Cyber Operations in DOD Policy and Plans: Issues for Congress

Updated January 5, 2015

Congressional Research Service
https://crsreports.congress.gov
R43848

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Cyberspace is defined by the Department of Defense as a global domain consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Attacks in cyberspace have seemingly been on the rise in recent years with a variety of participating actors and methods. As the United States has grown more reliant on information technology and networked critical infrastructure components, many questions arise about whether the nation is properly organized to defend its digital strategic assets. Cyberspace integrates the operation of critical infrastructures, as well as commerce, government, and national security. Because cyberspace transcends geographic boundaries, much of it is outside the reach of U.S. control and influence.

The Department of Homeland Security is the lead federal agency responsible for securing the nation's non-security related digital assets. The Department of Defense also plays a role in defense of cyberspace. The National Military Strategy for Cyberspace Operations instructs DOD to support the DHS, as the lead federal agency, in national incident response and support to other departments and agencies in critical infrastructure and key resources protection. DOD is responsible for defensive operations on its own information networks as well as the sector-specific agency for the defense of the Defense Industrial Base. Multiple strategy documents and directives guide the conduct of military operations in cyberspace, sometimes referred to as cyberwarfare, as well as the delineation of roles and responsibilities for national cybersecurity. Nonetheless, the overarching defense strategy for securing cyberspace is vague and evolving.

This report presents an overview of the threat landscape in cyberspace, including the types of offensive weapons available, the targets they are designed to attack, and the types of actors carrying out the attacks. It presents a picture of what kinds of offensive and defensive tools exist and a brief overview of recent attacks. The report then describes the current status of U.S. capabilities, and the national and international authorities under which the U.S. Department of Defense carries out cyber operations. Of particular interest for policy makers are questions raised by the tension between legal authorities codified at 10 U.S.C., which authorizes U.S. Cyber Command to initiate computer network attacks, and those stated at 50 U.S.C., which enables the National Security Agency to manipulate and extrapolate intelligence data—a tension that Presidential Policy Directive 20 on U.S. Cyber Operations Policy manages by clarifying the Pentagon's rules of engagement for cyberspace. With the task of defending the nation from cyberattack, the lines of command, jurisdiction, and authorities may be blurred as they apply to offensive and defensive cyberspace operations. A closely related issue is whether U.S. Cyber Command should remain a sub-unified command under U.S. Strategic Command that shares assets and its commander with the NSA. Additionally, the unique nature of cyberspace raises new jurisdictional issues as U.S. Cyber Command organizes, trains, and equips its forces to protect the networks that undergird critical infrastructure. International law governing cyberspace operations is evolving, and may have gaps for determining the rules of cyberwarfare, what constitutes an "armed attack" or "use of force" in cyberspace, and what treaty obligations may be invoked.

Contents

Appendixes

Contacts

Introduction[1]

Cyberspace has taken on increased strategic importance as states have begun to think of it as yet another domain—similar to land, sea, and air—that must be secured to protect their national interests. Cyberspace is another dimension, with the potential for both cooperation and conflict. The Obama Administration's 2010 National Security Strategy identifies cybersecurity threats "as one of the most serious national security, public safety, and economic challenges."

Cyberattacks are now a common element of international conflict, both on their own and in conjunction with broader military operations. Targets have included government networks, media outlets, banking services, and critical infrastructure. The effects and implications of such attacks may be small or large; cyberattacks have defaced websites, temporarily shut down networks and cut off access to essential information and services, and damaged industrial infrastructure. Despite being relatively common, cyberattacks are difficult to identify at their source and thwart, in particular because politically motivated attacks are often crowd-sourced,[2] and online criminal organizations are easy to join. Suspicions of state-sponsored cyberattacks are often strong but difficult to prove. The relative anonymity under which actors operate in cyberspace affords a degree of plausible deniability.

This report focuses specifically on cyberattacks as an element of warfare, separate and distinct from diplomatic or industrial espionage, financially motivated cybercrime, or state-based intimidation of domestic political activists.[3] However, drawing clean lines between cyberwar, cyberterrorism, cyberespionage, and cybercrime is difficult. State and non-state actors carry out cyberattacks every day. When and under what conditions cyberattacks rise to the level of cyberwar is an open question. Some experts contend that all warfare, including cyberwarfare, by definition includes the destruction of physical objects. According to this point of view, to be an act of cyberwarfare, the attack must originate in cyberspace and result in the destruction of critical infrastructure, military command-and-control capabilities, and/or the injury or death of individuals.[4] On the other hand, some analysts have a more inclusive view of cyberwarfare. These experts would include, in addition to cyberattacks with kinetic effects, the exfiltration or corruption of data, the disruption of services, and/or manipulation of victims through distraction.

As our military becomes increasingly information dependent, potential vulnerabilities in network-centric operations are crystalized. A cyberattack on a military asset may be considered an act of war to which the military will respond under the Law of Armed Conflict. However, there may also be attacks on civilian systems which would warrant a military response.

[1] Information contained in this report is derived from unclassified open source material and discussions with senior government officials and industry technology and security experts.

[2] Crowd-sourcing refers to the use of online communities to obtain ideas, information, and services.

[3] Industrial espionage events are widely covered and notorious: attacks on Target, Home Depot, and Sony have caught national attention and have serious economic implications. Such events, however challenging, are not considered warfare for purposes of this report.

[4] Bruce Schneier, *Schneier on Security* (Indianapolis: Wiley, 2008); Michael Schmitt et al., *Tallinn Manual on the Internationl Law Applicable to Cyber Warfare*, prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press, 2013.

Background

Cyberspace: The Operating Environment

The Internet represents a portion of the global domain of cyberspace; however, there are networks and systems that are not connected to the Internet. Included among these are national strategic assets whose compromise could have serious consequences. In its 2010 Quadrennial Defense Review, the Department of Defense (DOD) identified cyberspace as a global commons or domain, along with air, sea and space. Previous views of cyberspace had focused mainly on the enabling or force multiplier aspects of information technology and networked workfare. Cyberspace is currently defined by the DOD as a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[5] It is also described in terms of three layers: (1) a physical network, (2) a logical network, and a (3) cyber-persona:[6]

- The *physical network* is composed of the geographic and physical network components.
- The *logical network* consists of related elements abstracted from the physical network, (e.g., a website that is hosted on servers in multiple locations but accessed through a single URL).
- The *cyber-persona layer* uses the rules of the logical network layer to develop a digital representation of an individual or entity identity.

Because one individual or entity can have multiple cyber personae, and vice versa, attributing responsibility and targeting attacks in cyberspace is challenging. Another challenge lies in insider threats, when an authorized user or users exploits legitimate access to a network for nefarious purposes.

From a military perspective, the *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.[7] The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information, further broken down into the physical, informational, and cognitive dimensions.

Cyberspace operations employ capabilities whose primary purpose is to achieve objectives in or through cyberspace. The following section gives examples of some of the tools through which these objectives may be achieved.

Cyber Weapons

There are several tools through which effects in cyberspace are achieved. Effects can range in severity from disrupting or slowing down access to online goods and services, to degrading and destroying entire network operations. The actors who employ these tools can range from individual hacker groups to nation states and their proxies. The following section describes the most common attack tools, or cyber weapons, that these actors employ.

[5] Department of Defense Joint Publication 3-12, *Cyberspace Operations*, February 5, 2013.

[6] Ibid.

[7] Ibid.

Malware

Malware is a general term for malicious software. Bots, viruses, and worms are varieties of malware. Bots, as described below, are used to establish communication channels among personal computers, linking them together into botnets that can be controlled remotely. Botnets are one way that other forms of malware, such as viruses and worms, spread. As the names imply, viruses spread by infecting a host. They attach themselves to a program or document. In contrast, worms are stand alone, self-replicating programs.[8]

The first known malware aimed at PCs, a virus, was coded in 1986 by two brothers in Pakistan. They named the virus Brain after their computer shop in Lahore and included their names, addresses, and phone numbers in the code. Calling Brain malware is slightly misleading because the brothers had no ill intentions. They were simply curious to find out how far their creation could travel. Within a year it had traveled around the globe.[9]

Malware that targets the internal networks of particular companies are often spread by infecting "watering-holes," a term for public websites frequented by employees. Another common method is "spearphishing"—sending emails to targeted individuals that contain malicious links. The email appears to be innocuous and sent from a trusted source, but clicking on the link opens a virtual door to outsiders.[10] So-called "air-gapped" networks, computer systems that are not connected to the Internet, are not vulnerable to these types of attacks; however, such networks can be infected by viruses and worms when an external device, such as a thumb drive, is inserted into a networked computer.

Botnets

Robotic networks, commonly known as botnets, are chains of home and business PCs linked together by a script or program. That program (the bot) enables a single operator to command all of the linked machines. Botnets are not necessarily malicious. The computer code botnets use also enables desirable communication across the Internet, such as the chat rooms that were popular in the 1990s. However, programmers have figured out how to exploit vulnerabilities in widely used Microsoft Windows operating platforms to degrade, destroy, and manipulate computer networks—often without the knowledge of the machine's owner or local operator.[11] Because they are automated programs, when released, bots lurk on the Internet and take over computers, turning them into a network of "zombies" that can be operated remotely. The majority of email spam is generated by botnets without the host computer's knowledge.[12] In fact, owners are often not aware that their computers are part of a botnet, the only indication of which is sluggish response time.[13]

---

[8] CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John W. Rollins, and Catherine A. Theohary.

[9] Joshua Davis, "John McAfee Fled to Belize, But He Couldn't Escape Himself," *Wired*, December 24, 2012, http://www.wired.com/2012/12/ff-john-mcafees-last-stand/all.

[10] Chris Strohm, "Hedge-Fund Hack Part of Wall Street Siege Seen by Cyber-Experts," *BloombergGovernment*, June 23, 2014.

[11] Zheng Bu, Pedro Bueno, Rahul Kashyap, et al., *The New Era of Botnets*, McAfee: An Intel Company, white paper, Santa Clara, CA, 2010, pp. 3-4, http://www.mcafee.com/us/resources/white-papers/wp-new-era-of-botnets.pdf.

[12] John Markoff, "A Robot Network Seeks to Enlist Your Computer," *New York Times*, October 20, 2008.

[13] Richard A. Clark and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), p. 13.

Early botnet operators were often skilled coders. In contrast, today an underground industry of skilled botnet providers exists, but operators no longer have to be fluent coders. Starting in 2004, bots got considerably easier to use as the result of new applications that allowed hackers to build bots by pointing and clicking, resulting in a bloom of spam in email inboxes across the globe.[14] In addition to unwanted advertising, botnets can generate denial-of-service (DoS) attacks and spread malware.

Distributed Denial of Service Attacks

Distributed Denial of Service (DDoS) attacks flood their target with requests, consuming the target's bandwidth and/or overloading the capacity of the host server, resulting in service outages. These attacks are "distributed" because effective attacks employ botnets, distributing the source of requests across an entire network of zombie computers. DDoS attacks are unique for three reasons: (1) they exploit vulnerabilities in their target's software or operating system that cannot be easily repaired or "patched;" (2) each individual packet is a legitimate request—only the rate and total volume of packets gives an attack its destructive impact; and (3) the severity of the attack is measured in terms of its duration. Unlike malware, which alters or infects its target, DDoS attacks consist of the same types of packets, a unit of data, that a typical user would send when making a legitimate request. The only difference is in the number and frequency with which the attacker generates requests. The goal of a DDoS attack is to render targeted networks unavailable or non-responsive, thereby preventing users from accessing information for the duration of the attack.[15]

The pathway of a DDoS attack is known as a *vector*. Today it is common for an attack to have multiple vectors. A DDoS attack carried out by botnets along multiple vectors can interrupt services for days, weeks, or even months. More sophisticated attacks take advantage of vectors that amplify their strength through a process that generates exponential reverberations. The ability to amplify an attack, for instance by tricking a server into responding to a target with an even larger packet than what was originally sent, increases an already substantial asymmetric advantage. Botnet applications not only make DDoS attacks relatively easy to mount, but the redundant and decentralized nature of the Internet makes attribution difficult.[16] In theory, a DDoS attack could temporarily take down the entire web by simultaneously targeting the 13 root servers on which all Internet traffic depends.[17] In practice, this has not yet happened.

Automated Defense Systems

Retaliatory hacking, a response to network breaches that has been used in the private sector, has gained traction within DOD as a means to stage an "active defense." These potentially offensive operations may occur when a systems administrator sees an intrusion and in turn breaches the assumed point of origin, either to retrieve or destroy information. However, such activities are complicated for two reasons: uncertainty in attack attribution and active defense may violate

[14] Zheng Bu, Pedro Bueno, Rahul Kashyap, et al., *The New Era of Botnets*, McAfee: An Intel Company, White Paper, Santa Clara, CA, 2010, pp. 3-4, http://www.mcafee.com/us/resources/white-papers/wp-new-era-of-botnets.pdf.

[15] Ziv Gadot, Eyal Benishti, Lior Rozen, et al., *Radware Global Application & Network Security Report 2012*, Radware, White Paper, Mahwah, NJ, 2013, p. 1, file:///C:/Users/aharrington/Downloads/a7b991da-b96e-4cd7-bf8c-236b1e7e4c67.pdf.

[16] Ziv Gadot, Eyal Benishti, Lior Rozen, et al., *Radware Global Application & Network Security Report 2012*, Radware, white paper, Mahwah, NJ, 2013, p. 18.

[17] http://www.root-servers.org/.

terms enacted in the Computer Fraud and Abuse Act of 1986.[18] This law criminalizes unauthorized breaches and other computer-related activity, including the distribution of malware and use of botnets. Although the military would be involved in a counterattack only during a national security crisis, the government may tacitly encourage companies to engage in retaliatory hacking as the first line of defense for the nation's critical infrastructure. For example, the Defense Advanced Research Projects Agency (DARPA) has launched a Cyber Grand Challenge program to hasten the development of automated security systems capable of responding to and neutralizing cyberattacks as fast as they are launched. Automated defense systems may also be configured to launch a counterattack in the direction of a network breach.

Targets

Attacks on information technology destroy, degrade, and/or exfiltrate data from a host computer. The intended effect of a cyberattack can be related to the attack target. Within the context of cyberwarfare, two areas are attractive targets for a potential adversary: government and military networks, and critical infrastructure and industrial control systems.

Government and Military Networks

Nation states and other entities target government and military networks to exfiltrate data, thereby gaining an intelligence advantage, or to potentially plant a malicious code that could be activated in a time of crisis to disrupt, degrade, or deny operations. In 2008, The Pentagon itself was a target of a massive breach, when an infected thumb drive was inserted into a computer connected to DOD classified networks. The discovery of the malware, named Agent.btz, led to a massive cleanup operation code-named Buckshot Yankee.[19] While the incident appeared to be related to espionage and theft of sensitive information, it is possible that malware could also contain a hidden, more nefarious function, such as the capability to disable communications or spread disinformation.

Critical Infrastructure and Industrial Control Systems

Civilian critical infrastructure comprises networks and services that are considered vital to a nation's operations and are owned and operated by the private sector.[20] Examples of these sectors include energy, transportation, financial services, food supplies, and communications. These sectors may be particularly vulnerable to cyberattack because they rely on open-source software or hardware, third-party utilities, and interconnected networks.

Large-scale industrial control systems (ICS), such as the supervisory control and data acquisition (SCADA) systems that provide real-time information to remote operators, present a unique vulnerability. Disabling an electric power plant by attacking its SCADA system, for instance, will have many follow-on effects. These systems, as they control the operations of a particular platform, are referred to by the Defense Department as "operations technology."

---

[18] 18 U.S.C. §1030.

[19] Ellen Nakashima, "Cyber-intruder sparks response, debate" *Washington Post*, December 8, 2011, http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

[20] Critical Infrastructure is defined in 42 U.S.C. 5195c(e) as: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

From highly specialized equipment, such as uranium enrichment plants, to mundane heating and air conditioning systems and office photocopiers, the capability to remotely control industrial hardware for maintenance and operations purposes also makes these machines vulnerable to cyberattacks. Attacks against operations technology (OT) are different than information technology (IT) attacks because OT attacks can produce kinetic effects. Although OT controls primarily mundane infrastructure, these built environments are increasingly networked environments, which adds a complicated layer to training and maintenance.

Actors and Attribution

With low barriers to entry, multiple actors may take part in use of the Internet and networked technology as a means to achieve strategic effects. These actors may represent nation states, politically motivated hacker groups or "hactivists," or terrorist and other criminal organizations. Directly attributing a cyberattack to any one of these groups can be challenging, particularly as they may sometimes operate in concert with each other, though for differing motivations.

Nation States

Cyberwarriors are agents or quasi-agents of nation states who develop capabilities and undertake cyberattacks to support a country's strategic objectives.[21] These entities may or may not be acting on behalf of the government with respect to target selection, attack timing, or type(s) of cyberattack. Moreover, cyberwarriors are often blamed by the host country when the nation that has been attacked levies accusations against that country. Typically, when a foreign government is presented with evidence that a cyberattack is emanating from its country, the nation that has been attacked is told that the perpetrators acted of their own volition, not at the behest of the government.

Politically Motivated Hacktivists

Cyberhactivists are individuals who perform cyberattacks for pleasure, or for philosophical or other nonmonetary reasons. Examples include someone who attacks a technology system as a personal challenge (who might be termed a "classic" hacker), and a "hacktivist," such as a member of the cybergroup Anonymous, who undertakes an attack for political reasons. The activities of these groups can range from simple nuisance-related DoS attacks to disrupting government and private corporation business processes.

Terrorists and Organized Crime

Cyberterrorists are state-sponsored or non-state actors who engage in cyberattacks as a form of warfare. Transnational terrorist organizations, insurgents, and jihadists have used the Internet as a tool for planning attacks, recruiting and radicalizing members, distributing propaganda, and communicating.[22] No unclassified reports have been published regarding a terrorist-initiated cyberattack on U.S. critical infrastructure. However, the essential components of that infrastructure are demonstrably vulnerable to access and even destruction via the Internet. In 2007, a U.S. Department of Energy test at Idaho Labs demonstrated the ability of a cyberattack to

[21] For additional information, see CRS Report RL31787, *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*, by Catherine A. Theohary.

[22] For additional background information, see archived CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John W. Rollins and Clay Wilson.

shut down parts of the electrical grid. In the test, known as the Aurora Experiment, a cyberattack on a replica of a power plant's generator caused it to self-destruct.

Advanced Persistent Threats

The term "Advanced Persistent Threat" (APT) has been used within the intelligence community to describe nation-state cyberespionage activities. However, organizations that may or may not be state-sponsored may also use APT techniques to gain a competitive military advantage. Characteristics of an APT include a high level of sophistication in the malware's code, along with the targeting of certain networks or servers to glean specific information of value to the attackers or to cause damage to a specific target. Likely targets include government agencies and corporations in critical infrastructure sectors such as financial, defense, information technology, transportation, and health. In 2013, the U.S. security firm Mandiant published a 60-page intelligence report on a Chinese operation, which the firm identified as APT1, that allegedly stole hundreds of terabytes of data from at least 141 organizations across 20 industries worldwide since 2006.[23] Mandiant's analysis concluded that APT1 is likely government-sponsored (believed to be the 2nd Bureau of the People's Liberation Army General Staff Department's 3rd Department) and one of the most persistent of China's cyber threat actors.

Attribution Issues

Analysts trying to determine the origin of a cyberattack are often stymied by the use of botnets. First, computers infected by a botnet may be located in countries around the world, obscuring the country of origin of the botnet's commander, known as the bot herder. Second, the identity of the server controlling the botnet may be obscured by the prevalence of peer-to-peer software[24]. In addition to these concerns, Internet provider (IP) addresses that might otherwise trace the location of a computer that launched an attack can be faked (known as "spoofing"), and even with a valid IP address, it may be virtually impossible to verify who was behind the computer at the time an attack was launched. This uncertainty is also true of a computer that has been infected unbeknownst to the user. At the nation-state level, a certain amount of deniability in terms of cybersecurity and network control is plausible. Given the proliferation of hacker organizations and the cyber weapons at their disposal, states can easily claim a lack of responsibility for rogue cyber actors and attacks that appear to stem from within state borders.

Threat Environment

Cyberattack is a persistent threat. This section describes events that have provoked a political and/or military response from leaders in one or more state. The case studies provided are not exhaustive; excluded are many instances of cyber espionage that could arguably be considered international incidents. Instead, this section focuses primarily on cyberattacks that (1) have had strategic effects, (2) play a tactical role in a larger military operation, (3) carry implications for the ability of a state to carry out future military operations, or (4) threaten public trust in the reliability and security of information on the Internet.

[23] Accessed at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[24] Peer-to-peer software refers to computer networks in which each computer can act as a server for the others, obviating the need for a central server for command and control.

Cyberattack Case Studies

Each of the cyberattacks in this section illustrates a different tactical and/or strategic use of weapons in cyberspace. The events in each of these cases raised questions about acts of terror and/or war in cyberspace and the role of the military.

Estonia: Cyberattack as Siege

Estonia is a Baltic state of approximately 1.3 million people that regained its independence from the Soviet Union in 1991. In 2004, Estonia joined the European Union (EU). Technologically, Estonia distinguished itself as the home of Skype, a widely popular online voice and video communication software. Today, Estonia is one of the most wired nations on earth. Estonians conduct most of their daily business online, even carrying out the basic rights and responsibilities of democratic citizenship, such as voting, through the Internet. As a result, Estonia is particularly vulnerable to cyberattack.[25]

On the morning of April 28, 2007, waves of DDoS attacks besieged websites in Estonia. Over the next two weeks, attackers targeted crucial sectors, shutting down Internet access to hundreds of key government, banking, and media web pages. Estonians were unable to bank online or retrieve cash from ATMs. Attackers also targeted Internet addresses for servers, threatening the telephone network and the credit card verification system. Vital services simply ceased to function, unable to stand back up before the next wave of attack. Where possible, organizations cut off all international traffic, closing the gates against the attack. Unlike previous DoS attacks that hit a single site over the course of days, this attack brought communication and commerce in a sovereign nation to a halt for weeks.[26]

The 2007 cyberattacks appear to have originated in Russia. On April 27, 2007, Estonian officials carried out a controversial plan to relocate a World War II-era statue of a Red Army soldier from a central location in Tallinn, the nation's capital, to a military cemetery in a suburb. Despite ominous warnings from the Russian government that removing the statue honoring the sacrifice of Russian soldiers would prove "disastrous for Estonians," Estonia, after 16 years of independence, decided to move the reminder of Soviet occupation.[27]

What role, if any, the Russian government actually played in the attack is unclear. The Russian government claimed the attack was an online version of an angry mob. Evidence suggests that patriotic hackers played an important role in the attack. The Pro-Putin movement Nashi ("Ours"), which organizes political events for young adults, claimed at least partial responsibility for engaging in cyber activities to counter "anti-Fatherland" forces.[28] Suspicion remains about government involvement, though. Patriotic hacking can provide cover for behind-the-scenes coordination efforts.

The attacks followed instructions posted in Russian language Internet chat rooms on how to generate DoS attacks. The posts included calls for a coordinated attack at the stroke of midnight on May 9, the day Russians celebrate their World War II victory. At exactly midnight in Moscow,

[25] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[26] Richard A. Clark and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010).

[27] Ibid.

[28] Peter Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2013), pp. 110-111.

11p.m. in Tallinn, nearly 1 million computers around the globe navigated to Estonian websites. Surging at 4 million packets per second, Internet traffic in Estonia increased 200-fold, squeezing the bandwidth of an entire nation.[29]

Prepared for the surge, the head of the Estonian computer emergency response team enlisted the help of individuals responsible for the health and care of the Internet root server system to follow attacks back to their source and block specific computers from accessing the servers. This strategy mitigated the effects of the attack. Then suddenly the surges in traffic stopped as suddenly as they had started.[30]

Because Estonia is a member of NATO and the European Union, this event exposed how unprepared those organizations may have been to respond to a cyberattack against a member state. Had Estonia invoked NATO's Article V collective security provision, doing so would have raised several thorny questions about what kind of attack triggers those alliance obligations. The fact that the cyberattack was targeted at a member state and prompted an official state response was complicated by the inability to identify the aggressor. Moreover, the attack did no physical damage, and in the end did no permanent damage to Estonia's web-based infrastructure. The damage was measurable only in terms of short-lived commercial losses.[31] This kind of cyberattack is sometimes likened to a weather event. Snow storms, although a temporary crisis, rarely have any lasting effects. How serious a threat the storm presents depends, at least in part, on one's capability to weather the storm.[32] Although Estonian Defense Ministers viewed this event in terms of a national security crisis, other security analysts described it as a "cyber riot" or "costly nuisance," comparing it to an electronic sit-in where traffic to public and commercial sites is slowed or blocked to make a political point.

Georgia: Cyberattack and Invasion

In 2008, Russia invaded Georgia by land and air and blockaded the nation by sea. Simultaneously, pro-Russian hackers besieged Georgia's Internet, all but locking down communication for the duration of the armed conflict. Although Georgia is not a heavily wired society—at the time experts ranked it 74th out of 234 nations in terms of Internet addresses, behind Nigeria, Bangladesh, Bolivia, and El Salvador[33]—the attacks were a significant event in the development of cyberwar because they synchronized patriotic hacking with government-sponsored military movements.[34]

Like Estonia, Georgia is a former Soviet state; it declared its independence in 1991. Tensions with Russia have persisted and were not eased by Georgia's failed bid to join NATO in the spring of 2008.[35] Over the course of that same summer, well-armed Russian-backed separatists began consolidating control over two predominately Russian-speaking regions on the country's northern

---

[29] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[30] Ibid.

[31] Ibid.

[32] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Washington, DC: RAND, 2007).

[33] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

[34] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011.

[35] For further discussion, see CRS Report RL34618, *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. Interests*, by Jim Nichol

border, Abkhazia and South Ossetia. As tensions rose, separatists—some of whom were believed to be Russian special forces—clashed with Georgian police.[36]

In mid-July, the cyberattacks started. The Georgian President's website was the first high-profile target. Although the DDoS attack vector passed through a U.S.-based, commercial IP address, experts identified the malware that hackers used to generate the attack as a "MachBot" DDoS controller. Machbot is written in Russian and a known tool of Russian criminal groups.[37] Reportedly, pro-Russian hackers were discussing the attacks on websites and in chat rooms; in addition to the higher-profile attack, hackers also temporarily shut down Georgian servers.[38]

Three weeks later, on August 8, Russian tanks crossed the border into South Ossetia. Accompanying the ground invasion was a second round of DDoS attacks. One of the first targets was an online forum popular with pro-Georgian hackers. This preemptive attack reduced, but did not entirely eliminate, the number of counterattacks against Russian targets.[39] As the troops moved in, Georgians were unable to access 54 local websites with critical information related to communications, finance, and the government.[40]

Georgian officials transferred critical Internet resources to U.S., Estonian, and Polish host servers. Refuge for some websites, including those of the President and Ministry of Defense, was granted by an American executive from the privately owned web-hosting company Tulip Systems, but without the knowledge or authority of the U.S. government. Tulip Systems reported experiencing attacks on its servers, a fact that raises troubling questions about sovereignty in the age of cyberwarfare.[41]

The fighting lasted five days. During that time, Georgia's Internet connection was besieged by attacks and unable to communicate via web with the media. Reportedly, cyberattacks followed the same target patterns as the land and air invasions, with DDoS attacks taking out the communications prior to bombing or ground troop movements. Perhaps most importantly, the cyberattacks and the air attack spared critical infrastructure associated with Georgia's energy sector.[42]

Iran: Cyberattack with Kinetic Effect

When programmers at a small Belarussian cybersecurity firm first discovered a new computer worm in June 2010, they knew it was unusually sophisticated because it was exploiting a "zero-day vulnerability" in Microsoft Windows. Malware that outsmarts programmers and developers by identifying an unanticipated weakness in the Windows operating systems is rare. Even so, the cybersecurity specialists who originally detected Stuxnet had no idea just how sophisticated this new worm would turn out to be.[43] The idea of sabotaging industrial control systems from a

[36] Mikheil Saakashvili, "Let Georgia be a lesson for what will happen to Ukraine," *The Guardian*, March 14, 2014.

[37] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Winter 2008, p. 65, http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/08winter/korns.pdf.

[38] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, p. 3

[39] Ibid.

[40] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, p. 2.

[41] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," Parameters, Winter 2008, p. 65, http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/08winter/korns.pdf.

[42] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, p. 4.

[43] P. Mittal, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

remote location was not new, but creating a worm that could search for a single target was revolutionary, and this is what Stuxnet's authors had achieved. [44]

The intended target appears to have been industrial control systems in Iran's nuclear facility at Natanz. The first clue was the pattern of infected computers: the Stuxnet worm attacked air-gapped networks (i.e., those not connected to the Internet). The worm propagated by infecting local hosts via a USB thumb drive. While a computer scanned the contents of the inserted thumb drive, the worm surreptitiously installed a partially encrypted file. This file contained a stolen security certificate that fooled its host into believing that the Stuxnet worm was a trusted program. From its initial host computer, Stuxnet could travel throughout a networked system. Although Stuxnet did not propagate itself through the web, if an infected computer was connected to the Internet, the worm would automatically begin sending information back to one of two domain names hosted on servers in Denmark and Malaysia. Once cybersecurity experts realized that infected computers were "phoning home," they redirected that traffic into a sinkhole they controlled. By analyzing the collected data, the experts were able to map the pattern of infection. Unlike most malware, which spreads rapidly through densely networked countries like the United States and South Korea, Stuxnet was overwhelmingly concentrated in Iran. Of the first 38,000 infected computers, 22,000 were located in Iran.[45]

The second clue as to Stuxnet's intended target was that, reportedly starting in 2009, International Atomic Energy Agency inspectors noticed the significantly higher-than-average rate at which Iran was removing and repairing centrifuges in its uranium enrichment facility at Natanz.[46] Centrifuges built to process natural uranium into a form capable of fueling a nuclear power plant, or building a nuclear warhead, are extremely delicate. Among the fastest spinning objects on earth, any irregularities in a centrifuge's rotor will cause imbalances. Even a fingerprint on the rotor would cause it to spin out of control and do irreparable damage.[47] As cybersecurity specialists dug deeper into the code, they identified commands that were specific to the industrial control system Simatic WinCC Step7, produced by the German company Siemens. This is the same controller Iran uses in its uranium-enrichment facilities to control its centrifuges. Once Stuxnet identified its target, the malware automatically commanded the centrifuges to spin at frequencies significantly faster and then slower than normal, doing damage to the delicate rotors.

---

[44] In his memoir, Thomas Reed, a former U.S. Air Force secretary who served in the National Security Council during President Reagan's tenure, describes a successful CIA plot to sabotage the Soviet Union's Siberian pipeline in 1982 by tricking Moscow into stealing booby-trapped software. The faulty ICS software overpressurized the system causing "the most monumental non-nuclear explosion and fire ever seen from space." Alec Russell, "CIA plot led to huge blast in Siberian gas pipeline" *The Telegraph*, February 28, 2004, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html; Michael Joseph Gross, "A Declaration of Cyber-War," *Wired*, April 2011, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

[45] Eventually, specialists identified over 100, 000 corrupted devices. For more see P. Mittal, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/; Ralph Langer, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," November, 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf; William J. Broad, John Markoff, and David Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0; Paul Kerr, John Rollins and Catherine Theohary, "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability," *Congressional Research Service Report*, December 9, 2010.

[46] P. Mittal, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

[47] Anne Harrington and Matthias Englert, "How Much is Enough? The Politics of Technology and Weaponless Nuclear Deterrence" in *International Relations and the Global Politics of Science and Technology*, eds. Mariana Carpes and Maximilian Mayer, Berlin: Springer, 2014.

Meanwhile, Stuxnet evaded detection by making it appear to the operators monitoring the system (via a computer screen) that nothing had changed.[48]

The overall effect of Stuxnet on the Iranian nuclear program is unclear. Iran has since acknowledged the attack but maintains that Stuxnet did not change the rate at which it was able to increase its stockpile of enriched uranium.[49] David Albright and Christina Walrond of the Institute for Science and International Security argue that although the rate of production has not changed, starting in late 2009, Iran required more centrifuges to perform the same amount of work. Albright and Walrond did not definitively argue that Stuxnet caused Iran's efficiency to decline, nor did they discount that possibility, instead stating, "It is likely that multiple factors have played a role in the diminished effectiveness of the FEP [fuel enrichment plant].... The available data are too general to determine the actual situation."[50]

No one has claimed responsibility for the attack, but in January 2011, but the *New York Times* reported that Stuxnet was a joint venture of the United States and Israel. Reportedly, Israel constructed a centrifuge plant at Dimona identical to the one in Natanz to simulate the attack. The United States allegedly provided information about vulnerabilities in the Siemens controller, access to which had been gained through a cybersecurity collaboration between Siemens and the Idaho National Lab.[51]

The DOD and U.S. Cyber Command

The Department of Defense is responsible for securing its own networks, the Department of Defense information networks (DODIN), or .mil domain, formerly known as the Global Information Grid (GIG). The requested cybersecurity budget for DOD was approximately $5.1 billion for FY2015.This figure represents a portion of the President's requested overall IT budget for DOD that same year (approximately $36 billion). The DOD cybersecurity budget grew by $1 billion from 2013 to 2014, but this increase may reflect changes in how DOD programmatic elements have defined "cybersecurity" programs. In general, the DOD cybersecurity budget comprises the following activities: Information Assurance, Cyberspace Operations, National Cybersecurity Initiative/Defense Industrial Base/Defense Cyber Crime Center, and U.S. Cyber Command.[52]

After recognizing that cyberspace is a global operating domain as well as a strategic national asset, DOD reorganized its cyber resources and established the U.S. Cyber Command in 2010. This sub-unified command under the U.S. Strategic Command is co-located at Fort Meade, Maryland with the National Security Agency (NSA). It combines offensive and defensive

[48] The cybersecurity company Symantec has since established that there were multiple variants of Stuxnet. The earlier variant closed valves, causing a build-up of pressure that will make the centrifuge wobble and damage the rotors, rather than directly affecting the rate at which the centrifuge spins. For more, see Institute for Science and International Security, *Basic Attack Strategy of Stuxnet 0.5 rev. 1*, Institute for Science and International Security, Washington, DC, February 28, 2013, http://isis-online.org/isis-reports/detail/basic-attack-strategy-of-stuxnet-0.5/.

[49] Dr. Fereydoun Abassi, Vice President of the Islamic Republic of Iran and Head of Atomic Energy Organization of Iran, "Statement at the IAEA 56th General Conference," September 17, 2012; P. Mittal, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, pp. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

[50] David Albright and Christina Walrond, *Performance of the IR-1 Centrifuge at Natanz*, Institute for Science and International Security, Washington, DC, October 18, 2011, http://isis-online.org/isis-reports/detail/test1/8.

[51] William J. Broad, John Markoff, and David Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0.

[52] Source: Internal Department of Defense budget documents.

capabilities and is commanded by a four-star general, also the director of the NSA. The NSA's primary missions are information assurance for National Security Systems and signals intelligence. Also located within NSA is the Central Security Service, the military's cryptology component. As an intelligence agency, NSA operates under the authorities of Title 50 U.S.C., War and National Defense. U.S. Cyber Command operates under U.S.C. Title 10, Armed Forces—the authorities through which the military organizes, trains, and equips its forces in defense of the nation.

Cyber Command Mission and Force Structure

As previously stated, one of the main missions of U.S Cyber Command is to defend and operate the DODIN. In his nomination hearing before the Senate Armed Services Committee, then-Vice Admiral Michael S. Rogers, tapped to become the head of U.S. Cyber Command, described the duties of the Cyber Commander thusly:

> The Commander, U. S. Cyber Command (USCYBERCOM) is responsible for executing the cyberspace missions specified in Section 18.d.(3)of the Unified Command Plan (UCP) as delegated by the Commander, U.S. Strategic Command (USSTRATCOM) to secure our nation's freedom of action in cyberspace and to help mitigate risks to our national security resulting from America's growing dependence on cyberspace. Subject to such delegation and in coordination with mission partners, specific missions include: directing DODIN operations, securing and defending the DODIN; maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; integrating and synchronizing of cyberspace operations with combatant commands and other appropriate U.S. Government agencies tasked with defending the our nation's interests in cyberspace; provide support to civil authorities and international partners. All these efforts support DoD's overall missions in cyberspace of defending the nation against cyber attacks, supporting the combatant commands, and defending Department of Defense networks.[53]

Operators at the U.S. Cyber Command are sometimes referred to as "cyber warriors," although this term does not appear in official Department of Defense definitions. Reports of USCYBERCOM-planned workforce structures yield clues regarding the activities a so-called cyber warrior might undertake. First reported in the *Washington Post*, "The plan calls for the creation of three types of Cyber Mission Forces under the Cyber Command: 'national mission forces' to protect computer systems that undergird electrical grids, power plants and other infrastructure deemed critical to national and economic security; 'combat mission forces' to help commanders abroad plan and execute attacks or other offensive operations; and 'cyber protection forces' to fortify the Defense Department's networks."[54]

These multiservice Cyber Mission Forces numbered under 1,000 in 2013, when DOD announced plans to expand them to roughly 5,000 soldiers and civilians. The target number has since grown to 6,200, with a deadline at the end of FY2016. In early November 2014, a leaked classified document was reported to have stated that "additional capability may be needed for both surge capacity for the [Cyber Mission Forces] and to provide unique and specialized capabilities" for a

[53] Advanced Questions for Vice Admiral Michael S. Rogers, Nominee for Commander, United States Cyber Command, Senate Armed Services Hearing of March 11, 2014, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

[54] From http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html.

whole-of-government and nation approach to security in cyberspace.[55] USCYBERCOM Commander Admiral Michael S. Rogers has said that overall, Cyber Mission Forces will be about 80% military and 20% civilian. At a recent conference, Deputy Commander of USCYBERCOM Lieutenant General James McLaughlin said the Cyber Mission Force was being formed into 133 teams of tactical units that will [56] support all Combatant Commands, and that at least half of these teams would be used for defensive measures.

Each of the four military services provides cyber mission forces to USCYBERCOM. All of the services' cyber divisions plan to steadily increase their number of cyber operators over the next two years.

USCYBERCOM and Information Sharing

In May 2011, DOD launched a pilot voluntary program (the DIB Cyber Pilot) involving several defense industry partners, the NSA and DOD, to share classified threat-vector information among stakeholders. Under the DIB Cyber Pilot, NSA shares threat signatures with participating defense companies. One aspect of the program was sharing by the NSA of threat signatures obtained through its computer monitoring activities. DHS subsequently initiated the Joint Cybersecurity Services Pilot (JCSP) in January 2012 and announced in July that the program would be made permanent, with the renamed DIB Enhanced Cybersecurity Services (DECS) as the first phase. In this program, DHS communicates with participating commercial Internet service providers directly, while DOD still serves as the point of contact for participating DIB contractors.

Authorities

Authorities for U.S. military operations in cyberspace are not currently organized according to the nature of the perceived threat, whether espionage, crime, or war. Instead, authorities are organized according to the domain (.mil, .gov, .com, etc.) in which the activity is taking place, as opposed to its motivations or effects. Presidential Policy Directive 20, discussed in greater detail below, distinguishes between *network defense* on the one hand and *offensive and defensive cyberspace operations* on the other.

U.S. policy on network defense is to adopt a risk-management framework published by the Department of Commerce's National Institute of Standards and Technology. Responsibility for implementing the framework is shared among different government departments and agencies, with U.S. Cyber Command responsible for the .mil domain and the Department of Homeland Security responsible for the .gov domain. Adoption of the NIST framework is voluntary for private companies and their own network defense.

One of the instruments through which offensive cyberspace operations are conducted may be a classified "Execute Order," defined by DOD as an order issued by the Chairman of the Joint Chiefs of Staff, at the direction of the Secretary of Defense, to implement a decision by the President to initiate military operations.[57] According to The Federation of American Scientists' *Secrecy News,* Air Force Instruction 10-1701, entitled "Command and Control (C2) for Cyberspace Operations," dated March 5, 2014, states, "Classified processes governing C2

[55] http://www.defensenews.com/article/20141103/TRAINING/311030018/As-cyber-force-grows-manpower-details-emerge.

[56] Wyatt Olson, "Cyber Command trying to get running start, add staff," *Stars and Stripes*, December 11, 2014.

[57] DOD Dictionary of Military and Associated Terms, JP1-02.

[command and control] of AF [Air Force] offensive and defensive cyberspace operations conducted by AF Cyber Mission Forces are addressed in a classified CJCS [Chairman, Joint Chiefs of Staff] Execute Order (title classified) issued on 21 Jun 13."[58] Then-Vice Admiral Michael Rogers, as a nominee for Commander, U.S. Cyber Command (and NSA Director), said before the Senate Armed Services Committee that "geographic combatant commanders already have authority to direct and execute certain Defensive Cyberspace Operations (DCO) within their own networks." However, the Execute Order suggests that there may be standing orders to conduct offensive cyberspace operations as well.

The following section provides a brief overview of evolving norms in cyberspace and the authorities that govern network defense and cyberspace operations.

Legislative Authorities

Section 941of the National Defense Authorization Act for Fiscal Year 2013 (P.L. 112-239), affirms the Secretary of Defense's authority to conduct military activities in cyberspace. The provision's language is similar to that in Section 954 of final conference report to accompany H.R. 1540, the National Defense Authorization Act for Fiscal Year 2012. In this version, this section reaffirms that the Secretary of Defense has the authority to conduct military activities in cyberspace. In particular, it clarifies that the Secretary of Defense has the authority to conduct clandestine cyberspace activities in support of military operations pursuant to a congressionally authorized use of force outside of the United States, or to defend against a cyberattack on an asset of the DOD.[59] The section highlights the blurred lines between military operations and intelligence activities, particularly with respect to cyberspace. In general, Title 10 and Title 50 of the U.S. Code refer to distinct chains of command and missions belonging to the armed forces and intelligence agencies, respectively. The U.S. Cyber Command, the military entity responsible for offensive operations in cyberspace and subject to Title 10 authorities, is co-located with and led by the Director of the National Security Agency, a Title 50 intelligence organization. Computer Network Attack, the military parlance for offensive operations, is closely related to and at times indistinguishable from Computer Network Exploitation, which is used to denote data extrapolation or manipulation.

According to DOD, a clandestine operation is one that is "sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor."[60] Under Title 50, a "covert action" is subject to presidential finding and Intelligence Committee notification requirements. Traditional military activity, although undefined, is an explicit exception to the Title 50 U.S.C. covert action definition in Section 913 as the identity of the sponsor of a traditional military activity may be well known.

According to the Joint Explanatory Statement of the Committee of Conference, H.R. 1455, July 25, 1991, traditional military activities

[58] U.S. Military Given Secret "Execute Order" on Cyber Operations Military Doctrine, Secrecy http://blogs.fas.org/secrecy/2014/03/execute-order/.

[59] The previous version would have given the Secretary of Defense the authority to conduct clandestine cyberspace activities in support of military operations pursuant specifically to the Authorization for the Use of Military Force (P.L. 107-40; 50 U.S.C. 1541 note) outside of the United States or to defend against a cyberattack on an asset of the Department of Defense.

[60] Department of Defense Dictionary of Military and Associated Terms, Joint Publication1-02, as amended through August 15, 2014. [reconcile with similar footnote above]

> include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding and related to hostilities which are either anticipated (meaning approval has been given by the National Command Authorities for the activities and or operational planning for hostilities) to involve U.S. military forces, or where such hostilities involving United States military forces are ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly.

By this reading, a clandestine operation falls under the traditional military activity rubric, because the identity of the sponsor is not concealed. Hence, by referring only to "clandestine" operations rather than covert operations, the provision distinguishes between approval and reporting requirements for military-directed cyberspace operations and those conducted by the intelligence community. By requiring quarterly briefings to the congressional defense committees, the language would also appear to address concerns that a "clandestine" or "traditional military activity" designation for a cyber operation would skirt the strict oversight requirements of its covert counterpart. However, confusion may remain regarding the proper role and requirements of the military, because some cyber operations may contain both covert and clandestine elements. Another consideration is the military's responsibility to notify congressional intelligence committees of computer network exploitation activities undertaken as "operational preparation of the environment."

Executive Authorities

In December 2008, President-elect Obama offered details about the cybersecurity goals his Administration would pursue, including "strengthening federal leadership on cybersecurity, developing next-generation secure computers and networking for national security applications, and protecting the IT infrastructure to prevent corporate cyberespionage."[61] In February 2009, he initiated a 60-day interagency review with the goal of developing "a strategic framework to ensure" that federal cybersecurity initiatives "are appropriately integrated, resourced, and coordinated with Congress and the private sector."[62] The White House released the *Cyberspace Policy Review* in May 2009.[63] At that time, the President announced[64] that the Administration would "pursue a new comprehensive approach to securing America's digital infrastructure," and that he was creating a new White House office to be led by a Cybersecurity Coordinator—a senior cybersecurity policy official, often referred to as the "Cyber Czar," assigned to the Office of the President and responsible for coordinating the nation's cybersecurity-related policies.

While many security observers saw these initial efforts by the Obama Administration as a positive step, others were concerned that government-wide collaborative efforts were not keeping pace

[61] "Report: White House should oversee cybersecurity," *CNN*, December 8, 2008, http://www.cnn.com/2008/TECH/12/08/cyber.security/.

[62] The White House, "President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review," press release, February 9, 2009, http://www.whitehouse.gov/the-press-office/president-obama-directs-national-security-and-homeland-security-advisors-conduct-im.

[63] The White House, *Cyberspace Policy Review*, May 29, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; the White House, "Cyberspace Policy Review [Supporting Documents]," May 2009, http://www.whitehouse.gov/cyberreview/documents/.

[64] The White House, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," press release, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

with the threats directed at U.S. technological global interests. Between 2009 and 2013, cyber threats to U.S. infrastructure and other assets became a growing concern to policy makers.[65]

In the absence of legislative action, in 2012 the Obama Administration announced a new Presidential policy directive related to U.S. Cyber Operations, the contents of which remain classified, and began drafting an executive order on cybersecurity practices, Executive Order 13636, Improving Critical Infrastructure Cybersecurity, released after a year of interagency debate and review.

At the federal level, five executive orders and Presidential directives authorize offensive and defensive action in cyberspace:

National Security Presidential Directive 54/Homeland Security Presidential Directive 23—The Comprehensive National Cybersecurity Initiative

The Obama Administration's *Cyberspace Policy Review* builds on the Comprehensive National Cybersecurity Initiative (CNCI) launched in January 2008 by the George W. Bush Administration via a classified presidential directive.[66] The CNCI established a multipronged approach for the federal government to identify threats, address telecommunications and information-system vulnerabilities, and respond to or proactively address entities that wish to steal or manipulate protected data on secure federal systems.[67]

Presidential Policy Directive 20 (PPD-20)—U.S. Cyber Operations Policy

President Obama implemented PPD-20 on U.S. Cyber Operations Policy in October 2012. Although subsequently leaked to the public in June of 2013,[68] PPD-20's contents remain classified, with the exception of what the White House shared in a brief fact sheet. A widely cited *Washington Post* article published on November 14, 2012 asserted the significance of PPD-20:

> For the first time ... the directive explicitly makes a distinction between network defense and cyber-operations to guide officials charged with making often-rapid decisions when confronted with threats. The policy also lays out a process to vet any operations outside government and defense networks and ensure that U.S. citizens' and foreign allies' data and privacy are protected and international laws of war are followed.

The article went on to quote an unnamed senior administration official on the distinction between defense and offense, clarifying that "network defense is what you're doing inside your own networks.... Cyber-operations is stuff outside that space, and recognizing that you could be doing that for what might be called defensive purposes."[69]

---

[65] CRS Report R41674, *Terrorist Use of the Internet: Information Operations in Cyberspace*, by Catherine A. Theohary and John W. Rollins; CRS Report R42507, *Cybersecurity: Authoritative Reports and Resources, by Topic*, by Rita Tehan.

[66] "The Comprehensive National Cybersecurity Initiative," http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative; National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23).

[67] CRS Report R40427, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, by John W. Rollins and Anna C. Henning.

[68] Joshua Eaton, "American cyber-attack list uncovered," *Al Jazeera*, http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html, accessed August 12, 2014.

[69] Ellen Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks" *Washington Post*, November 14, 2012.

PPD-20 closes a perceived gap in the authorities necessary for DOD to defend the nation in cyberspace, a gap that has not been addressed by Congress. The directive does not create new powers for federal agencies or the military; however, by distinguishing between network defense and cyber operations, it provides a policy framework for the Pentagon's rules of engagement for cyberspace. As specifically described in the White House fact sheet, PPD-20:

- takes into account the evolution of the threat and growing experience with the threat;
- establishes principles and processes for using cyber operations so cyber tools are integrated with the full array of national security tools;
- provides a whole-of-government approach consistent with values promoted domestically and internationally and articulated in the International Strategy for Cyberspace;
- mandates that the United States take the least action necessary to mitigate threats; and
- prioritizes network defense and law enforcement as preferred courses of action.[70]

Executive Order 13636—Improving Critical Infrastructure Cybersecurity

The White House released EO 13636 on February 12, 2013. This executive order declares that "it is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure (CI) and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" (Section 1). The order:

- expands information sharing and collaboration between the government and the private sector, including sharing classified information by broadening a program developed for the defense industrial base to other CI sectors;
- develops a voluntary framework of cybersecurity standards and best practices for CI protection, through a public/private effort;
- establishes a consultative process for improving CI cybersecurity;
- identifies CI with especially high priority for protection, using the consultative process;
- establishes a program with incentives for voluntary adoption of the framework by CI owners and operators;
- reviews cybersecurity regulatory requirements to determine whether they are sufficient and appropriate; and
- incorporates privacy and civil liberties protections in activities under the order.

In addition to codifying the DECS program, the order provides specific responsibilities to DHS and the sector-specific agencies, as well as the Departments of Commerce, Defense, and Justice, the intelligence community, the General Services Administration, and the Office of Management and Budget, addressed below.

[70] Cheryl Pellerin, "DOD Readiness Elements Crucial to Cyber Operations" U.S. Department of Defense, American Forces Press Service, http://www.defense.gov/news/newsarticle.aspx?id=120381.

Presidential Policy Directive 21—Critical Infrastructure Security and Resilience

Along with EO 13636, the White House released Presidential Policy Directive 21 (PPD-21),[71] "Critical Infrastructure Security and Resilience," which addresses the protection of CI. PPD-21 supersedes Homeland Security Presidential Directive 7 (HSPD 7), "Critical Infrastructure Identification, Prioritization, and Protection," released December 17, 2003. PPD-21 seeks to strengthen the security and resilience of CI by

- clarifying functional relationships among federal agencies, including the establishment of separate DHS operational centers for physical and cyber-infrastructure;
- identifying baseline requirements for information sharing;
- applying integration and analysis capabilities in DHS to prioritize and manage risks and impacts, recommend preventive and responsive actions, and support incident management and restoration efforts for CI; and
- organizing research and development (R&D) to enable secure and resilient CI, enhance impact-modeling capabilities, and support strategic DHS guidance.

The directive provides specific responsibilities to DHS and the sector-specific agencies, as well as the Departments of Commerce, Interior, Justice, and State; the intelligence community; the General Services Administration; and the Federal Communications Commission.

National Infrastructure Protection Plan, National Response Framework and Defense Support for Civil Authorities

The National Infrastructure Response Plan (NIPP), developed by DHS with other federal agencies and private sector owners of critical infrastructure, outlines how government and private sector critical infrastructure stakeholders work together to manage risks and achieve security and resiliency. The NIPP 2013 meets the requirements of PPD-21, "Critical Infrastructure and Resilience."

The phrase "defense support of civil authorities" refers to DOD's mission to help civil authorities respond to a domestic emergency or other domestic activity. This support may be provided through the military services, the National Guard, and other DOD resources. For the civil cybersecurity mission, DHS leads the interagency with DOD support. The National Cyber Incident Response Plan outlines roles and responsibilities for coordinating and executing a response to a domestic cyber incident.[72] This plan fits into DHS's National Response Framework, a tiered response guide for local, state, and federal governments with respect to major disasters or emergencies. A 2010 memorandum of agreement between DOD and DHS also guides cooperation between the two entities with respect to securing national cyber assets.[73]

International Authorities

The DOD's role in defense of cyberspace follows the body of laws, strategies, and directives outlined above. For the military to respond to an act of cyberterrorism or cyberwar, a presidential

[71] The White House, "Critical Infrastructure Security and Resilience," *Presidential Policy Directive 21*, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[72] Department of Homeland Security, National Cyber Incident Response Plan, Interim Version, September 2010.

[73] Accessed at https://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

finding must be issued and an order must be executed. However, discussions have been underway in various international fora that may affect how the U.S. government views certain actions in cyberspace and when a military response is warranted. Although the President still decides ultimately what the military will do, the decisions made in the international arena could affect how the Department of Defense organizes, trains, and equips its forces in order to fulfill treaty obligations.

As of yet, no international instruments have been drafted explicitly to regulate inter-state relations in cyberspace. One apparent reason for the absence of such a treaty is that the international governance of cyberspace has largely been the purview of private, professional organizations such as the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN). However, politically motivated cyberattacks are increasingly common and, although difficult to attribute, often raise strong suspicion of government involvement. More importantly, perhaps, states have become targets of cyberattack, provoking a sense of urgency regarding the creation of national strategies and capabilities for cyberdefense and cyberoffense.

The U.S. Position on International Authorities

The Obama Administration has responded to the internationalization of the cyberspace threat environment by releasing in 2011 an *International Strategy for Cyberspace*.[74] The Strategy calls for strengthening bilateral and multilateral government partnerships, and a strong role for the private sector. It does not call for any new treaties or agreements, and the only existing instrument cited is the Budapest Convention (discussed below). It recommends, instead, preservation of the openness that has been a hallmark of the Internet age. This puts the United States at odds with China and Russia, both of which prefer a more nationalistic approach to Internet governance.

In September 2012, the U.S. State Department, for the first time, took a public position on whether cyber activities could constitute a use of force under Article 2(4) of the U.N. Charter and customary international law. According to State's then-legal advisor, Harold Koh, "Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[75] Examples offered in Koh's remarks included triggering a meltdown at a nuclear plant, opening a dam and causing flood damage, and causing airplanes to crash by interfering with air traffic control. By focusing on the ends achieved rather than the means with which they are carried out, this definition of cyberwar fits easily within existing international legal frameworks. If an actor employs a cyber weapon to produce kinetic effects that might warrant fire power under other circumstances, then the use of that cyber weapon rises to the level of the use of force.

However, the United States recognizes that cyberattacks without kinetic effects are also an element of armed conflict under certain circumstances. Koh explained that cyberattacks on information networks in the course of an ongoing armed conflict would be governed by the same principles of proportionality that apply to other actions under the law of armed conflict. These principles include retaliation in response to a cyberattack with a proportional use of kinetic force. In addition, "computer network activities that amount to an armed attack or imminent threat thereof" may trigger a nation's right to self-defense under Article 51 of the U.N. Charter. Here Koh cites the *International Strategy for Cyberspace*, which affirmed that "when warranted, the

[74] The White House, *International Strategy for Cyberspace*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[75] Remarks of Harold Hongju Koh, Legal Advisor U.S. Department of State, at a USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012.

United States will respond to hostile acts in cyberspace as we would to any other threat to our country." The International Strategy goes on to say that the U.S. reserves the right to use all means necessary – diplomatic, informational, military, and economic – as appropriate and consistent with applicable law, and exhausting all options before military force whenever possible.

International Consensus-Building Activities

One of the Defense Objectives of the *International Strategy for Cyberspace* is to work internationally "to 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 national assets." A growing awareness of the threat environment in cyberspace has led to two major international processes geared toward developing international expert consensus international cyber authorities.

First, the threat environment has spurred NATO interest in understanding how existing international law applies to cyberwarfare. A year after the 2007 DDoS attack on Estonia, NATO established the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn, Estonia. The CCDCOE hosts workshops and courses on law and ethics in cyberspace, as well as cyber-defense exercises. In 2009, the center convened an international group of independent experts to draft a manual on the law governing cyberwarfare. The Tallinn Manual, as it is known, was published in 2013. It sets out 95 "black letter rules" governing cyber conflict addressing sovereignty, state responsibility, the law of armed conflict, humanitarian law, and the law of neutrality. The Tallinn Manual is an academic text: although it offers reasonable justifications for the application of international law, it is non-binding and the authors stress that they do not speak for NATO or the CCDCOE.

Second, the cyberspace threat environment has prompted the United Nations to convene Groups of Governmental Experts (GGE) to study "Developments in the Field of Information and Telecommunications in the Context of International Security." The first successful U.N. GGE report came out in 2010, followed by a second report in 2013. The current GGE is expected to reach consensus again in 2015. The stated purpose of this process is to build "cooperation for a peaceful, secure, resilient and open ICT environment" by agreeing upon "norms, rules and principles of responsible behaviour by States" and identifying confidence and capacity-building measures, including for the exchange of information. Unlike the work done at Tallinn under the auspices of NATO, this U.S.-led process includes both China and Russia.

Existing International Instruments That Bear on Cyberwarfare

As previously discussed, the military's role in cyberwarfare is governed by U.S. law. Yet many international instruments bear on cyberwarfare, including those relating to law enforcement (e.g., extradition and mutual legal assistance treaties), defense, and security, along with broad treaties and agreements, such as the United Nations Charter and the Geneva Conventions, as well as international law. Such instruments include, but are not limited to, those described below.

Council of Europe Convention on Cybercrime

This law-enforcement treaty, also known as the Budapest Convention, requires signatories to adopt criminal laws against specified types of activities in cyberspace, to empower law-enforcement agencies to investigate such activities, and to cooperate with other signatories. Those activities include both attacks on the integrity of cyber-systems and content-related crimes such as fraud, pornography, and "hate speech." The convention focuses on identification and

punishment of criminals rather than prevention of cybercrime. Consequently, it may act as a deterrent, but it has no remediating effect on the criminal acts that do occur. Also, the provisions on content may not be consistent with the different approaches of various nations to freedom of expression. While widely cited as the most substantive international agreement relating to cybersecurity, some observers regard it as unsuccessful. [76]

In addition to most members of the Council of Europe, the United States and three other nations have ratified the treaty. [77]

United Nations Resolutions

A series of U.N. General Assembly resolutions relating to cybersecurity have been adopted over the past 15 years. One resolution called for a report from an international group of government experts from 15 nations, including the United States. That 2010 report, sometimes referred to as the Group of Governmental Experts (GGE) Report, recommended a series of steps to "reduce the risk of misperception resulting from ICT[78] disruptions" but did not incorporate any binding agreements.[79] Nevertheless, some observers believe the report represents progress in overcoming differences between the United States and Russia about various aspects of cybersecurity.[80] In December 2001, the General Assembly approved Resolution 56/183, which endorsed the World Summit on the Information Society (WSIS) to discuss on information society opportunities and challenges. This summit was first convened in Geneva, in 2003, and then in Tunis, in 2005, and a10-year follow-on in Geneva in May 2013. Delegates from 175 countries took part in the first summit, where they adopted a Declaration of Principles—a road map for achieving an open information society. The Geneva summit left other, more controversial issues unresolved, including the question of Internet governance and funding. At both summits, proposals for the United States to relinquish control of ICANN were rejected.

Law of War

The so-called "Law of War" embodied in the Geneva and Hague Conventions and the U.N. Charter may in some circumstances apply to cyberattacks, but without attempts by nation states to apply it, or specific agreement on its applicability, its relevance remains unclear. It is also complicated by difficulties in attribution, the potential use of botnets (see the "Malware" section above), and possible harm to third parties from cyber-counterattacks, which may be difficult to contain. In addition, questions of territorial boundaries and what constitutes an armed attack in

[76] Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View" Future Challenges Essay, June 2, 2011, http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf. He cites "vague definitions," reservations by signatories, and loopholes as reasons for its lack of success.

[77] Council of Europe, "Convention on Cybercrime, CETS No. 185," accessed February 18, 2013, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG. See also Michael Vatis, "The Council of Europe Convention on Cybercrime," in Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy (Washington, DC: National Academies Press, 2010), pp. 207–223.

[78] The abbreviation ICT, which stands for information and communications technologies, is increasingly used instead of IT, (information technologies) because of the convergence of telecommunications and computer technology.

[79] United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, July 30, 2010, http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201.

[80] Oona Hathaway et al., "The Law of Cyber-Attack," *California Law Review 100*, no. 4 (2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932.

cyberspace remain. The law's application would appear clearest in situations where a cyberattack causes physical damage, such as disruption of an electric grid. As mentioned above, the Tallinn Manual addresses many of these questions.[81]

International Law on Countermeasures

This body of international law relates to "how states may respond to international law violations that do not rise to the level of an armed attack justifying self-defense." It does not expressly address cyberattacks but presumably would be applicable to them, provided the countermeasures target the responsible nation and are "temporary and instrumentally directed" to induce cessation of the violation.[82] Similar caveats apply to such countermeasures with respect to attribution and effects on innocent parties.

North Atlantic Treaty Organization (NATO)

Since the 2007 attack on Estonia,[83] NATO has established authorities relating to cyberdefense, with the goals of advancing strategy and centralizing defense capabilities across members. A policy on cyberdefense[84] and an associated action plan were adopted in 2011, and the NATO Communications and Information Agency (NCIA) was established in 2012 to facilitate the centralization effort.[85] The NATO Cyber Center of Excellence located in Tallinn, Estonia, is another source of legal analysis.

International Telecommunications Regulations

The International Telecommunication Union (ITU) regulates international telecommunications through binding treaties and regulations and nonbinding standards. Regulations prohibit interference with other nations' communication services and permit control of non-state telecommunications for security purposes. The regulations do not, however, expressly forbid military cyberattacks. Also, ITU apparently has little enforcement authority.[86]

---

[81] For a detailed discussion, see Hathaway et al., "The Law of Cyber-Attack." See also CRS Report RL31787, *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*, by Catherine A. Theohary; James A. Lewis, Conflict and Negotiation in Cyberspace (Center for Strategic and International Studies, February 2013), https://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf; Mary Ellen O'Connell and Louise Arimatsu, Cyber Security and International Law (London, UK: Chatham House, May 29, 2012), http://www.tsa.gov/sites/default/files/assets/pdf/Intermodal/pipeline_sec_incident_recvr_protocol_plan.pdf.

[82] Hathaway et al., "The Law of Cyber-Attack," p. 857.

[83] See CRS Report RL31787, *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*, by Catherine A. Theohary.

[84] The concept document (available at http://www.nato.int/cps/en/natolive/official_texts_68580.htm) states that NATO will "develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyberdefence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations."

[85] North Atlantic Treaty Organization, "NATO and Cyber Defence," February 19, 2013, http://www.nato.int/cps/en/SID-537741AA-89F4BEF4/natolive/topics_78170.htm?.

[86] Hathaway et al., "The Law of Cyber-Attack." See also Anthony Rutkowski, "Public International Law of the International Telecommunication Instruments: Cyber Security Treaty Provisions Since 1850," Info 13, no. 1 (2011): 13–31, http://www.emeraldinsight.com/journals.htm?issn=1463-6697&volume=13&issue=1&articleid=1893240&show=pdf&PHPSESSID=9r0c5maa4spkkd9li78ugbjee3.

Other International Law

Some bodies of international law, especially those relating to aviation and the sea, may be applicable to cybersecurity; for example by prohibiting the disruption of air traffic control or other conduct that might jeopardize aviation safety.[87] Bilaterally, mutual legal assistance treaties between countries may be applicable for cybersecurity forensic investigations and prosecution.

Defense Instruments

The United States has signed 16 treaties and other agreements with 13 other countries and the European Union that include information security, mostly of classified military information, or defense-related information assurance and protection of computer networks. According to news reports, the United States and Australia have agreed to include cybersecurity cooperation within a defense treaty, declaring that a cyberattack on one country would result in retaliation by both.[88]

Other International Organizations

A number of regional associations of nation states have issued declarations of goals and statements of intent relating to cybersecurity, including:

- the G8 Group of States,
- the Asian Pacific Economic Cooperation (APEC),
- the Organization of American States (OAS),
- the Association of South East Asian Nations (ASEAN),
- the Arab League, and
- the Organization for Economic Cooperation and Development (OECD).

However, none of the documents issued by these organizations appear to be binding in effect.[89]

SCO-Proposed International Code of Conduct for Information Security

In September 2011, members of the Shanghai Cooperation Organization, including Russia and China, submitted a proposed voluntary code of conduct for cybersecurity and requested that it be placed on the U.N. General Assembly agenda.[90] Its focus on the rights of governments, such as "reaffirming that policy authority for Internet-related public issues is the sovereign right of States," among other concerns, led to resistance from the United States and other countries.[91]

---

[87] Hathaway et al., "The Law of Cyber-Attack."

[88] See, for example, Lolita Baldor, "Cyber Security Added to US-Australia Treaty," Security on NBCNews.com, 2011, http://www.msnbc.msn.com/id/44527648/ns/technology_and_science-security/t/cyber-security-added-us-australia-treaty/.

[89] For summaries, see International Telecommunication Union, Global Cybersecurity Agenda (GCA): *Global Strategic Report,* 2008, http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf.

[90] Ministry of Foreign Affairs of the People's Republic of China, "China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations," September 13, 2011, http://www.fmprc.gov.cn/eng/zxxx/t858978.htm.

[91] Among the concerns cited were the absence of provisions on international law enforcement and combating cyberespionage; its call for international cooperation relating to "curbing dissemination of information" relating to "political, economic, and social stability" and "spiritual and cultural environment"; and ambiguity with respect to censorship policy (Jeffrey Carr, "4 Problems with China and Russia's International Code of Conduct for Information

OSCE Early Warning Resolution

Under the auspices of the Organization for Security and Cooperation in Europe (OSCE), in 2011 and 2012, the United States, Russia, and other countries negotiated a possible agreement that would warn parties early on when cyber-operations might lead to unintentional conflict, but they were unable to reach consensus on the resolution.[92] Although some observers have expressed interest in such an agreement, others doubt its effectiveness, arguing that conflicting interests and the difficulties of attribution, among other problems, make it unfeasible.[93]

ITU Dubai Summit

The ITU convened the World Conference on International Telecommunications (WCIT) in Dubai, United Arab Emirates, during December 3-14, 2012, to review the International Telecommunications Regulations. In the run-up to the summit, many security observers expressed concern over the closed nature of the talks and feared a shift of Internet control away from private entities such as ICANN toward the U.N. and national governments. Although these concerns proved to be largely baseless, a controversial deep packet inspection proposal from the People's Republic of China was adopted at the summit.[94] Dissenting countries, including Germany, fear that this recommendation will result in accelerated Internet censorship in repressed nations.

Issues for Congress

Authorities: Is Current Law Enough?

Does the military have the authorities it needs to effectively fight and win wars in cyberspace? Some have argued that to fulfill its homeland defense mission, USCYBERCOM should be given increased authority over private sector critical infrastructure protection. Yet business owners, particularly in the IT sector, contend that this would represent a "militarization of cyberspace" that would create distrust among consumers and shareholders, and could potentially stifle innovation, leading to decreases in profits. Others argue that the military's role is to fight and win wars, rather than to bolster a private company's cyber defenses.

As discussed, the international community must contend with a certain amount of ambiguity regarding what constitutes an "armed attack" attack in cyberspace and what the thresholds are for cyberattack as an act of war, an incident of national significance, or both. Without clear redlines and specific consequences articulated, deterrence strategies may be incomplete. On the other hand, a lack of redlines and consequences could constitute a form of strategic ambiguity that gives the U.S. military operational maneuverability. Congress may wish to consider these concerns as new legislation regarding critical infrastructure protection is proposed.

Security," *Digital Dao*, September 22, 2011, http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html).

[92] Aliya Sternstein, "U.S., Russia, Other Nations Near Agreement on Cyber Early-Warning Pact," *Nextgov: Cybersecurity*, December 5, 2012, http://www.nextgov.com/cybersecurity/2012/12/us-russia-other-nations-near-agreement-cyber-early-warning-pact/59977/; Aliya Sternstein, "Cyber Early Warning Deal Collapses After Russia Balks," *Nextgov: Cybersecurity*, December 7, 2012, http://www.nextgov.com/cybersecurity/2012/12/cyber-early-warning-deal-collapses-after-russia-balks/60035/.

[93] Goldsmith, "Cybersecurity Treaties: A Skeptical View."

[94] Deep packet inspection allows the content of a unit of data to be examined as it travels through an inspection point, a process which enables data mining and eavesdropping programs.

Skilled cyber operators are in demand in the military, and the national supply of cyber professionals tends to reside in the private sector. Some of the services are looking at bolstering opportunities for officers who wish to pursue careers in cybersecurity by creating new occupational specialties and career tracks. Yet barriers to hiring skilled civilians for the DOD cyber mission may hinder the development of a robust workforce. Congress may choose to consider ways to incentivize and bolster recruitment of talent outside of the military, such as providing special hiring authorities for certain mission critical positions, streamlining or revising the clearance process for national security personnel, and compensation comparable to private sector equivalent jobs.

How Do DOD and Cyber Command Responsibilities for Cybersecurity Fit Within the Interagency and Private Sector?

Reports have described the USCYBERCOM cyber force's "National Mission Teams" as protecting the networks that undergird critical infrastructure. Given that the majority of this critical infrastructure resides in the private sector, for which DHS has coordinating authority, how do USCYBERCOM teams protect these assets during peacetime without violating *Posse Comitatus*, the prohibition against using the military for domestic policing? How do these national teams interact and coordinate with DHS?

Should U.S. Cyber Command Be Its Own Unified Combatant Command?

The Unified Command Plan organizes combatant commands into geographic and functional areas. U.S. Cyber Command is currently organized under the functional Strategic Command, and co-directed and located with the National Security Agency (NSA). With the complicated lines of authority (Title 10 vs. Title 50) associated with this structure, some have suggested separating the two organizations and giving civilian control to the NSA while elevating Cyber Command to the level of a full unified combatant command. DOD has been tasked by Congress to study and report on the possible implications of this realignment. Specifically, The National Defense Authorization Act for Fiscal Year 2013 (P.L. 112-239) asks in Section 940 "how a single individual could serve as a commander of a combatant command that conducts overt, though clandestine, cyber operations under Title 10, United States Code, and serve as the head of an element of the intelligence community that conducts covert cyber operations under the National Security Act of 1947."

Is a Separate Cyber Force Necessary?

Given that the DOD views cyberspace as one of five global domains, some proponents in Congress contend that a separate cyber force, akin to the Army, Navy, Air Force, or Marine Corps, is necessary to properly address the military aspects of the domain. However, critics point to the multi-layered aspect of cyberspace in which all services have equities.

What Are the Authorizing and Oversight Committees and Jurisdictional Implications?

As previously discussed, blurred lines between operations undertaken under Title 10 and Title 50 authorities can complicate efforts to determine the chain of command and jurisdictional review process. What does this ambiguity mean for congressional oversight committees? Have some

operations taken place without congressional notification? What has been the Department of Defense's role in responding to cyberattacks on private networks?

Current Legislation

The National Defense Authorization Act for Fiscal Year 2015 (P.L. 113-291) contains some provisions related to DOD cybersecurity and cyber operations. These provisions:

- require reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors.
- require the Principal Cyber Advisor to identify improvements to ensure sufficient civilian workforce to support USCYBERCOM and components.
- direct a program of decryption to inspect content for threats and insider activity within DOD networks.
- state the Sense of Congress that as ICANN turns to global community for leadership, support should be given only if assurances are provided for current legacy IP numbers used by DOD and the U.S. government.
- direct that a new mission forces, training, manning and equipping plan and associated programmatic elements be submitted to Congress.
- state a Sense of Congress for consideration regarding role of reserve components in defense against cyberattacks given their unique experience in private and public sectors and existing relationships with local and civil authorities for emergency response.

Appendix. Timeline of International Attacks[95]

February-June 1999: Kosovo was the arena for the first large-scale Internet war, involving pro-Serbian forces cyberattacking the North Atlantic Treaty Organization (NATO). As NATO planes bombed Serbia, pro-Serbian hacker groups, such as the "Black Hand," attacked NATO, U.S., and UK Internet infrastructure and computers via DoS attacks and virus-infected email. In the United States, the White House website was defaced. The UK admitted to losing database information. At NATO Headquarters in Belgium, a public affairs website for the war in Kosovo was "virtually inoperable for several days." Simultaneously, NATO's email server was flooded and choked with email.[96] During the Kosovo conflict, a NATO jet bombed the Chinese embassy in Belgrade in May 1999. The Chinese Red Hacker Alliance retaliated by launching thousands of cyberattacks against U.S. government websites. [97]

October 2000: Riots in the Palestinian territories sparked rounds of cyberattacks between Israelis and Palestinians. Pro-Israeli attacks targeted the official websites of the Palestinian Authority, Hamas, and the government of Iran. Pro-Palestinian hackers retaliated against Israeli political, military, telecommunications, media, the financial sector, commercial, and university websites. Since 2000, the Middle East cyberwar has kept pace with the ground conflict.[98]

April-May 2007: DDoS attacks shutdown websites of Estonia's parliament, banks, ministries, newspapers, and broadcasters. Estonian officials accused the Russian government of responding to their decision to move a Soviet-era war memorial with retaliatory cyberattacks.[99]

September 2007: Israel disrupted Syrian air defense networks during the bombing of an alleged nuclear facility in Syria.[100]

July 2008: Government and corporate websites in Lithuania were defaced. The Soviet-themed graffiti implicated Russian nationalist hackers.[101]

August 2008: Georgian government and commercial websites were shut down by DoS attacks at the same time that Russian ground troops invaded the country.[102]

---

[95] Unless otherwise noted, these events are cited in "Significant Cyber Events" Washington, DC: Center for Strategic and International Studies, http://csis.org/program/significant-cyber-events; accessed August 7, 2014.

[96] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," keynote speech, Japan, 2008, http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf.

[97] Jeffrey Carr, "Real Cyber Warfare: Carr's Top Five Picks," *Forbes*, February 4, 2011, http://www.forbes.com/sites/jeffreycarr/2011/02/04/real-cyber-warfare-carrs-top-five-picks/; Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," keynote speech, Japan, 2008, http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf.

[98] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," keynote speech, Japan, 2008, http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf.

[99] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[100] "Significant Cyber Events" Washington, DC: Center for Strategic and International Studies, http://csis.org/program/significant-cyber-events; accessed August 7, 2014.

[101] Brian Krebs, "Lithuania Weathers Cyberattack, Braces for Round 2," *The Washington Post*, July 3, 2008, http://voices.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html.

[102] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

January 2009: DoS attacks originating in Russia shut down Kyrgyzstan's two main Internet servers on the same day that the Russian government pressured Kyrgyzstan to bar U.S. access to a local airbase.[103]

July 2009: Servers in South Korea and the United States sustained a series of attacks, reportedly by North Korea.[104]

June 2010: "Stuxnet" worm damaged an Iranian nuclear facility. The United States and Israel were implicated in the attack.[105]

September 2011: "Keylogger" malware was found on ground control stations for U.S. Air Force unmanned aerial vehicles (UAVs) and reportedly infected both classified and unclassified networks at Creech Air Force Base in Nevada.

May 2012: An espionage worm called "Flame," allegedly 20 times more complex than Stuxnet, was discovered on computers in the Iranian Oil Ministry, as well as in Israel, Syria, and Sudan.

August 2012: "Gauss" worm infected 2,500 systems worldwide. The malware appeared to have been aimed at Lebanese banks, and contained code whose encryption has not yet been broken.

August 2012: The "Cutting Sword of Justice," a group reportedly linked to the government of Iran, used the "Shamoon" virus to attack major oil companies including Aramco, a major Saudi oil supplier, and the Qatari company RasGas, a major liquefied natural gas (LNG) supplier. The attack on Aramco deleted data on 30,000 computers and infected (without causing damage) control systems.

September 2012-June 2013: The hacker group Izz ad-Din al-Qassam launched DoS attacks against major U.S. financial institutions in "Operation Ababil." Izz ad-Din al-Qassam is believed to have links to Iran and Hamas.

January 2013: The *New York Times*, *Wall Street Journal*, *Washington Post*, and *Bloomberg News* revealed that they were targeted by persistent cyberattacks. China was the suspected source.

May 2013: Israeli officials reported a failed attempt by the Syrian Electronic Army to compromise water supply to the city of Haifa.

August 2013: Leaks revealed that the U.S. government purportedly conducted 231 cyber intrusions in 2011 against Russia, China, North Korea, and Iran. Most of the intrusions were related to nuclear proliferation.

April 2014: The disclosure of the Heartbleed bug revealed vulnerability in the OpenSSL protocol previously considered the standard for Internet security. Canada reported more than 900 compromised social security numbers.[106]

---

[103] Daniel McLaughlin, "Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites" (*Irish Times*, July 2, 2008) p. 10, http://lumen.cgsccarl.com/login?url=http://proquest.umi.com/pqdweb?did=1503762091&sid=2&Fmt=3&clientld=5094&RQT=309&VName=PQD.

[104] "Significant Cyber Events" Washington, DC: Center for Strategic and International Studies, http://csis.org/program/significant-cyber-events; accessed August 7, 2014.

[105] Ralph Langer, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," November, 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

[106] http://heartbleed.com/; "OpenSSL Heartbleed Vulnerability" Cyber Security Bulletins. Public Safety Canada. April 11, 2014, retrieved April 14, 2014. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser.

May 2014: The United States indicted five Chinese military officers on charges of computer hacking, economic espionage, and other offenses against six targets in the United States' nuclear power, metals, and solar power industries. China has denied the charges.[107] According to U.S. Attorney General Eric Holder, "This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking."[108]

July 2014: The United States charged a Chinese entrepreneur with breaking into the computer systems of the U.S. defense giant Boeing and other firms to steal data on military programs concerning warplanes, including C-17 cargo aircraft, and the F-22 and F-35 fighter jets.[109] At the same time, the security firm Kapersky reported a massive cyber operation dubbed "Energetic Bear," which targeted more than 2,800 industrial firms around the globe. Although some reports identified a Russian hacker group as the source, Kapersky refrained from attributing the attack to any one country.[110]

December 2014: U.S. cybersecurity firm Cylance reported that an Iranian hacker group has breached airlines, energy and defense firms, and the U.S. Marine Corps intranet in an attack known as "Operation Cleaver."[111]

Author Information

Catherine A. Theohary
Specialist in National Security Policy, Cyber and
Information Operations

Acknowledgments

Anne I. Harrington, APSA Congressional Fellow, contributed to this report.

Disclaimer

[107] Song Sang-ho, "Concerns rise over militarization of cyberspace," *The Korean Herald*, July 13, 2014, http://www.koreaherald.com/view.php?ud=20140713000188.

[108] Office of Public Affairs, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, Department of Justice, May 19, 2014, http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

[109] Dan Levine, "US Charges Chinese Man with Hacking into Boeing," *Reuters*, July 11, 2014, http://www.reuters.com/article/2014/07/11/boeing-china-cybercrime-idUSL2N0PM2FV20140711.; Song Sang-ho, "Concerns rise over militarization of cyberspace," *The Korean Herald*, July 13, 2014, http://www.koreaherald.com/view.php?ud=20140713000188.

[110] See http://www.darkreading.com/attacks-breaches/energetic-bear-under-the-microscope/d/d-id/1297712.

[111] See http://www.defensenews.com/article/20141202/DEFREG04/312020030/Report-Iran-Hackers-Infiltrated-Airlines-Energy-Defense-Firms.