Homeland Security v. Homeland Defense: Gaps Galore

By Jody R. Westby[1]

Paper for St. Mary's University School of Law, Center for Terrorism Law
State Open Government Law and Practice in a Post-9/11 World:
Legal and Policy Analysis
November 15-16, 2007
National Press Club
Washington, DC

Introduction

Since the formation of the President's Commission on Critical Infrastructure Protection in 1996, significant work has been undertaken by U.S. agencies and departments and state and local governments with respect to the protection of critical infrastructure (CI) and public-private sector coordination in the event of a cyber attack. The associated legal and policy issues have also been reviewed and actions have been taken to ensure an appropriate legal framework is in place to support Homeland Security response measures.[2] *Little has been done, however, with respect to (a) public-private sector response coordination in a cyber warfare context, and (b) the development of domestic and international legal and policy frameworks to support such responses*. Thus, there are significant preparedness gaps between the Homeland Security capabilities exercised by infrastructure owners and local, state, and federal responders and the Homeland Defense capabilities required from the U.S. military and other nation states. It is precisely these Homeland Defense gaps that leave America most vulnerable. In the post-9/11 world, responses to major cyber attacks will require (a) enormous interaction and cooperation

---

[1] Jody R. Westby is CEO of Global Cyber Risk LLC in Washington, D.C. and serves as Adjunct Distinguished Fellow to Carnegie Mellon CyLab. She chairs the American Bar Association's Privacy & Computer Crime Committee (Section of Science & Technology Law) and is a member of the World Federation of Scientists' Permanent Monitoring Panel on Information Security. She represents the ABA on the National Conference of Lawyers and Scientists.

[2] *See e.g., Adequacy of Criminal Law and Procedure (Cyber): A Legal Foundations Study*, President's Commission on Critical Infrastructure Protection, 1997, http://chnm.gmu.edu/cipdigitalarchive/object.php?id=184; *Approaches to Cyber Intrusion Response: A Legal Foundations Study*, 1997, President's Commission on Critical Infrastructure Protection, 1997, http://chnm.gmu.edu/cipdigitalarchive/object.php?id=190; *Federal Government Model Performance: A Legal Foundations Study,* President's Commission on Critical Infrastructure Protection, 1997, http://chnm.gmu.edu/cipdigitalarchive/object.php?id=189; *Legal Authorities Database: A Legal Foundations Study,* President's Commission on Critical Infrastructure Protection, 1997, http://chnm.gmu.edu/cipdigitalarchive/object.php?id=181; *Legal Foundations, Studies and Conclusions: A Legal Foundations Study,* President's Commission on Critical Infrastructure Protection, 1997, http://chnm.gmu.edu/cipdigitalarchive/object.php?id=167; *Legal Impediments to Information Sharing: A Legal Foundations Study,* President's Commission on Critical Infrastructure Protection, 1997, http://chnm.gmu.edu/cipdigitalarchive/object.php?id=188; *Liability and Insurance: Infrastructure Assurance,* President's Commission on Critical Infrastructure Protection, 1997, http://chnm.gmu.edu/cipdigitalarchive/object.php?id=168; *Major Federal Legislation: A Legal Foundations Study,* President's Commission on Critical Infrastructure Protection, 1997, http://chnm.gmu.edu/cipdigitalarchive/object.php?id=179; Ethan B. Kapstein, *Regulating the Internet*, President's Commission on Critical Infrastructure Protection, 1997, http://chnm.gmu.edu/cipdigitalarchive/object.php?id=170.

between the public and private sectors, (b) clear legal authority for actions taken by the U.S. military and any collective assistance from other nation states, and (c) authorization from private sector boards of directors and senior management regarding the use of private sector networks in offensive and defensive actions.

Definitions and context are important when discussing Homeland Security, Homeland Defense, and critical infrastructure protection, and when analyzing the legal instruments that govern potential responses by nation states to cyber attacks. For purposes of this paper, "Homeland Security" is defined as "A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[3] "Homeland Defense" is defined as "[t]he protection of United States territory, sovereignty, domestic population and critical infrastructure through deterrence of and defense against direct attacks as well as the management of the consequences of such attacks."[4] Section 2 of the U.S. Homeland Security Act defines "critical infrastructure" as having the same meaning as that used in the USA PATRIOT Act:

> [T]he term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the …[nation] 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.[5]

The Threat

The threat of cyber warfare is not new. In fact, the U.S. Government has exercised cyber warfare tactics probably more than any other nation. Two excellent examples of U.S. cyberwar tactics are Operation Desert Storm and a successful CIA plot to disrupt Soviet pipelines. In 1982, President Reagan approved a plan to transfer software used to run pipeline pumps, turbines, and valves to the Soviet Union that had embedded features designed to cause pump speeds and valve settings to malfunction. "The result was the most monumental non-nuclear explosion and fire ever seen from space," noted former Air Force Secretary Thomas C. Reed in his book, *At the Abyss: An Insider's History of the Cold War.*"[6] The attack caused enormous economic and psychological impact to the Soviet Union and is credited with helping to end the Cold War.[7] The U.S. deployed cyber warfare tactics again when it invaded Iraq in 1991. Phase I of Operation Desert Storm was a strategic air campaign that would "attack Iraq's strategic air defenses; aircraft/airfields; …command and control systems; … telecommunications facilities; and key elements of the national infrastructure, such as critical … electric grids…."[8] The U.S.

---

[3] *National Strategy for Homeland Security,* Office of Homeland Security, July 2002 at 2, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.
[4] General Military Training – Homeland Defense, https://www.cnet.navy.mil/cnet/gmt/gmt03/1_5.pdf.
[5] Homeland Security Act of 2002, Pub. Law 107-296, Section 2, http://whitehouse.gov/deptofhomeland/bill. The USA PATRIOT Act is an acronym for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.
[6] David E. Hoffman, "CIA slipped bugs to Soviets," *Washington Post,* Feb. 27, 2004, http://www.msnbc.msn.com/id/4394002.
[7] *Id.*
[8] *Operation Desert Storm: Evaluation of the Air Campaign,* U.S. Government Accountability Office, Letter Report, GAO/NSIAD-97-134, June 12, 1997 at Appendix V, http://www.fas.org/man/gao/nsiad97134/app_05.htm.

also used its extensive communication and satellite systems to support its Desert Storm activities.[9]

The U.S. is not alone in developing cyber warfare tactics and strategies. As early as 1996, U.S. Government officials estimated that more than 120 countries either had or were developing computer attack capabilities that could enable them to take over the Department of Defense's (DoD) information systems and "seriously degrade the nation's ability to deploy and sustain military forces."[10] Considering that today over one billion online users[11] and 233 countries are connected to the Internet,[12] the number of countries with such capabilities is likely higher.

China has long been considered one of the more aggressive countries focusing on cyber warfare capabilities, but speculation in this area was clarified when *Xinhua* published the full text of China's *National Defense in 2006*. In this document, China declared its goal of "building informationized armed forces and being capable of winning informationized wars by the mid-21st century."[13] The U.S.-China Economic and Security Review Commission (USCC) noted in its 2006 annual report to Congress that:

> Chinese military strategists write openly about exploiting the vulnerabilities created by the U.S. military's reliance on advanced technologies and an extensive C4ISR infrastructure it uses to conduct operations. China's approach to exploiting the technological vulnerabilities of adversaries extends beyond destroying or crippling military targets. Chinese military writings refer to attacking key civilian targets such as financial systems….According to the Department of Defense, the PLA's [People's Liberation Army] cyber-warfare strategy has evolved from defending its own computer networks to attacking the networks of its adversaries and limiting their ability to obtain and process information….Such attacks would be intended to disable defense systems that facilitate command and control and intelligence communication and the delivery of precision weapons, primary instruments for the conduct of modern U.S. warfare.[14]

---

[9] Jon Trux, "Desert Storm: A space-age war," *NewScientist,* July 27, 1991, http://www.newscientist.com/article/mg13117794.900-desert-storm-a-spaceage-war--one-year-ago-next-week-iraqinvaded-kuwait-provoking-a-war-with-the-us-and-its-allies-but-withoutanarmada-of-snooping-satellites-iraqs-battle-was-lost-almost-before-it-began.html.

[10] *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,* United States Gov't. Accountability Office, GAO/AIMD-96-84, May 22, 1996, http://www.fas.org/irp/gao/aim96084.htm.

[11] "Internet Usage Statistics – The Big Picture: World Internet Users and Population Stats," Internet World Stats, http://internetworldstats.com/stats.htm (hereinafter "Internet Usage Statistics").

[12] "Internet World Stats: Usage and Populations Statistics," http://www.internetworldstats.com/.

[13] "China's National Defense in 2006," *Xinhua,* Dec, 29, 2006 at 5, http://news.xinhuanet.com/english/2006-12/29/content_5547029.htm.

[14] *2006 Report to Congress of the U.S.-China Economic and Security Review Commission*, Nov. 2006 at 137, http://www.uscc.gov/annual_report/2006/06_annual_report_contents.php. C4ISR is an acronym for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

The USCC's 2007 report to Congress expanded on its earlier warnings by noting that a Chinese cyber attack might go beyond government systems and target U.S. financial, economic, energy, and communications infrastructure.[15]

In June 2007, Pentagon computer networks were allegedly hacked by the Chinese military in what has been called "the most successful cyber attack on the U.S. defense department,"[16] shutting down parts of the Pentagon's systems for more than a week.[17] Chinese hackers have also been blamed for attacks that compromised German government systems and cyber espionage incidents against the United Kingdom's (UK) government systems.[18] The Director-General of the UK's counter-intelligence and security agency, MI5, recently posted a confidential letter to 300 CEOs and security officers on the website of the Centre for the Protection of National Infrastructure, warning them that their infrastructure was being targeted by "Chinese state organizations" and that the attacks were designed to defeat security best practices.[19]

Cyber threats do not emanate solely from nation states, however. Government officials have repeatedly warned that terrorists or other rogue actors have the capability to attack critical infrastructure and cause catastrophic consequences. Analysis of the use of the Internet and information and communication technologies (ICTs) by terrorists confirms their interest in and ability to use these technologies for asymmetric attacks. For example, after September 11, the U.S. Federal Bureau of Investigation (FBI) discovered that online users, whose activity was routed through switches in Saudi Arabia, Pakistan, and Indonesia, were exploring the digital systems of emergency telephone, electrical generation and transmission, water storage and distribution, nuclear power plants, and gas facilities.[20] Computers seized in Pakistan in July 2005 contained material from "casings" of key financial institutions located in New York, Washington, D.C., and Newark, New Jersey, prompting Homeland Security alerts to these organizations and locales.[21]

The Need for Response Coordination

Cyber response capabilities must be closely coordinated because, at the time of a cyber attack, it is not possible to immediately determine whether the attacker is a script kiddie, an insider, a rogue actor (organized crime, terrorist organization, or radical), or a nation state. Therefore, the "response baton" may have to be passed from the private sector to law enforcement to the

---

[15] *2007 Report to Congress of the U.S.-China Economic and Security Review Commission*, June 1, 2007 at 8, http://www.uscc.gov/annual_report/2007/annual_report_full_07.pdf.
[16] Demetri Sevastopulo, "China 'hacked' into Pentagon defence system," *Financial Times,* Sept. 6, 2007 at 1.
[17] Demetri Sevastopulo, "Real security fear over virtual invasions," *Financial Times,* Sept. 4, 2007 at 2.
[18] "China's cyber-spies spread their net," *Financial Times,* Sept. 4, 2007 at 12; Andrew Ward and Demetri Sevastopulo, "US concedes danger of cyber-attack," *Financial Times,* Sept. 6, 2007 at 3.
[19] Rhys Blakely, "MI5 alert on China's cyberspace spy threat," *Times Online,* Dec. 1, 2007, http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece.
[20] Jody R. Westby, "Countering Terrorism with Cyber Security," *Jurimetrics,* Vol. 47, No. 3, Spring 2007 at 297, 306-307, http://lawlib.wlu.edu/CLJC/index.aspx?mainid=163&issuedate=2007-09-12&homepage=no (hereinafter "Westby") (citing Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*, June 26, 2002, http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26).
[21] Westby at 306-307 (citing "Al-Qaeda surveillance techniques detailed," *USA Today,* Dec. 29, 2004, http://www.usatoday.com/news/washington/2004-12-29-terror-surveillance_x.htm).

military with swift, efficient coordination and certainty regarding legal authority for actions taken.

It is imperative that cyber response capabilities be analyzed from the perspective of cyber warfare and/or attacks from terrorists, including public-private sector coordination and the information sharing that will be required to shift from local responders to military involvement. Unlike traditional defense categories (i.e., land, air, and sea), the military capabilities required to respond to an attack on U.S. infrastructure will necessarily involve infrastructure owned and operated by the private sector. Indeed, 85 percent of CI in the U.S. is owned by the private sector.[22] What is more, the Department of Defense (DoD) is critically dependent upon these infrastructures, both domestically and globally, to support its operations. A 1995 research report to the Joint Chiefs of Staff noted that, "Over 95 percent of the worldwide telecommunications needs of the Department of Defense (DoD) are satisfied by commercial telecommunications carriers."[23] Thus, the very networks that support DoD operations and network-centric warfare capabilities – including defensive and offensive cyber capabilities – are not under the direct control of DoD and require private sector involvement for offensive and defensive capabilities.

The military has long embraced the concept of information operations and has developed extensive materials in the area of cyber warfare.[24] In 2005, the Joint Functional Component Command for Network Warfare (JFCCNW) was established to "facilitate cooperative engagement with other national entities in computer network defense and offensive information warfare."[25] The JFCCNW is headed by the director of the National Security Agency (NSA), presently Lt. General Keith B. Alexander, but it is a component of the United States Strategic Command (STRATCOM), which coordinates offensive computer network operations for DoD.[26] The establishment of the JFCCNW is a critical step toward creating a formal cyber defense category and response capability.

Since its establishment, however, the JFCCNW has done little to reach out to the private sector to plan their involvement – and the use of their networks – in the cyberwar offensive and defensive actions. The deployment of military weapons is traditionally under the complete control of the U.S. President as Commander and Chief of the Armed Forces and the Department of Defense. *Perhaps the notion that a cyber defense category and response capability involves*

---

[22] *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics,* Government Accountability Office, GAO-07-39, Oct. 2006 at 1, http://www.gao.gov/new.items/d0739.pdf.

[23] Science Applications International Corp., *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance,* A Research Report for the: Chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon, Washington, D.C. July 4, 1995 at 1-1, http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA316285&Location=U2&doc=GetTRDoc.pdf.

[24] *See, e.g.,* Cyberspace & Information Operations Study Center, Air University, U.S. Air Force, http://www.au.af.mil/info-ops/; Naval Information Warfare Activity, http://www.fas.org/irp/agency/navsecgru/niwa/; U.S. Army Training and Doctrine Command, *Concept for Information Operations*, Aug. 1, 1995, http://www.tradoc.army.mil/tpubs/pams/p525-69.htm.

[25] Statement of Gen. James E. Cartwright, Commander, United States Strategic Command, Before the Strategic Forces Subcommittee on Space Policy, Mar. 16, 2005 at 12, http://www.globalsecurity.org/space/library/congress/2005_h/050316-cartwright.pdf.

[26] Joint Functional Component Command for Network Warfare, http://en.wikipedia.org/wiki/Joint_Functional_Component_Command_for_Network_Warfare.

private sector participation is foreign to military planning, but there is an urgent need for the JFCCNW to engage the private sector in offensive planning and the development of coordinated response capabilities in the event of cyber warfare.

The establishment of a cyber defense category and cyber response capability within DoD can only be effective – and considered within our correlation of forces – if it includes the coordination and cooperation of the private sector that owns and operates the very networks at risk and which would be used to launch an attack or counter-attack.

Quite simply, effective cyber actions require open channels of communication between the military and critical infrastructure owners, with scenarios and interactions well thought-out and rehearsed. These actions are a giant step beyond the Homeland Security efforts voluntarily undertaken by U.S. companies on an industry-sector basis to develop CI plans and establish information sharing and analysis centers (ISACs). This work has been undertaken in concert with a Government department or agency as the industry sector's public sector counterpart, as designated by Homeland Security Presidential Directive # 7 (HSPD-7). HSPD-7 instructs each Government Sector-Specific Agency to "collaborate with … the private sector, including key persons and entities in their infrastructure sector."[27] HSPD-7 designates DoD as the Sector-Specific Agency (SSA) [28]for the defense industrial base (DIB).

HSPD-7 is implemented in DoD through Department of Defense Directive 3020.40 (DD 3020.40), which incorporates the collaboration requirement in the Directive's Purpose. DD3020.40 defines Defense Critical Infrastructure as "DoD and non-DoD networked assets essential to project, support, and sustain military forces and operations worldwide."[29] DD3020.40 defines the Defense Industrial Base (DIB) Defense Sector as "The Department of Defense, the U.S. Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.[30] Notably, this definition excludes the private sector entities that DoD would have to rely upon for cyber warfare offensive and defensive actions. In fact, the *Defense Industrial Base Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan* specifically notes that:

> The DIB *does not* include commercial infrastructure that provides, for example, power, communications, transportation, and other utilities that DoD warfighters and support organizations use to meet their respective operational needs. Those commercial infrastructures are addressed by the other SSAs and through dependency analysis.[31]

---

[27] Homeland Security Presidential Directive / HSPD-7, "Critical Infrastructure Identification, Prioritization, and Protection, Dec. 17, 2003 at 4, http://www.fas.org/irp/offdocs/nspd/hspd-7.html.

[28] *Defense Industrial Base Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan,* U.S. Department of Defense, May 2007 at 5, http://www.dhs.gov/xlibrary/assets/DIB_SSP_5_21_07.pdf (hereinafter "DIB Plan").

[29] Department of Defense Directive, "Defense Critical Infrastructure Program (DCIP)", No. 3020.40, Aug. 19, 2005 at 2, http://www.fas.org/irp/doddir/dod/d3020_40.pdf.

[30] *Id.* at 11.

[31] DIB at 5, http://www.dhs.gov/xlibrary/assets/DIB_SSP_5_21_07.pdf (emphasis added).

To date, DoD's interactions with the private sector have largely been limited to working with defense industrial base companies to secure their information technology systems to protect information regarding U.S. weapons systems and DoD data. Efforts to work more broadly with the private sector on defining roles and responsibilities in cyber warfare offensive and defensive situations have not occurred, yet somehow DoD conveys the message that the U.S. is prepared for such actions.

General Cartwright, former commander of STRATCOM, aroused attention in his March 21, 2007 testimony before the House Armed Services Subcommittee by declaring that the best defense to cyber attacks against U.S. military, civilian, and commercial networks was a good offense:

> [If] we apply the principle of warfare to the cyber domain, as we do to sea, air and land, we realize the defense of the nation is better served by capabilities enabling us to take the fight to our adversaries, when necessary, to deter actions detrimental to our interests.[32]

The General's comments are unhinged from the reality of private sector ownership of the critical infrastructure that must be used to launch an offensive attack and DoD's lack of interactions with the private sector on planning such attacks. *Indeed, with the exception of historic interactions with the communications sector through the National Communications Coordinating Center and the National Security Telecommunications Advisory Committee, DoD and the JFCCNW has not reached out to private sector entities to plan and coordinate cyber offensive and defensive actions.* Likewise, although CI owners have developed sector-specific plans for CI protection, they have not (a) adequately examined their role in responding to cyber warfare attacks on their infrastructure, (b) analyzed the legal considerations and risks that may be involved, and (c) developed response plans that involve coordination with the U.S. military and the involvement of their own personnel. In addition, neither the Government nor CI owners have adequately examined the interdependencies in critical infrastructure to begin developing response plans that support more than their own CI.

This gap between Homeland Security and Homeland Defense preparedness planning must be addressed immediately if the U.S. is to keep pace with the cyber warfare activities of other nation states and rogue actors and effectively execute offensive attacks and manage defensive response capabilities. The recent attacks on government and private sector networks in Estonia demonstrate the rapid pace at which a cyber attack can escalate to a national security issue, involve other nation states, and raise the issue of collective defense. The Estonian attacks may also represent a situation in which rogue actors are aligned with a nation state in conducting and concealing such attacks, though this has not been proven. Serious cyber attacks, such as those directed at Estonia, cannot be countered by any private sector company; government assistance is necessary. These situations rapidly escalate beyond the capabilities of law enforcement, CERTs, and ISACs and military and cyber warfare expertise is required.

---

[32] Bob Brewin, "Cybersecurity defense requires a good offense," *FCW.com,* Mar. 22, 2007, http://www.fcw.com/online/news/98016-1.html

The attacks against Estonian government and private sector systems began April 26, 2007 and continued for several weeks. They involved hacking, web defacement, and sustained denial of service attacks that were amplified by the use of a large network of bots.[33] The attacks began after Estonian officials took down a popular bronze statue of a World War II Soviet soldier. They started with a flood of spam messages that eventually shut down the Estonian Parliament's email system. In another attack, hackers broke into the web site of the Reform Party and posted a phony letter from Estonia's prime minister apologizing for removing the statue. The attacks quickly escalated into what Estonia's defense minister called "a national security situation," seriously impacting government web sites and systems and shutting down newspaper and financial networks.[34] The Estonian government was forced to close large parts of the country's network to outside traffic as it attempted to gain control of the situation. Estonia blames the attacks on Russia and claims that it has tracked some communications to an Internet address belonging to a Kremlin official.[35] Notably, Russia refused to cooperate in the investigation of the attacks even though it strongly denied any responsibility for them.[36] "They won't even pick up the phone," complained Rein Lang, Estonia's minister of justice regarding Russia's refusal to help end the attacks or investigate evidence that Russian state employees were behind them.[37]

The head of Estonia's Computer Emergency Response Team (CERT) initially summoned security experts from Estonia's Internet service providers (ISPs), financial institutions, government agencies, and police and called on contacts in other countries to help track and block suspicious Internet addresses and traffic. Before the attacks ended, computer security experts from the U.S., Israel, the European Union (EU), and the North Atlantic Treaty Organization (NATO) were assisting Estonia – and learning its lessons.[38] Traffic involved in the attacks was traced to countries as diverse as the U.S., China, Vietnam, Egypt, and Peru.[39] In a Joint Motion for a Resolution of the European Parliament, Estonia called on the European Commission and the Member States of the EU " to assist in the analyses of the cyber-attacks on Estonian websites and to present a study on how such attacks and threats can be addressed at the EU level…."[40] Linton Wells II, then the principal Deputy Assistant Secretary of Defense for DoD networks and information integration, commented that, "This [the Estonian attacks] may well turn out to be a watershed in terms of widespread awareness of the vulnerability of modern society."[41]

---

[33] Bots are software robots that are planted in a computer by a hacker without the knowledge of the owner. They can be linked together into networks (called botnets) controlling millions of computers and can be activated remotely to perform automatic tasks, such as sending large packets of information. *See generally*, http://en.wikipedia.org/wiki/Internet_bot.

[34] Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times,* May 29, 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1&pagewanted=print&oref=slogin (hereinafter "Landler and Markoff").

[35] *Id.*

[36] David J. Smith, "Cyber-war!" *24 Saati*, Tblisi, Sept. 25, 2007, http://www.potomacinstitute.org/media/mediaclips/2007/Smith_24Hours_092507.pdf.

[37] Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *Washington Post,* May 19, 2007 at 1, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html (hereinafter "Finn").

[38] Landler and Markoff.

[39] Finn at A14.

[40] Joint Motion for a Resolution, European Parliament, May 23, 2007 at 4, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+P6-RC-2007-0205+0+DOC+PDF+V0//EN.

[41] Landler and Markoff.

Theory falls way to reality in the chaos that follows such crises: neither NATO nor the countries that came to the assistance of Estonia had clear legal authority to engage in defensive measures to aid Estonia. The Estonian attacks highlight the need to revise the doctrines and documents that traditionally support diplomatic, policy, and military decisions so they can accommodate cyber situations. The political and economic shifts caused by the Internet and globalization introduce geo-cyber considerations that impact more fundamental approaches to national security based on geo-political[42] interests and spheres of influence.

Geo-Cyber Considerations

On the heels of World War II, America was faced with a new kind of enemy: the Cold War, socialism, and threats of nuclear strikes. The Air Force became concerned about its ability to maintain command and control operations following a nuclear attack, and they commissioned RAND to do a study on a survivable military network that could provide "minimum essential communications."[43] The RAND work (1962-1965) concluded with a report by Paul Baran describing how a packet switched computer network could provide this capability.[44] The rest is history. In 1971, the ARPANET, as the Internet was first called, had 23 hosts connecting government research centers and universities across the nation. In 1995, NSF turned access to the Internet backbone over to four commercial companies, and, by 1996, there were nearly 10 million hosts online and the Internet spanned the globe. Within three decades, the Internet grew "from a Cold War concept for controlling the tattered remains of a post-nuclear society to the Information Superhighway."[45]

Today, there are no U.S. Government controls or geographical boundaries on the Internet. Policies are determined by the Internet Society (ISOC) and other international bodies.[46] Since the NSF unleashed the Internet in 1995, it has experienced explosive growth, increasing from 50 million users in 1996 to around 1.2 billion today,[47] served by around 490 million hosts around the globe.[48] The negative repercussions to the Internet boom – viruses, worms, trojan horses, bots, network attacks, intrusions, web defacements, economic espionage, and interceptions of data are commonplace – also originate from all over the world, creating new threats and more closely linking national and economic security.

---

[42] Geopolitics is defined as "(1) The study of the relationship among politics and geography, demography, and economics, especially with respect to the foreign policy of a nation, (2) a. A governmental policy employing geopolitics. b. A Nazi doctrine holding that the geographic, economic, and political needs of Germany justified its invasion and seizure of other lands, (3) A combination of geographic and political factors relating to or influencing a nation or region." American Heritage Dictionary, 2000, http://dictionary.reference.com/search?r=2&q=geopolitical.

[43] Dave Krisula, "The History of the Internet," Aug. 2001, http://www.davesite.com/webstation/net-history.shtml (hereinafter "Krisula"); "A Brief History of the Net," *Fortune*, Oct. 9, 2000 at 34; Stewart Brand, "Founding Father," *Wired*, Mar. 2001 at 148 (hereinafter "Brand").

[44] Brand at 145-153; Krisula.

[45] "Life on the Internet: Net Timeline," PBS, http://www.pbs.org/internet/timeline/timeline-txt.html; *see also* Krisula.

[46] *See e.g.*, http://www.isoc.org/isoc/; http://www.wia.org/ISOC/; http://www.iab.org/iab/.

[47] Internet Usage Statistics.

[48] Internet Systems Consortium, "ISC Domain Survey: Number of Internet Hosts," http://www.isc.org/index.pl?/ops/ds/host-count-history.php.

History repeats itself. Today, America once again faces new threats, and our ability to maintain our C4ISR capabilities against attacks from terrorists and nation states has become a national priority. September 11 changed our concept of national security, stood our military strategy on its head, and heightened our sensitivity to vulnerabilities in our critical infrastructure. We are faced with unprecedented asymmetrical challenges to our national and economic security. Although geo-political considerations still must be afforded great weight, threats to our critical infrastructure must be evaluated in a policy paradigm that is based on maintaining geo-cyber security and stability.

The author defines **"geo-cyber"** as the relationship between the Internet and the geography, demography, economy, and politics of a nation and its foreign policy. **"Geo-cyber security"** is defined as the ability to protect the infrastructure, systems, and information of a nation from intrusion, attack, espionage, sabotage, unauthorized access or disclosure, or other forms of negative or criminal activity that could undermine its national and economic security. **"Geo-cyber stability"** is defined as the ability to utilize the Internet for economic, political, and demographic benefit and to influence the policies, laws and regulations governing the Internet, while minimizing the risks and threats to economic and national security. [49]

Today, it is no longer a question of our maintaining "essential minimum communications:" it is a question of how we can maintain geo-cyber security so our critical infrastructure cannot be used as a weapon against us and how we can engage multilaterally to ensure geo-cyber stability. The irony is that the brainchild of the Cold War era now presents one of the most daunting challenges to Homeland Defense – one which we are ill-prepared to meet. Not only is there no planned coordination for offensive and defensive cyber attacks, the legal framework to support such actions is murky at best.

Legal Issues

Numerous legal and policy questions arise in the context of cyber warfare. Consider how the U.S. might launch an offensive attack on China through communications infrastructure. DoD systems are not connected to China, so any attack would necessarily involve private sector networks. Who on the public and private sector sides would have authority to approve military use of private sector networks? What international cooperation would be required? Would the attack have to traverse more than one provider's network? Would allowing the use of the private network for military purposes interfere with the fiduciary duty owed to the company's shareholders by the board of directors and officers to protect company assets and its market value? Who is responsible for damage that could occur to the private sector network as a consequence of the attack or as the result of a counterattack? Can the U.S. Government order a private sector company to let it take over its network for national security interests? What third party liability may arise as a result of such an attack?

Experts who have analyzed legal issues associated with cyber responses have noted that in kind cyber responses or active defense responses to cyber attacks could result in violations of

[49] Jody R. Westby, "A Shift in Geo-Cyber Stability and Security," Paper presented at ANSER Institute of Homeland Security Conference, "Homeland Security 2005: Charting the Path Ahead," College Park, MD, May 6-7, 2002 at 2-3.

domestic laws or, if the act is deemed to be a "use of force," it could violate the customary rules of war.[50] Other issues arise in the context of assistance from other countries, including multilateral assistance. The Estonian government quickly brought the cyber attacks on their systems to the EU and NATO, raising numerous questions regarding international law and prompting predictions that the attacks "will likely shape a debate inside many governments over how such attacks should be considered in the context of international law and what sort of response is appropriate."[51] "It was a concerted, well-organized attack, and that's why Estonia has taken it so seriously and so have we," noted Robert Pszczel, a NATO spokesman.[52]

Estonia's defense minister, Jaak Aaviksoo, pinpointed the gaps in the NATO treaty with respect to cyber attacks by stating:

> At present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country. Not a single NATO defense minister would define a cyber-attack as a clear military action at present. However, this matter needs to be resolved in the near future."[53]

International cooperation is almost always needed in tracking and tracing cyber communications simply due to the interconnected nature of the Internet and the manner in which the Internet Protocol breaks a communication into packets and routes them across many networks before reassembling them at their destination point. Therefore, the cooperative efforts of nation states may also be necessary in defending against cyber attacks.

The two principal legal instruments that would govern multinational action in a cyber warfare situation are the NATO treaty and the United Nations (UN) Charter. Each document is more than 50 years old and their provisions do not accommodate cyber scenarios.

---

[50] Thomas C. Wingfield, James B. Michael, Duminda Wijesekera, "Optimizing Lawful Responses to Cyber Intrusions," http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/290.pdf.
[51] Christopher Rhoades, "Estonia Gauges Best Response to Cyber Attack," *The Wall Street journal,* May 18, 2007 at A6.
[52] Finn.
[53] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian,* May 17, 2007, http://www.guardian.co.uk/russia/article/0,,2081438,00.html.

UN Charter

The United Nations defines aggression as "the use of armed force by a State against a sovereignty, territorial integrity, or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations…."[54]

The UN Charter has five articles that require scrutiny in the cyber warfare context: Article 2, paragraph 4, and Articles 41, 42, 51, and 99:

> Article 2
> 4. All Members shall refrain in their international relations from the threat or use of force **against the territorial integrity or political independence** of any state, or in any other manner inconsistent with the Purposes of the United Nations.[55]
>
> Article 41
> The Security Council may decide what measures not involving the **use of armed force** are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These **may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication**, and the severance of diplomatic relations.[56]
>
> Article 42
> Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it **may take such action by air, sea, or land forces** as may be necessary to maintain or restore international peace and security. **Such action may include demonstrations, blockade, and other operations by air, sea, or land forces** of the Members of the United Nations.[57]
>
> Article 51
> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an **armed attack** occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this **right of self-defense shall be immediately reported** to the Security Council….[58]

---

[54] United Nations General Assembly Resolution 3314 (XXIX), Dec. 14, 1974, http://jurist.law.pitt.edu/3314.htm; *see also* Jeffrey F. Addicott, *Terrorism Law: Materials, Cases, Comments,* Lawyers & Judges Publishing Co., Inc., 4th ed., 2007 at 28 (hereinafter "Addicott").
[55] Charter of the United Nations, Chapter I, Purposes and Principles, Article 2, para. 4, http://www.un.org/aboutun/charter/ (hereinafter UN Charter) (emphasis added).
[56] UN Charter, Chapter VII, Article 41 (emphasis added).
[57] UN Charter, Chapter VII, Article 42 (emphasis added).
[58] UN Charter, Chapter VII, Article 51 (emphasis added).

> Article 99
> The Secretary-General may bring to the attention of the Security Council any matter which in his opinion may threaten the **maintenance of international peace and security**.[59]

In analyzing these provisions, one first has to ask whether a cyber attack constitutes the use of force against the **territorial integrity or political independence** of another nation, as proscribed by Article 2. Although some cyber attacks that have the force to destroy communication networks (such as the Desert Storm attacks) might be deemed to harm the territorial integrity of a country, the general view is that they would not. Such attacks might well impact the political independence of a nation, however, if its government systems are shut down, web sites are defaced, and electronic government services are impaired. Would economic impact resulting from a cyber attack be considered the use of force against territorial integrity? Perhaps…the CIA plot to sell the Soviet Union bogus software that blew up its pipelines and wreaked significant economic harm to the country allegedly impacted the Soviet Union's territorial integrity by attributing to its downfall. It is a stretch, however, to fit cyber attacks within the meaning of Article 2.

Article 51 indicates that nothing shall block a nation or group of nations from engaging in collective self-defense if an **armed attack** occurs, raising the question of whether a cyber attack could be deemed to be an "armed attack." Even if the attack came from a branch of the armed forces, Article 41 cuts against this interpretation because it discusses **actions that may be taken that are *not* involving the use of armed force**. It specifically includes the complete or partial interruption of communications, which could encompass a cyber attack. Article 42 discusses actions that may be taken by **air, sea, or land forces, including blockades and "other operations.**" Cyber capabilities are well developed within the traditional air, land, and sea branches of the U.S. and foreign militaries. Could cyber military action by the Air Force, for example, that blocked traffic from a specific country or countries be considered an air attack or a blockade? Article 99 allows the Secretary-General to bring matters before the Security Council if **threaten international peace and security**. Would a cyber attack qualify as such a threat? If so, the Security Council could authorize actions by Member nations to block communications from one or more countries or to counter-attack under Article 42.

In sum, none of the UN Charter provisions neatly accommodate cyber attacks and provide clear legal authority for these types of events. The best course of action would be to amend the Charter to make it specifically address the geo-cyber security issues associated with cyber attacks and cyber warfare. It is also important that amendments to the UN Charter include the recognition that cyber defense categories and response capabilities constitute a legitimate branch of military forces alongside air, land, and sea. Chapter XVIII of the Charter governs amendments.

<u>NATO Treaty</u>

The North Atlantic Treaty (NATO Treaty) uses similar language as that in the UN Charter and is equally ambiguous regarding cyber attacks. In fact, Article 1 of the NATO Treaty requires the

[59] UN Charter, Chapter XV, Article 99 (emphasis added).

parties to "refrain in their international relations from the threat or use of force in any manner inconsistent with the purposes of the United Nations."[60] Traditionally, the term "act of war" "refers to the use of aggressive force against a sovereign State by another State in violation of the United Nations Charter and customary international law."[61] However, following the terrorist attacks on September 11, 2001, the North Atlantic Treaty Organization (NATO) invoked its collective defense clause, Article V, even though the attack came from a terrorist organization instead of a country.[62]

The five relevant provisions of the NATO treaty in the context of cyber attacks and cyber warfare are:

> Article 3
> In order more effectively to achieve the objectives of this Treaty, the Parties, **separately and jointly, by means of continuous and effective self-help and mutual aid**, will maintain and develop their individual and collective capacity to resist **armed attack**.[63]
>
> Article 4
> The Parties will consult together whenever, in the opinion of any of them, the **territorial integrity, political independence or security of any of the Parties is threatened**.[64]
>
> Article 5
> The Parties agree that an **armed attack** against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.[65]
>
> Article 6(1)
> For the purpose of Article 5, an **armed attack** on one or more of the Parties is deemed to include an armed attack:
> - On the **territory** of any Parties….;
> - On the **forces, vessels, or aircraft** of any of the Parties….[66]

[60] The North Atlantic Treaty, Article 1, North Atlantic Treaty Organization, Apr. 4, 1949, http://www.nato.int/docu/basictxt/treaty.htm (hereinafter "NATO Treaty").
[61] Addicott at 23.
[62] Addicott at 23.
[63] NATO Treaty, Article 3 (emphasis added).
[64] NATO Treaty, Article 4 (emphasis added).
[65] NATO Treaty, Article 5 (emphasis added).
[66] NATO Treaty, Article 6(1) (emphasis added).

> Article 12
> After the Treaty has been in force for ten years, or at any time thereafter, the Parties shall, if any of them so requests, consult together **for the purpose of reviewing the Treaty**, having regard for the **factors then affecting peace and security** in the North Atlantic area, including the development of universal as well as regional arrangements under the Charter of the United Nations for the maintenance of international peace and security.[67]

A review of the NATO Treaty leaves geo-cyber issues as unsettled as the UN Charter. Article 3 of the Treaty refers to self-help and mutual assistance, but only in the context of an **"armed attack."** Since the NATO Treaty is intended to be consistent with the UN Charter, it is unlikely that a cyber attack would be deemed to be an armed attack absent special circumstances, such as an attack using an electromagnetic pulse generation techniques.[68] The same issues with respect to **territorial integrity and political independence** arise under Article 4 of the Treaty as with Article 2 of the UN Charter. The addition of the words **"or security"** in Article 4, however, may open the door for consultation among NATO member states. Cyber attacks certainly raise national and economic security concerns since defense and financial networks are so dependent upon computer systems and connected networking capabilities. The central provision of the NATO Treaty is Article 5, calling for **collective assistance in the event of an "armed attack"** upon any Party to the Treaty. As the Estonian defense minister pointed out, NATO at this point would most likely not consider a cyber attack an armed attack for purposes of invoking an Article 5 collective response. This conclusion is further supported by Article 6(1) and its reference to **territory, forces, vessels, or aircraft** of any of the Parties. Article 12 does not authorize action but it does offer an avenue for reviewing the NATO Treaty in the context of cyber attacks and geo-cyber security and to include universal approaches and regional arrangements for responding to cyber events.

Upon examination of cyber attacks and the existing legal framework, the World Federation of Scientists' Permanent Monitoring Panel on Information Security supported the following conclusion in its report to the Secretary-General of the UN and the World Summit on the Information Society.

> As electronic information networks expand and military and industrial infrastructures become more dependent on them, cyber-attacks are bound to increase in frequency and magnitude. Interpretations of the UN Charter and of the laws of armed conflict will have to evolve accordingly in order to accommodate the novel definitions of the use of force that such attacks imply….
>
> In terms of the laws of armed conflict, the potentially dangerous consequences of an unnecessary response, a disproportional response or a mistakenly targeted response argue for keeping a human being in the decision loop.

---

[67] NATO Treaty, Article 12 (emphasis added).
[68] Carlo Kopp, "The Electromagnetic Bomb: A Weapon of Electrical Mass Destruction," http://www.globalsecurity.org/military/library/report/1996/apjemp.htm.

> Beyond these preliminary conclusions, there is far more work to be done on both the international, technical, and legal fronts. Nations that choose to employ information operations, or that expect to be targeted by them, should facilitate tracking, attribution, and transnational enforcement through multilateral treaties and, more broadly, by clarifying international customary law regarding the use of force and self-defence in the context of the UN Charter and the laws of armed conflict.[69]

The need to update the legal instruments governing the actions of nation states with respect to cyber warfare and attack capabilities has never been more urgent. The rule of law is already in a precarious state due to the disruptions caused by terrorist activities. The ominous threat of cyber attacks by nation states and rogue actors can no longer be ignored. The UN Charter and NATO Treaty are antiquated and do not accommodate the electronic capabilities of the 21st century. Governments, the private sector, and multinational organizations must begin an international dialogue in this area to accommodate new military capabilities, collective action, and geo-cyber considerations.

Conclusion

There are gaps galore in our ability to counter cyber attacks and protect our critical infrastructure. There are gaps in ownership of weapons (i.e., the CI networks are owned by the private sector but would need to be deployed by the military in a cyber warfare situation). There are gaps in the response coordination that would be required to execute such attacks or defend the networks and gaps in defining responsibilities for command and control. There are gaps in the legal frameworks that would support such offensive, defensive, or collective cyber warfare actions. There are gaps in the prevailing policy mindset that would likely preclude effective decision-making: 20th century principals are not wholly adequate in the 21st cyber century.

The Internet has connected the globe and introduced new ways to harm national and economic security interests. It has also changed the traditional roles of the public and private sectors regarding national defense and public safety. Hard lines between law enforcement and military responsibilities are more blurred in the cyber context. An incident may look like an inside event at the outset but, upon investigation, require law enforcement assistance and, within short order, end up being a cyber attack by a nation state in concert with rogue actors.

The course ahead is clear. Military leaders must engage the private sector and develop offensive and defensive cyber response plans. CI owners must begin analyzing cyber

---

[69] Toward a Universal Order: Managing Threats From Cybercrime to Cyberwar. Report and Recommendations, World Federation of Scientists Permanent Monitoring Panel on Inforrmation Security, Nov. 19, 2003, World Summit on the Information Society, Document No. WSIS-03/GENEVA/CONTR/6-E, http://www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf (*citing* Grove, Goodman, and Lukasik at 100, http://survival.oupjournals.org/cgi/content/abstract/42/3/89).

warfare scenarios and mapping out response plans that will involve military engagement and possibly coordination with other CI sectors. Legal experts, policy makers, and diplomats must work together to bring the legal instruments that underpin international peace and security into the electronic age. The urgency of the situation can hardly be overstated: without such action, we will face legal uncertainty and chaos when managing cyber attacks that are of such a nature that they can jeopardize public safety, national and economic security, global stability, and international peace. This is a risk we cannot afford to take.