model that most countries are going to—stand up a new and separate organization to handle cyber war. Very few are trying to integrate a cyber capability into their traditional forces. This follows in the same pattern that Space support went through before it was integrated into tactical operations on the battlefield.

From The Fog of Cyber Defence by Eds. Jari Rantapelkonen and Mirva Salminen, we get a view of the Nordic countries. Finland aims to be a globally strong player in the field of cyber and cyber defense. Originally known as information security, cyber defense has become an issue on the strategic and individual levels. Norway released a revised "National Strategy for Information Security" in late 2012. The Norwegian national CERT has been provided increased funding for 2013, and the Norwegian Armed Forces Cyber Defence (NOR CYDEF) changed its name in the second half of 2012 in order to underscore the increased importance of cyber defense in the military sector. Swedish cyber defense aims at protecting Sweden and the Swedish interests against cyber-attacks from resourceful and advanced players. This includes strategic control and planning, cooperation and coordination as well as operational protection measures. Coordination, exercises and exchange of information with skilled and well-informed parties internationally is a top priority for the Swedish Armed Forces, as well as for other authorities that are in charge of national cyber security [29]. There is a high degree of cooperation between these three countries.

The Czech Republic has published their cybersecurity strategy for 2011-2015. This states, "Essential objectives of the cybersecurity policy include protection against threats which information and communication systems and technologies (hereinafter 'ICTs') are exposed to, and mitigation of potential consequences in the event of an attack against ICTs. The implementation, operation, and security of credible information and communication systems is a duty of the Czech Republic and a responsibility of all levels of government and administration, the private sector and the general public, the objective being to maintain a safe, secure, resistant, and credible environment that makes use of available opportunities offered by the digital age. The strategy focuses mainly on unimpeded access to services, data integrity, and confidentiality of the Czech Republic's cyberspace and is coordinated with other related strategies and concepts." It is worth noting they call on their general public as part of the solution [30].

Private or Mercenary Armies

"In an age where cyber warfare is more common than the physical battlefield, it may be necessary for the private sector to stop playing defense and go on offense," Gen. Michael Hayden said on August 1, 2011. Hayden, who led the National Security Agency and Central Intelligence Agency under president George W. Bush, said during a panel discussion at the 2011 Aspen Security Forum that the federal government may not be the sole defender of private sector companies—and that there is precedent for such action. "We may come to a point where defense is more actively and aggressively defined even for the private sector and what is permitted there is something that we would never let the private sector do in physical space," he said. "Let me really throw out a bumper sticker for you: how about a digital Blackwater?" he asked. "I mean, we have privatized certain defense activities, even in physical space, and now you have got a new domain in which we do not have any paths trampled down in the forest in terms of what it is we expect the government—or will allow the government—to do" [31]. Blackwater is a private military contractor that has changed its name to Academic after incidents in Iraq gave them a negative image. If companies decide to hire forces (hackers) to strike back or conduct recovery operations it could change the cyberspace battlefield dramatically.

KEY MILITARY PRINCIPLES THAT MUST BE ADAPTED TO CYBER WARFARE

There are a number of Tactics, Techniques, and Procedures (TTPs) that are used to implement doctrine. Some of the fundamental TTPs are Intelligence Preparation of the Operational Environment (IPOE), Force Analysis using Joint Munitions Effectiveness Manual (JMEM) factors, Measures of Effectiveness (MOEs), Battle Damage Assessment (BDA) to determine if MOEs were achieved, Close Air Support (CAS) to integrate air and land forces, and Counterinsurgency (COIN) to adapt classic force on force doctrine to asymmetric battlefield.

Intelligence Preparation of the Operational Environment

Intelligence Preparation of the Battlefield (IPB) has evolved to become Intelligence Preparation of the Operational Environment (IPOE) in today's complex wars. It is, "the analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. It is a continuous process that includes defining the operational environment; describing the impact of the operational environment; evaluating the adversary; and determining adversary courses of action" [32]. This requires evaluating both traditional enemy capabilities and terrain but also now includes many new demographics (i.e., economic, race, religious, gender, ethnic, and cultural). When looking at lines of communication, influence operation, and terrain it is now necessary to include cyberspace in that analysis. Cyber IPOE is vital to keeping inside the enemies OODA loop (Observe/Orient/Decide/Act). "IPB must be: timely, accurate, usable, complete, and relevant to be useful. In most cases, the basic groundwork needs to be 80% complete before operations and logistics can start planning" [33]. So with terrain that can change by the minute, forces that can be spread across the world and motives as diverse as the groups involved IPOE must relook at how it produces products like "enemies most likely course of action" but these products are still vital to the commander and must not be ignored in cyberspace.

Joint Munitions Effectiveness Manual

Joint Munitions Effectiveness Manual (JMEM) is formal capabilities analysis that determines effectiveness of different weapon systems (e.g., can an AT4 bazooka destroy a T64 Tank). These estimates may be generated using probabilistic mathematical models that take into account the target's critical vulnerabilities, performance data on the assets contemplated for application against the target, and means of delivery or they can be done via field testing. These predictions are based on historical data using strike performance and analyses of likely success given the specific planned weapon/target pairings (e.g., Air-to-Surface, Special Operations Target Vulnerability, or Surface-to-Surface) [33]. This is fairly straightforward when measuring kinetic effects but there are a multitude of factors that can impact the effectiveness of a cyber-weapon. We need to establish a standard to measure effectiveness that is used for a baseline so a commander can understand which cyber munitions are best for their needs. The standard will be based on some type of effect like "time not available" or "ability to influence decision."

There has been some work on this under the title JOINT NON-KINETIC EFFECTS INTEGRATION (JNKEI) which was completed in September 2010. The purpose was to develop joint TTPs to assist joint planners in integrating the non-kinetic effects of electronic attack, computer network attack, and offensive space control capabilities into operational planning. The following was accomplished:

- Improved integration of non-kinetic capabilities during operational planning that expand the range of possible courses of action for joint force commanders.
- Information exchange requirements based on the JNKEI TTPs and incorporated into the Integrated Strategic Planning and Analysis Network (ISPAN) and Virtual Integrated Support for the Information Operations Environment (VisIOn) collaborative tools.
- Input provided to Joint Publication (JP) 5-0, Joint Operational Planning; Joint Test Publication 3-12, Cyberspace Operations; JP 3-13, Information Operations; and JP 3-60, Joint Targeting.
- JNKEI TTPs provided to Joint Information Operations Planning Course (Joint Forces Staff College), Joint Targeting School (USJFCOM), and Advanced Integrated Warfighter Weapons Instructor Course (US Air Force Weapon School).
- JNKEI TTPs provided to USEUCOM; USPACOM; US Force, Korea; and USSTRATCOM to enhance existing standard operating procedures.

Measures of Effectiveness

Measures of Effectiveness (MOEs) assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. They do not measure task performance. When evaluating a course of action or combat assessment we need to evaluate it based on the impact or MOE it will have. These MOEs should use assessment metrics that are relevant, measurable, responsive, and resourced so there is no false impression of task or objective accomplishment [33]. This can be very complex if we are talking about influence operations or information operations. We need to establish a standard by which every branch of the military and federal agencies measure both impact and effectiveness. It will need to be a matrix that can deal with compromise to confidentiality, denial of access, and loss of integrity that reflects the consequences to the aspect of national power that was affected (military, economic, information, or diplomatic). It should be done in an unclassified format so that everyone trains and uses it to the point that it is universally understood.

Battle Damage Assessment

Battle Damage Assessment (BDA) is another key TTP. It is the estimate of damage resulting from the application of lethal or non-lethal military force. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. The purpose of BDA is to compare post-execution results with the projected/expected results generated during target development. Comprehensive BDA requires a coordinated and integrated effort between joint force intelligence and operations functions. Traditionally, BDA is composed of physical damage assessment, functional damage assessment, and functional assessment of the next higher target system [33]. BDA is vital to determining if the attack method has a successful MOE. For example, the Air Force would not launch aircraft until they were sure the enemy's anti-aircraft batteries were destroyed. Similarly, Cyber forces would not launch their exploit until they knew they could bypass the defensive firewalls. Generally, it is best to use "all source" information (indicators from all the Intel Functions) to provide accurate analysis.

Close Air Support

Close Air Support (CAS) is air action by fixed- and rotary-wing aircraft against hostile targets that are in close proximity to friendly forces and that require detailed integration of each air mission with the fire and movement of those forces [33]. This TTP reminds us that combined forces are more powerful when they are integrated. The United States does not fight wars alone, but rather as part of multinational coalitions. The Army rarely fights alone, but rather as part of a Joint Task Force. A cyber war will most likely be part of the integrated effort using multiple aspects of national power.

Counterinsurgency

Counterinsurgency (COIN) is comprehensive civilian and military efforts taken to simultaneously defeat and contain insurgency, and address its core grievances. COIN is primarily political, and incorporates a wide range of activities, of which security is only one. Unified action is required to successfully conduct COIN operations and should include all host nations (HN), the United States, and multinational agencies or actors [33]. Combating insurgency is the most prevalent type of conflict the United States has been engaged in recent history. In this kind of environment Information Operations and Influence Operations are key force multipliers. Cyber is a critical weapon for both sides in this kind of fight. As commanders analyze how to fight and win on today's battlefield they must understand how to dominate cyberspace. The same tools they use to fight on the local terrain can be modified to be used in cyberspace if we force the staff functions to focus on the right requirements.

GUIDANCE AND DIRECTIVES

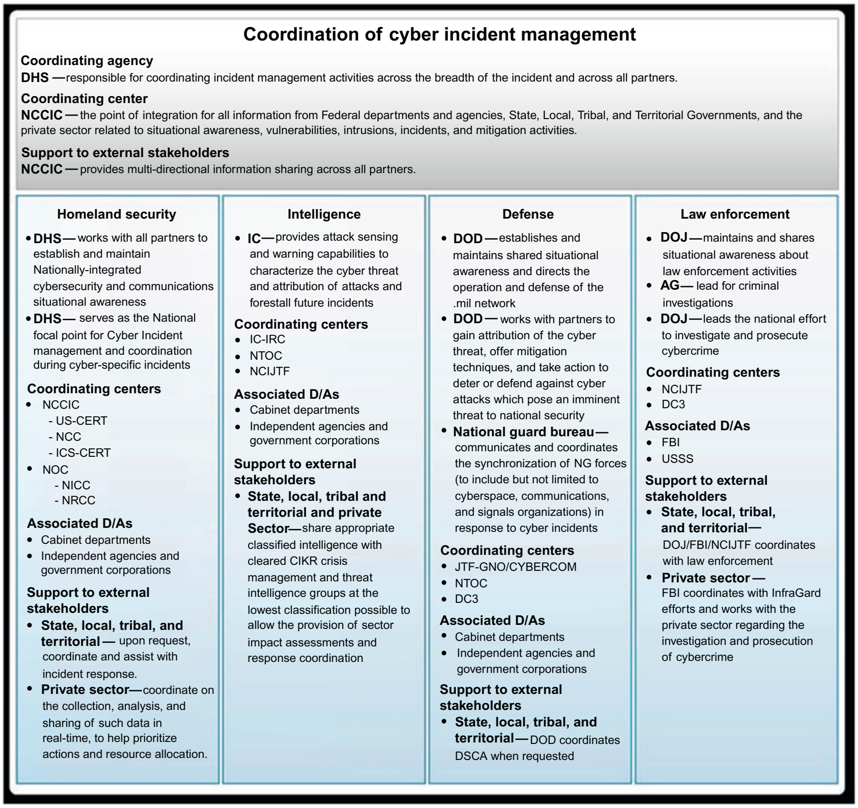
Not all national strategy comes from military doctrine; much of it is in the rest of the federal government as guidance and directives which can act as both constraints and permission. For cyber strategy we have the Comprehensive National Cybersecurity Initiative (CNCI), National Cyber Incident Response Plan (NCIRP), Homeland Security/Presidential Directives (HSPDs), and National Institute of Science and Technology (NIST). On the civilian side we have supporting organizations like academic institutions, commercial associations, and government/civilian partnerships. All of these contribute to a tapestry of efforts to secure the Internet.

Comprehensive National Cybersecurity Initiative

Comprehensive National Cybersecurity Initiative (CNCI) consists of a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace that were covered in Chapter 1. The key tasks were creating, or enhancing, shared situational awareness of network vulnerabilities, threats, and events within the federal government—and ultimately with state, local, and tribal governments and private sector partners. Tasks also include to: defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies; strengthen education, research, and development; and to define and develop strategies to deter hostile or malicious activity in cyberspace [34]. This effort was funded by the government in acknowledgement of the critical threat cyber vulnerabilities are to national security. We covered CNCI in Chapter 1 as it is the major investment the United States has made to secure cyberspace.

Department of Homeland Security

The Department of Homeland Security (DHS) has published the National Cyber Incident Response Plan (NCIRP). The NCIRP is designed in full alignment with these initiatives to ensure that federal cyber incident response policies facilitate the rapid national coordination needed to defend against the full spectrum of threats. The NCIRP focuses on improving the human and organizational responses to cyber incidents, while parallel efforts focus on



Coordination of cyber incident management

Coordinating agency
DHS —responsible for coordinating incident management activities across the breadth of the incident and across all partners.

Coordinating center
NCCIC —the point of integration for all information from Federal departments and agencies, State, Local, Tribal, and Territorial Governments, and the private sector related to situational awareness, vulnerabilities, intrusions, incidents, and mitigation activities.

Support to external stakeholders
NCCIC —provides multi-directional information sharing across all partners.

Homeland security

- **DHS**— works with all partners to establish and maintain Nationally-integrated cybersecurity and communications situational awareness
- **DHS**— serves as the National focal point for Cyber Incident management and coordination during cyber-specific incidents

Coordinating centers

- NCCIC
  - US-CERT
  - NCC
  - ICS-CERT
- NOC
  - NICC
  - NRCC

Associated D/As

- Cabinet departments
- Independent agencies and government corporations

Support to external stakeholders

- **State, local, tribal, and territorial**— upon request, coordinate and assist with incident response.
- **Private sector**—coordinate on the collection, analysis, and sharing of such data in real-time, to help prioritize actions and resource allocation.

Intelligence

- **IC**—provides attack sensing and warning capabilities to characterize the cyber threat and attribution of attacks and forestall future incidents

Coordinating centers

- IC-IRC
- NTOC
- NCIJTF

Associated D/As

- Cabinet departments
- Independent agencies and government corporations

Support to external stakeholders

- **State, local, tribal and territorial and private Sector**—share appropriate classified intelligence with cleared CIKR crisis management and threat intelligence groups at the lowest classification possible to allow the provision of sector impact assessments and response coordination

Defense

- **DOD**—establishes and maintains shared situational awareness and directs the operation and defense of the .mil network
- **DOD**— works with partners to gain attribution of the cyber threat, offer mitigation techniques, and take action to deter or defend against cyber attacks which pose an imminent threat to national security
- **National guard bureau**— communicates and coordinates the synchronization of NG forces (to include but not limited to cyberspace, communications, and signals organizations) in response to cyber incidents

Coordinating centers

- JTF-GNO/CYBERCOM
- NTOC
- DC3

Associated D/As

- Cabinet departments
- Independent agencies and government corporations

Support to external stakeholders

- **State, local, tribal, and territorial**—DOD coordinates DSCA when requested

Law enforcement

- **DOJ**—maintains and shares situational awareness about law enforcement activities
- **AG**— lead for criminal investigations
- **DOJ**—leads the national effort to investigate and prosecute cybercrime

Coordinating centers

- NCIJTF
- DC3

Associated D/As

- FBI
- USSS

Support to external stakeholders

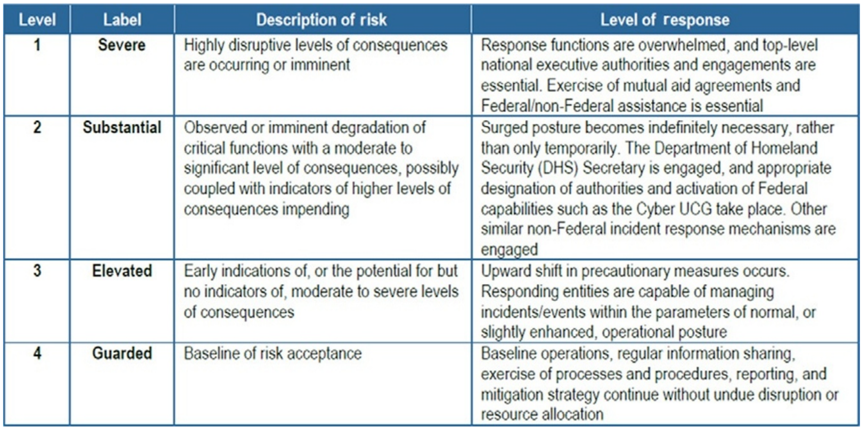
- **State, local, tribal, and territorial**— DOJ/FBI/NCIJTF coordinates with law enforcement
- **Private sector** — FBI coordinates with InfraGard efforts and works with the private sector regarding the investigation and prosecution of cybercrime

FIGURE 4.3 Federal cyber incident lanes.

enhancing the community's technological capabilities. NCIRP was developed according to the principles outlined in the National Response Framework (NRF) and describes how the nation responds to Significant Cyber Incidents [35]. This plan is designed to bridge the DoD capabilities to federal agencies and ultimately to the national critical infrastructure. The plan lays out the roles and responsibilities across the federal government, military, intelligence community, and law enforcement. This integration is as vital to the nation as joint operations are to the military. See Figure 4.3 to understand the roles and responsibilities that have been laid out to facilitate cooperation.

DHS has made progress creating a baseline to measure the impacts we mentioned in the military TTP section. They have classified Significant Cyber Incidents as a set of conditions in the cyber domain that requires increased national coordination. This increase in national coordination is triggered when the National Cyber Risk Alert Level (NCRAL) system reaches Level 2 (see Figure 4.4 to understand the different levels).

A key new development is the "Strategy for Homeland Defense and Defense of Support of Civil Authorities" signed by Defense Secretary Leon Panetta in Feb 2013. The executive summary states, "We are now moving beyond traditional distinctions between homeland and national security. National security draws on the strength and resilience of our citizens,



Level	Label	Description of risk	Level of response
1	Severe	Highly disruptive levels of consequences are occurring or imminent	Response functions are overwhelmed, and top-level national executive authorities and engagements are essential. Exercise of mutual aid agreements and Federal/non-Federal assistance is essential
2	Substantial	Observed or imminent degradation of critical functions with a moderate to significant level of consequences, possibly coupled with indicators of higher levels of consequences impending	Surged posture becomes indefinitely necessary, rather than only temporarily. The Department of Homeland Security (DHS) Secretary is engaged, and appropriate designation of authorities and activation of Federal capabilities such as the Cyber UCG take place. Other similar non-Federal incident response mechanisms are engaged
3	Elevated	Early indications of, or the potential for but no indicators of, moderate to severe levels of consequences	Upward shift in precautionary measures occurs. Responding entities are capable of managing incidents/events within the parameters of normal, or slightly enhanced, operational posture
4	Guarded	Baseline of risk acceptance	Baseline operations, regular information sharing, exercise of processes and procedures, reporting, and mitigation strategy continue without undue disruption or resource allocation

FIGURE 4.4 National cyber risk alert levels.

communities, and economy. This includes a determination to prevent terrorist attacks against the American people by fully coordinating the actions that we take abroad with the actions and precautions that we take at home. It must also include a commitment to building a more secure and resilient nation, while maintaining open flows of goods and people. We will continue to develop the capacity to address the threats and hazards that confront us, while redeveloping our infrastructure to secure our people and work cooperatively with other nations." This increases the level of the U.S. military in the active defense of critical infrastructure, pushes for more information sharing, and acknowledges cyberspace as an aspect they must protect.

Homeland Security/Presidential Directives

Homeland Security/Presidential Directives (HSPDs) are issued by the president on matters pertaining to Homeland Security. While they are not part of the military doctrine they provide a similar function for the other elements of national power—specifically diplomatic and economic. They are intended to provide guidance, set standards, and increase coordination across all federal agencies [36]. Following are the HSPDs that impact cyberspace.

- HSPD—1: Organization and Operation of the Homeland Security Council. Ensures coordination of all homeland security-related activities among executive departments and agencies and promotes the effective development and implementation of all homeland security policies.
- HSPD—5: Management of Domestic Incidents. Enhances the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.
- HSPD—7: Critical Infrastructure Identification, Prioritization, and Protection. Establishes a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

- HSPD—8: National Preparedness. Identifies steps for improved coordination in response to incidents. This directive describes the way federal departments and agencies will prepare for such a response, including prevention activities during the early stages of a terrorism incident. This directive is a companion to HSPD-5.
- HSPD—12: Policy for a Common Identification Standard for Federal Employees and Contractors. Establishes a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees).
- HSPD—23: National Cyber Security Initiative. Details are classified but are generally focused on a series of efforts covered in Chapter 1.
- HSPD—24: Biometrics for Identification and Screening to Enhance National Security. Establishes a framework to ensure that federal executive departments use mutually compatible methods and procedures regarding biometric information of individuals, while respecting their information privacy and other legal rights.
- Presidential Policy Directive (PPD)—20 is a classified directive relating to cyber operations which establishes principles and processes for the use of cyber operations so that cyber tools are integrated with the full array of national security tools we have at our disposal.
- PDD 21—Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

NOTE

The key to understanding where the authority is for cyber is the same as any function: follow the money. A new command or presidential directive without funding is more posturing than executing a plan of action. Naming someone into a new position or declaring a new committee that does not have budget authority is more public relations than fixing a problem. When we look cyber-related activity it is vital to see who controls the resources.

National Institute of Standards and Technology

The one agency that is at the center of establishing standards for the nation is the National Institute of Standards and Technology (NIST). The government has stated that for cyber and network security NIST is focused on ensuring three security objectives of information technology systems: confidentiality, integrity, and availability. NIST does not publish rules like Defense Information Systems Agency (DISA), NSA, and DoD but instead provides the groundwork for those organizations to create regulations. The Cyber and Network Security Program addresses NIST's statutory responsibilities in the domain and the near- and long-term scientific issues in some of the building blocks of IT and network security, including cryptography, security testing and evaluation, access control, Internet-working services and protocols (Domain Name System, Border Gateway Protocol, IPv6, Wi-Max, etc.), security metrics, vulnerability analysis, security automation, and security properties. These efforts will provide a more scientific foundation for cybersecurity, while maintaining a focus on near-term security issues in emerging technologies [37]. NIST is responsible for determining how the government will protect systems today, setting guidelines and shaping Institute of Electrical and Electronics Engineers (IEEE) standards for the future. They have traditionally

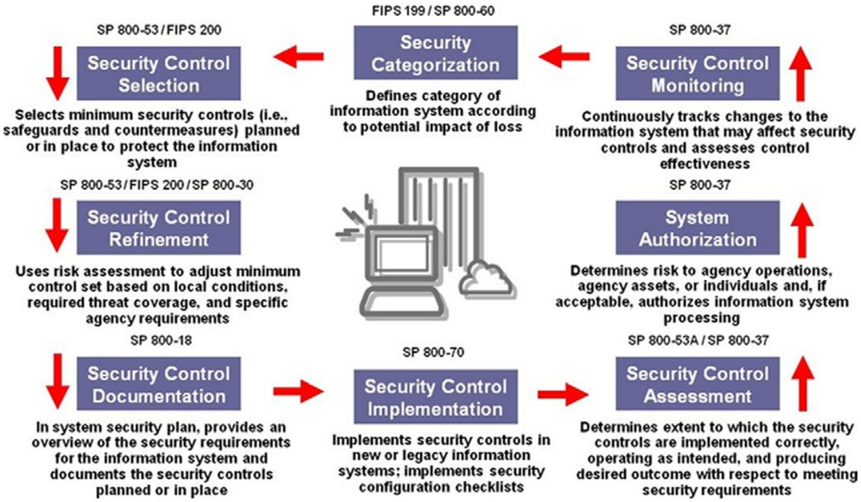

FIPS 199 / SP 800-60
Security Categorization
Defines category of information system according to potential impact of loss
SP 800-53 / FIPS 200
Security Control Selection
Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system
SP 800-37
Security Control Monitoring
Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness
SP 800-53 / FIPS 200 / SP 800-30
Security Control Refinement
Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements
SP 800-37
System Authorization
Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing
SP 800-18
Security Control Documentation
In system security plan, provides an overview of the security requirements for the information system and documents the security controls planned or in place
SP 800-70
Security Control Implementation
Implements security controls in new or legacy information systems; implements security configuration checklists
SP 800-53A / SP 800-37
Security Control Assessment
Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

FIGURE 4.5 NIST risk management framework.

been focused on configuration management, compliance validation, and vulnerability detection but are shifting to a real-time situational awareness model.

Currently, there are over 300 NIST information security documents. This number includes Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, Information Technology Laboratory (ITL) Bulletins, and NIST Interagency Reports (NIST IR). The Federal Information Processing Standards (FIPS) Publication Series is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations. Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis [37]. See Figure 4.5 to understand the flow of the documentation. These are the foundation for all government cybersecurity guidance and compliance specifications. These standards are the baseline for multiple regulations but are implemented differently by each.

Academia and Industry Associations

Two key supporting functions to doctrinal development come from the commercial sector. First is academia for both skills and innovation and the second are industry organizations like National Defense Industrial Association (NDIA) or Armed Forces Communications and Electronics Association (AFCEA). First we will talk about some of the key academic institutions (though there are far too many to mention all the great work being done). To find a list of what universities are nationally ranked we refer to National Centers of Academic Excellence. NSA and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA Education and research programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA, and producing a growing number of professionals with IA expertise in various disciplines [38]. Next, we will look at a couple of universities that have been consistently doing great work in the field: Purdue's Center for Education and Research in Information Assurance and Security (CERIAS) and Carnegie Mellon University with both the Computer Emergency Readiness Team (CERT) and CyLab. These are just two of a number of outstanding programs but are good examples of what is being done. All these institutions are training the future cyber warriors and helping develop the future tools need to conduct CNO.

There are two basic types of associations: industry based and government partnerships. Industry associations focus on certifications, awareness training, and ethical standards. A sample list of these include: International Information Systems Security Certification Consortium (ISC)2®, Information Systems Security Association (ISSA), and Information Systems Audit and Control Association (ISACA). Partnerships are sponsored by many different government agencies, including: Executive Office with Advisory Councils on Infrastructure, Telecommunications and Science & Technology; DHS with National Security Information Exchange (NSIE); Industrial Control System Joint Working Group; National Cyber Coordination and Integration Center; Information Sharing and Analysis Centers and Defense Industrial Base (DIB) Program; DoD with Domestic Security Alliance Council; Counterintelligence Strategic Partnership-Business Alliance and Science Boards; FBI with InfraGard; Dept of Treasury with Advisory Committees on Information Policies and Telecommunications; and Department of State with Information Security and Privacy Advisory Board, to name a few. These partnerships are designed to help share policy within the government and encourage industry self-governance. The partnerships face challenges like companies who are unwilling to share because of the fear of exposure. These companies do not want to lose credibility by letting the public know they were hacked into. The government in many cases will not protect information the companies would share from Freedom of Information Act (FOIA) so anyone could ask for the details on who was compromised and publish it. Another concern companies have is in regards to how much of their shared information can be used by any agency of the government, in particular prosecution by the Department of Justice.

OPERATIONS AND EXERCISES

Finally, we have to train and practice to be successful when it comes time to execute. There are many efforts in the federal government, military, academia, and jointly (both commercial and international) to exercise the different cyber plans. There are two basic types of exercises, Table Top and Simulations. Table Top exercises are scripted and designed to take the organization through the thought process, while simulations are designed to recreate the environment and take the team through the actual actions they would take in the real world. Exercises can be purely cybersecurity focused, or cyber can be an active part built into an operational exercise. There are federal exercises, military exercises, and academic exercises.

Federal Exercises

For the U.S. government, the major exercises are Cyber Storm and National Level Exercises (formally known as Top Off). Cyber Storm is focused on the National Cyber Incident response plan. Cyber Storm IV: 2011-2012 was the latest installment of the series, Cyber Storm IV

(CS IV), it was designed as a set of building block exercises, which began in fall 2011 and concluded in 2012. It promoted more focused exercise activities, allowing participants to delve deeper into particular cyber issues. Members of the cyber incident response community are actively collaborating with DHS in the design and execution of these building block exercises [39]. Cyber Storm was the primary vehicle to exercise the newly developed National Cyber Incident Response Plan (NCIRP)—a blueprint for cybersecurity incident response—to examine the roles, responsibilities, authorities, and other key elements of the nation's cyber incident response and management capabilities and use those findings to refine the plan. The goals were increased federal, state, international, and private sector participation (multiagency, over 20 states and nations). The National Level Exercise 2009 was designated as a Tier I National Level Exercise. Tier I exercises are conducted annually in accordance with the National Exercise Program (NEP), which serves as the nation's overarching exercise program for planning, organizing, conducting, and evaluating national level exercises. The NEP was established to provide the U.S. government, at all levels, exercise opportunities to prepare for catastrophic crises ranging from terrorism to natural disasters [40]. These exercises are vital to building relationships and procedures for the different agencies to work together. The downside to them is there are many problems that are identified and not addressed. We need formal After Action Reviews (AARs) with a plan of action to remedy the issues identified. This goes back to the problem that there is no one person responsible for solving the problems identified so as the participants get back to their normal jobs they focus on the near term problems they are directly responsible for.

TIP

Most organizations do not have disaster recovery/continuity of operations plans. Those who do often do not exercise them. Find out if your company has a plan and organize a Table Top walk through the plan. Get the IT department to transfer one application to your alternate site for a week every year. These little steps could prevent your company from going under given a major catastrophe.

DoD Exercises

The U.S. military has built cyber warfare into some of their key exercises. Below is a list of exercises (broken out by major commands and services) that have significant cyber Mission Event Synchronization List (MESL) events:

- EUCOM—Austere Challenge, Agile Response, Flexible Leader
- PACOM—Terminal Fury, Ulchi Focus Lens, RSOI
- CENTCOM—Unified Endeavor
- NORTHCOM—Ardent Sentry, Northern Edge, Vigilant Shield
- SOUTHCOM—Fuertas Defensas, Blue Advance
- STRATCOM—Global Lightning, Global Shield, Bulwark Defender
- TRANSCOM—Turbo Challenge, Turbo Distribution
- USA—Warfighter Program (simulation)
- USN—JTFeX
- USAF—Black Daemon
- U.S. Marines—MEFEx, FEDOS

Although these exercises have a cyber component, they cost millions of dollars to run, and the cyber events are not allowed to have a severe impact on the exercise. There is no exercise that is designed to see how the military would operate without cyber. How well the military could perform without cyber-enabled command and control systems may never be known until they are forced to.

Educational Exercises

There are also some very strong educational sponsored exercises. At the high school level there is CyberPatriot, at the college level is the National Collegiate Cyber Defense Competition (NCCDC) and for the U.S. Military Academies is the Cyber Defense Exercise (CDX). UK has officially launched its Cyber Security Challenge to find and attract new talent to the IT security industry. In the "hacker" community there is a competition called Capture the Flag contest (CTF) at DEFCON (since 2010 there have been both a network and social engineering contests). Finally, SANS (a major commercial training company) hosts NetWars. The educational sponsored exercises are very defense-oriented. DEFCON and SANS have both attack and defending aspects. These are designed to encourage development of the skills needed to be successful in this new domain. These competitions are monitored by federal agencies, DoD, and commercial companies in search of cyber talent.

Sample MESLs

We include some sample MESL events for organizations considering conducting an exercise:

1. Disaster Recovery Plan/Continuity of Operations Plan execution
   a. Analyze team response (focus on legal, HR, public relations actions)
2. Major IT support vendor failure to perform (i.e., going out of business)
3. Vulnerability Assessment/Penetration Test
   a. Both external and internal threat test with full staff response to incident
   b. Conduct Forensic analysis of simulated incident and determine response
4. Detection of a Massive Data Exfiltration or Theft of IP
5. Sample Vignettes to talk through at staff meetings

- Zero Day Attack takes down over 20% of the companies systems
- Critical System failure (key application or email server)
- Degraded Connectivity/Denial of Service impacts access
- Insider accidental data deletion
- Insider proprietary information theft
- Insider malicious activity
- Insider inappropriate activity
- Partner network compromise
- Compromised web page
- Discovery of software license abuse
- Compromise of privacy information
- Unauthorized Device on the enterprise network

SUMMARY

This chapter has explored the state of current cyber warfare doctrine on both the nation state and military. Every country with a dependence on IT infrastructure is developing strategies and capabilities to protect and exercise national power. We then examined some of the traditional tactics and products that the military needs to adapt to the cyberspace environment. We covered some of the directives used by federal agencies and governments to guide behavior in this virtual environment. Finally, we took a look at how organizations are training to both develop new doctrine and execute their current plans.

Today we are at the beginning of a new era of culture, individual and nation state influence, and possibly warfare (both economic and force on force conflicts). Governments and militaries all over the world are aggressively working on developing doctrine to defend, fight, and win in this new domain.

References

[1] DoD. Joint electronic library, http://www.dtic.mil/doctrine/; 2010 [accessed 17.02.13].

[2] DoD. Secretary of Defense Robert Gates. Wall Street J Resource Documents, http://online.wsj.com/public/resources/documents/OSD05914.pdf; 2009 [accessed 17.02.13].

[3] Alexander, General Keith B. Statement of commander United States Cyber Command before the house committee on armed services; 2010.

[4] Gates, Secretary of Defense Robert. Wall Street J Resource Documents [online] DoD, http://online.wsj.com/public/resources/documents/OSD05914.pdf; 2009.

[5] Congressman W. Mac. Thornberry (R) definitions, focal point, and methodology needed for DOD to develop full-spectrum cyberspace budget estimates, http://www.gao.gov/products/GAO-11-695R; 2011 [online].

[6] Compendium of Key Joint Doctrine Publications Compiled by Deputy Directorate, Joint Staff, J-7 Joint and Coalition Warfighting Joint Doctrine Support Division as of 7 January 2013.

[7] DoD. Joint electronic library, http://www.dtic.mil/doctrine/; 2010 [accessed 17.02.13].

[8] Baldor LC. Pentagon creates new medal for cyber, drone wars. Washington: Associated Press; 2013 [accessed 17.03.13].

[9] Major General Webber RE. USAF. U.S. House of Representatives House Armed Services Committee. Presentation to the subcommittee on terrorism and unconventional threats. US Navy. http://www.airforce-magazine.com/SiteCollectionDocuments/Testimony/2010%20docs/092310Webber.pdf; 2010 [accessed 17.02.13].

[10] VADM Jack Dorsett DCNO for Information Dominance. Information dominance and the U.S. Navy's cyber warfare vision. The Defense Technical Information Center. US Navy, http://www.dtic.mil/ndia/2010SET/Dorsett.pdf; 2010 [accessed 17.02.13].

[11] Vice Admiral Kendall L. Card interview on cyber http://defensesystems.com/articles/2011/06/17/chief-of-naval-intelligence-card-navy-technology.aspx [accessed 17.03.13].

[12] Navy Cyber Power 2020 – Sustaining the US global leadership: priorities for 21st century defense, www.public.navy.mil/fcc-c10f/Strategies/Navy_Cyber_Power_2020.pdf.

[13] U.S. Army. TRADOC pam 525-7-8, Cyberspace operations concept capability plan 2016–2028; 2010.

[14] Department of Defense. TRICARE. Military health system information assurance guidance, http://www.health.mil/Libraries/ia-files/14-INFOCON-10102008.pdf; 2008 [accessed 17.02.13].

[15] Robinson N, Gribbon L, Horvath V, Robertson K. Cyber-security threat characterization: a rapid comparative analysis. Stockholm: Prepared for the Center for Asymmetric Threat Studies (CATS), Swedish National Defence College; 2013.

[16] Liang Q, Xiangsui W. Unrestricted warfare. Beijing: PLA Literature and Arts Publishing House; 1999.

[17] Thomas T. Air Force Space Command High Frontier. Taiwan examines Chinese information warfare. Air Force, http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf; 2009.

[18] Krekel B. Capability of the people's republic of China to conduct cyber warfare and computer network exploitation. The US-China Economic and Security Review Commission, http://cdm266901.cdmhost.com/cdm/singleitem/collection/p266901coll4/id/3130/rec/12; 2009 [accessed 17.02.13].

[19] Associated Press 12 Chinese Hacker Teams Responsible for most US Cybertheft. http://www.foxnews.com/scitech/2011/12/12/12-chinese-hacker-teams-responsible-for-most-us-cybertheft/; 2011 [online].

[20] Strategy Page The Mighty 1st Technical Reconnaissance Bureau. http://www.strategypage.com/htmw/htiw/articles/20110417.aspx; 2011 [online].

[21] Mandiant APT1 report, www.mandiant.com [accessed 17.03.13].

[22] Bloomberg Businessweek February 18-24 cover story [accessed 17.03.13].

[23] Yasuhide Y, Atsuhiro Y, Katsumi BT. Comparative study of the information security policies of Japan and the United States, J Natl Security Law 2010; http://infosecmgmt.pro/sites/default/files/us-japan_information_security_comparison_4_yamada.pdf [accessed 17.03.13].

[24] Yong-sup H. Analyzing South Korea's Defense Reform 2020. Korean J Def Anal 2006;XVIII(1) [accessed 17.03.13].

[25] Bermudez Jr. JS. SIGINT, EW, and EIW in the Korean People's Army, Honolulu: Asia-Pacific Center for Security Studies; 2005. http://www.apcss.org/Publications/Edited%20Volumes/BytesAndBullets/CH13.pdf [accessed 17.03.13].

[26] Cooperative Cyber Defence Centre of Excellence. NATO and attained the status of International Military Organisation, http://www.ccdcoe.org/12.html [accessed 17.02.13].

[27] Centre, Office of Cyber Security and Cyber Security Operations. Cyber Security Strategy of the United Kingdom. Cabinet Office, http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf; 2009 [online].

[28] République, Présidence De La. The French White Paper on defence and national security. Le Livre blanc sur la défense et la sécurité nationale, http://www.livreblancdefenseetsecurite.gouv.fr/IMG/pdf/white_paper_press_kit.pdf; 2007 [online].

[29] Rantapelkonen J, Salminen M, editors. The fog of cyber defence. Helsinki: National Defence University Department of Leadership and Military Pedagogy; 2013, Publication Series 2 Article Collection no: 10.

[30] Czech Republic Czech Cyber Security Strategy for 2011–2015 published [online] August 2011, http://www.enisa.europa.eu/media/news-items/czech-cyber-security-strategy-published.

[31] Andrew Nusca Hayden Digital Blackwater may be necessary for private sector to fight cyber threats, http://www.zdnet.com/blog/btl/hayden-digital-blackwater-may-be-necessary-for-private-sector-to-fight-cyber-threats/53639; 2011 [online].

[32] Steve W. GSEC gold credentials. Cyber IPB, http://www.giac.org/paper/gsec/1752/cyber-ipb/103147; 2001.

[33] Department of Defense. Joint electronic library, http://www.dtic.mil/doctrine/; 2010 [accessed 17.02.13].

[34] National Security Council. White house comprehensive national cybersecurity initiative, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative; 2008.

[35] Department of Homeland Security. Federal news radio. National cyber incident response plan. DHS, http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf; 2010.

[36] Department of Homeland Security. White house homeland security presidential directives, http://www.dhs.gov/xabout/laws/editorial_0607.shtm; 2010 [accessed 17.02.13].

[37] National Institute of Standards and Technology. Cyber and network security. Information technology laboratory, http://www.nist.gov/itl/cns/index.cfm; 2010 [accessed 17.02.13].

[38] National Security Agency. National centers of academic excellence. Information assurance, http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml; 2010 [accessed 17.02.13].

[39] Department of Homeland Security. Cyber storm: securing cyber space, http://www.dhs.gov/files/training/gc_1204738275985.shtm; 2010 [accessed 17.02.13].

[40] National Exercise Program. http://www.dhs.gov/files/training/gc_1179350946764.shtm; 2010 [accessed 17.02.13].