Estonia Two-and-a-Half Years Later: A Progress Report on Combating Cyber Attacks

Scott J. Shackelford*

INTRODUCTION

Hackers have been online since a Cornell graduate student infected MIT's burgeoning network with the first Internet worm on November 2, 1988.[i] But recently cyber attacks on states have proliferated both in numbers and severity. The best-known recent example of such a cyber attack was on April 27, 2007. In a matter of hours, the websites of Estonia's leading banks and newspapers crashed. Government communications were compromised. An enemy had invaded and was assaulting dozens of targets across the country.[ii] But this was not the result of a nuclear, chemical, or biological weapon of mass destruction. Nor was it a classical terrorist attack. A computer network was responsible, with attacks coming from thousands of zombie private computers around the world.[iii] And this was just the beginning. Flash forward to August 7, 2008 when immediately prior to the Russian army invading Georgia en masse a cyber attack reportedly crippled the IT systems of the Georgian military including air defense. Georgian command and control was forced to resort to U.S. government and Google accounts while Estonian advisors helped to deflect the ongoing cyber onslaught.[iv]

These cyber attacks are far from unique. Literally thousands of largely unreported major and minor cyber attacks occur daily. Power utilities in the United States,[v] Polish and South Korean government websites, and UK technology firms have all be hit by cyber attacks in just the past few months.[vi] Even school districts in Illinois, Colorado, and Oklahoma have lost millions to fraudulent wire transfers.[vii] Responses have been varied, with many nations such as Singapore creating new cyber security authorities responsible for safeguarding IT.[viii]

Together these episodes exemplify that cyber attacks against states are increasingly common, and increasingly serious. No longer does it take thousands of planes and divisions of soldiers to destroy vital governmental institutions. It can now be done by a relatively small group of knowledgeable persons linking together zombie computers into a clandestine network that may be used to crash nearly any computer system in the world connected to the internet, from air traffic control to sewage treatment plants.[ix]

The central topic of this article is uncovering in brief what is being, and can be done to counter these attacks, both at the national and international level. The focus is on the last two-and-a-half years since the specter of cyber war fully entered public consciousness on the international scene with the cyber attack on Estonia. The question presented is what progress has been made since that time? In short, the answer is very little. Many nations have found mutual benefit in the status quo strategic ambiguity.[x] National information infrastructures, and the World Wide Web in general, remain acutely vulnerable to cyber attacks. Without concerted multilateral action, such as by coordinating the more than 250 Cyber Emergency Response Teams (CERTs) currently operating around the world while also clarifying the applicable legal regime, this intolerable state of affairs will continue.

The structure of the article is as follows. Part I analyzes the threat of cyber attacks to international peace and security. Part II briefly summarizes the current cyber defense policies of the major players, to the extent that information is publicly available, including the United States, Russia, China, and NATO. Part III lays out the current legal regime that may be applied to cyber attacks, highlighting the significant gaps in the system. Finally, Part IV concludes by arguing for the need for a new regime for regulating cyber attacks and proposes new minilateral and multilateral measures that should be taken to more effectively protect information infrastructures from cyber attacks.

THE THREAT OF CYBER ATTACKS – FROM NET WAR TO NUCLEAR WAR

The President's Commission on Critical Infrastructure Protection has noted that more than 19 million individuals have the knowledge with which to launch cyber-attacks. Little specialized equipment is needed.[xi] The basic attack tools consist of a laptop, modem, telephone, and software—the same instruments commonly used by hackers. Interpol has estimated that there are as many as 30,000 websites that provided automated hacking tools and software downloads.[xii] In 2000, a total of 22,144 attacks were detected on Defense Department networks, up from 5,844 in 1998.[xiii] Worldwide aggregate damage from these attacks is now measured in billions of U.S. dollars annually.[xiv] In fact, the U.S. is "under cyber-attack virtually all the time," according to Defense Secretary Robert Gates. Emblematic of this new threat, the U.S. Air Force adopted a new mission statement in 2005 "to fight in air, space, and cyberspace."[xv]

Due to the ease of launching cyber attacks, it is difficult if not impossible to stop them from occurring, since even the best defensive security systems in the world may be compromised given enough free attempts. The question then is how the United States and NATO should respond to these attacks. The potential threat that cyber attacks pose to international peace and security has been well recognized by the United States and Russia. U.S. Air Force General Kevin Chilton recently told *Stars & Stripes* that the U.S. military's response to a cyber-attack would not necessarily be limited to cyberspace.[xvi] Others both in the U.S. and in Russia have been even more bellicose, threatening nuclear reprisals in retaliation to a worst-case scenario cyber attack.

The nuclear analogy has also not been lost on victim states. Ene Ergma, the Speaker of the Estonian Parliament who has a doctorate in nuclear physics, has made the comparison that "When I look at a nuclear explosion and the explosion that happened in our country in May, I see the same thing."[xvii] As with nuclear radiation, information warfare (IW) can destroy a modern state, including its economy, and deprive much of its population of basic services, including electricity, water, sanitation, and even police and fire protection if the emergency bands similarly crash. This luckily did not happen in Estonia or Georgia. But if such a doomsday attack did take place, it would constitute an "electronic Pearl Harbor" that would destroy most of a nation's information infrastructure, just like an electromagnetic pulse from a nuclear weapon.[xviii] What is needed then is an active and vigorous cyber defense, at the national and global level, to combat cyber attacks and hold accountable those who launch them.

CYBER DEFENSE

Currently with the exception of NATO the vast majority of defensive strategies being employed to counter cyber attacks are being done domestically at the national level. Although nearly every nation in the world has been a victim of cyber attacks, the most serious consequences arise when countries with nuclear arsenals are attacked. As has been stated, both Russia and the United States have not ruled out the use of nuclear weapons in response to cyber attacks. China's policy is even more opaque. Thus, what follows is a brief summary of the current IW strategies of the great powers, along with a summary of NATO's evolving policy.

UNITED STATES

The United States in many ways pioneered cyber defense beginning with the creation of the first CERT at Carnegie Mellon University in 1988 in response to a growing number of network intrusions.[xix] Today the U.S. Cyber Emergency Response Team (USCERT) is an element within the Department of Homeland Security (DHS) that "coordinates defense against and responses to cyber attacks across the nation."[xx] There are now more than 250 CERTs currently in operation worldwide, but cooperation between CERTs remains limited.[xxi]

USCERT is only the beginning of the confused world of U.S. cyber defense. The Federal Bureau of Investigation also has a role to play in countering cyber attacks. If the source is foreign, then the Central Intelligence Agency is involved. While if the cyber attack involves financial intrusions, the Secret Service would be the primary agency on point.[xxii] The Department of Defense, and the National Security Agency also have cyber security specialists. In particular, U.S. Defense Secretary Robert Gates signed a memorandum on June 23, 2009 announcing the formation of U.S. Cyber Command (CYBERCOM), which is a "subordinate unified command" under U.S. Strategic Command. CYBERCOM is due to be in full operation by October 2010,[xxiii] but its place vis-à-vis the other cyber defense specialists in the agencies enumerated above remains largely undefined.

Recognizing both the confusion and the need for a coherent policy on cyber security, President Obama appointed a permanent "cyber czar." But since Melissa Hathaway resigned in August 2009, the post has remained vacant. And despite reshuffling, an integrated U.S. cyber command has yet to be established. Senators Lieberman and Collins have been debating about how much oversight authority to give DHS, whether the DHS should be a regulator or a resource for at-risk companies and institutions, and the extent to which a cyber czar is needed at the White House. At this point though, despite increasing resources being put towards cyber defense, such as U.S. Secretary of Homeland Security Janet Napolitano's hiring of up to 1,000 cyber security experts at the White House and opening of a new cyber security center, much remains undefined.[xxiv] For example, despite years of trying, still only two percent of the integrated circuits purchased by the Pentagon are made in the USA, with the majority coming from Asian nations with a track record of "unambiguous, deliberate subversions" of computer

hardware.[xxv] Such practices, and increasingly ambitious cyber attacks from foreign nations, including China, have led to the loss of 10 to 20 terabytes of sensitive information in recent years.[xxvi]

PEOPLE'S REPUBLIC OF CHINA

Numerous reports have been published about China's complicity, and even active state sponsorship, of cyber attacks against a huge array of targets. Security researchers at the Information Warfare Monitor in Toronto, and Cambridge University, have found that more than 1,200 computers in 103 nations have been compromised by Chinese computer systems.[xxvii] Attacks have recently spiked from one or two per week in 2005, to more than 50 per week in 2008. For example, Chinese hackers penetrated American electricity grids in 2007.[xxviii] In March 2007, the Department of Energy's Idaho National Laboratory conducted an experiment to see whether a power plant could be damaged or destroyed through hacking alone. Researchers were able to cause the generator to "shake, smoke, and shut down with a few keystrokes."[xxix]

China has frequently disavowed such charges, but China's own stated military goals include improving the country's ability to wage information warfare.[xxx] Although little public data exists, China is known to be aggressively hiring young, tech savvy "cyber warriors" to carry out cyber attacks against a variety of targets, including Taiwan.[xxxi] This force is being trained under a policy of Local War under Informationised conditions (LWUIC). The LWUIC is the People's Liberation Army's effort to develop a "fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the electromagnetic spectrum."[xxxii] The Department of Defense has confirmed that China is enhancing its IW capabilities, with an emphasis on weakening potential adversaries command and control systems.[xxxiii] In light of China's relative military weakness compared to the United States and Russia, a recent report has underscored the fact that China is likely making use of cyber attacks to secure an "asymmetric advantage to deter aggression from stronger military powers as they catch up in traditional military capabilities…and also allow China to leapfrog by means of technology transfer and exploiting adversary weaknesses."[xxxiv] But much of China's real intentions and capabilities is mostly guesswork.[xxxv] What is known is that China, like the United States and Russia, is pursuing an aggressive information warfare program with both substantial offensive and defensive components.

RUSSIA

Like China, Russia has become fully committed to developing its IW capabilities over the past decade. Although never proven due to the fundamental difficulty of attribution, i.e. proving the source of cyber attacks, Russia has been linked to the cyber attacks on Estonia in 2007, Georgia in 2008, and Poland in 2009.[xxxvi]

There are four primary institutions responsible for information security in Russia. First, the Russian Security Council is tasked with protecting national interests that could be compromised through IW. Second, the Federal Agency for Government

Communications and Information (FAPSI) is responsible for ensuring the security of state communications. Third, the State Technical commission is devoted to the development of international law, licensing, and certification of IW related policies. And fourth, the Russian armed forces are responsible for studying the impact of information operations on the military.[xxxvii] Since the breakup of the Soviet Union, Russia, like China, has viewed IW as a means to challenge US/NATO military dominance asymmetrically, and likely will continue to do so for the immediate future.

NATO

During the cyber attack on Estonia elements within Estonia's government advocated for evoking Article 5 of the North Atlantic Treaty Organization, which states that an assault on one allied country obligates the alliance to attack the aggressor.[xxxviii] This was the first time in NATO history that a member state had formally requested emergency assistance in the defense of its digital assets.[xxxix] It did not occur. Some have contended that the cyber attacks, to the extent that they were incited by Russia, amount to a test for NATO on its IW defenses.[xl] If this is the case, then it failed. NATO members dispatched specialists to Tallinn, but did not or could not have done much else given that so much of the Internet is run by the private sector and international organizations.[xli] The episode illustrated the lack of a coherent NATO cyber doctrine and strategy.[xlii]

The first time that NATO formally grappled with how the alliance should respond to cyber attacks was on May 14, 2008 during the Bucharest Summit.[xliii] Specifically, Section 47 of the Bucharest Summit Declaration declares that:

> NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defense, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defense emphasizes the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defense capabilities and strengthening the linkages between NATO and national authorities.[xliv]

There have been two tangible results from the Bucharest Summit. The first occurred when seven NATO nations and the Allied Command signed documents formalizing the creation of a Cooperative Cyber Defense (CCD) Centre of Excellence (COE) in Tallinn, Estonia.[xlv] The centre on cyber warfare will employ 30 persons, half of them specialists from the sponsoring countries of Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, and Spain.[xlvi] This is the tenth NATO COE in existence, and the only focused solely on defending against and countering cyber attacks.

The second result of the Bucharest Summit was the creation of a new Cyber Defense Management Authority (CDMA) in Brussels, which is a NATO effort to centralize cyber

defense capabilities.[xlvii] The goal of the Authority is to merge national and private sector cyber defense elements in the new CDMA with an eye towards preventing, detecting, and deterring attacks from either state or criminal sources.[xlviii] Little public data exists as to the precise capabilities of the CDMA, but it is thought to contain "real-time electronic monitoring capabilities for pinpointing threats and sharing cyber intelligence in real time."[xlix] Ultimately, the North Atlantic Council remains in overall control of NATO's policies and activities regarding cyber defense.[l] And at this point, cyber attacks will only activate Article 4 of the NATO treaty, meaning that members must only "consult together" in cases of cyber attacks, but are not bound to "assist" each other as foreseen as required under Article 5.[li]

Further steps need to be taken before NATO can effectively counter cyber attacks. These include coordinating the NATO CERTs of member nations, and ensuring that every CERT is fully manned and ready. National criminal laws relating to cyber attacks should also be harmonized. While the other far more critical and difficult issue remains clarifying the role of international law in combating cyber attacks.

THE EXISTING LEGAL REGIME FOR CYBER ATTACKS

The confusion about how to respond to large-scale cyber attacks on a state highlights the need for a new regime to regulate state-sponsored cyber attacks. Without a new regime, and given the horrific nature and growing prevalence of cyber attacks, states will resort to threatening to use their most powerful weapons available, including nuclear weapons, with potentially dire consequences.

The international legal framework to deal with cyber attacks is severely underdeveloped. Basic questions such as "is a cyber attack a 'use of force' under the U.N. Charter, and if so does it activate a right of self-defense against the aggressor state?' have not been answered. Indeed, they are only beginning to be asked. For example, even if Estonia could conclusively prove that Russia was behind the April 2007 attack, it is unsettled whether it could legally respond with force, cyber attacks, or other countermeasures. Proving which government or organization is behind a cyber attack is itself a tall order since many attacks are extremely difficult to trace, making attribution a key issue of any future regime. The unsatisfactory status quo suggests two options—adapt current regimes, or create a new treaty from whole cloth.

A cyber attack currently activates one of two different areas of international law. The critical issue in deciding which is applicable is how bad a cyber attack is, i.e., whether a cyber attack has such horrific results that it is like a traditional attack by another nation's armed forces. Above and below this "armed attack" threshold then, different laws are applicable. Relatively less serious cyber attacks, such as what happened in Estonia, activate various treaty provisions. These include, among others: (1) Article 35 of the International Telecommunications Union dealing with government communications and safety services; (2) Articles 19 and 113 of the United Nations Convention on the Law of the Sea if the defender nation is a coastal state; (3) applicable Mutual Legal Assistance Treaties, extradition treaties, and Status of Forces Agreements; and (4) the potential for

Chapter VII United Nations Security Council Resolutions. But few of these treaties have enforcement mechanisms, such as mandatory reparations or sanctions on aggressor states if they are breached.

In contrast, the law becomes much clearer above the threshold of an armed attack. If a very serious cyber attack occurs, such as that envisioned by Hollywood in *Die Hard 4.0*, international humanitarian law, or the laws of war, is activated. This provides for, among much else, proportional responses to armed attacks. But it is still unclear when a cyber attack reaches the level of an armed attack in practice, or how international human rights law should be combined within this emerging framework.

CREATING A NEW REGIME TO COUNTER CYBER ATTACKS

It is becoming exceedingly difficult to craft multilateral treaties designed to deal with regulations of common resources, including cyberspace. Add to that is the desire of the great powers, including the United States, China, and Russia to embrace a certain degree of strategic ambiguity in cyberspace.[lii] Along with the fact that diplomats and policymakers also often lack the technical expertise necessary to fashion effective multilateral regulations that would curtail cyber attacks. Together, these forces mean that a new international treaty on cyber security may well currently be unattainable in the short term. If that is the case, then other immediate measure should be taken. Both options are briefly discussed below.

PROPOSAL: MULTILATERAL TREATY ON CYBER SECURITY

Given the confused legal regime, the best way to ensure a comprehensive regime is through a new international accord dealing exclusively with cyber security and its status in international law. Building consensus for the adoption of a new treaty is no easy feat in an increasingly multipolar world. Nevertheless, the multilateral approach of the Obama Administration is potentially well suited to getting a handle on this problem. Specifically, a new treaty should: (1) define when a cyber attack rises to the level of an armed attack; (2) clarify which provisions of international law apply during cyber warfare; and (3) provide for enforcement mechanisms in the event of breach. Other worthwhile ideas include creating a Multinational Cyber Emergency Response Team (MCERT) to both investigate which nations are behind cyber attacks, and have the defensive expertise needed to be fast responders when serious attacks occur. This could be done by networking together the current network of more than 250 national CERTs with the NATO-wide CERT based in Estonia.

SHORT-TERM MEASURES BENEFITING GLOBAL CYBER SECURITY

Short of a new treaty, NATO should partner with the global network of CERTs and work together to a multilateral security partnership that could: (1) root out state sponsors of cyber attacks; (2) better defend against cyber attacks by pooling resources and talent; and (3) provide invaluable intelligence to overcome the fundamental issue of attribution. Collaboration with the private sector in combating cyber attacks has been strong,

including working with Microsoft, Google, and IBM, but a global regime built to curtail cyber attacks should more aggressively partner with technology firms around the world. Bilateral and multilateral partnerships with police bodies, including Interpol, should also be established especially since the majority of severe cyber attacks have a criminal component.[liii] Finally, the Obama Administration should demonstrate its leadership and release a white paper on how it would respond to different levels of cyber attacks to alleviate confusion and blunt the threat of nuclear war. This could be done in collaboration with foreign governments, in particular Russia and China, who could then follow suit. The Obama Administration should also once and for all decide which department should have primary responsibility for cyber security, while guaranteeing a budget that avoids the wavering commitments seen recently.

CONCLUSION

With an economy in crisis, two wars raging, and many domestic policy issues all vying for attention, it is easy to put off dealing with an issue like cyber attacks in a comprehensive manner. But without either defining how existing international law applies to cyber attacks, or ideally drafting a new multilateral treaty to deal with this area of international conflict, the international community will lurch from case to case, warding off Net War version 2.0 with vague and destabilizing threats of nuclear reprisal. Individual nations acting alone cannot combat this problem, especially since it is nearly impossible to prove who's behind cyber attacks. Collective action is required. It is that collective action that has been missing over the past two-and-a-half years. The status quo strategic ambiguity is unsustainable, and is a threat to international peace and security. Without multilateral action, such as through a treaty clarifying the applicable legal regime, or at least a global security partnership networking together CERTs into a multinational force working together to unmask attackers, Estonia could be just the beginning.

*Professional Background Summary:

Scott Shackelford is a graduate of Stanford Law School, and is currently a Ph.D. candidate at the University of Cambridge Department of Politics and International Studies. The author wishes to thank his lovely wife, Emily Shackelford, for her encouragement and help with this article.

---

[i] *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 37-45 (2008)

[ii] *See generally* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED MAGAZINE, Aug. 21, 2007, *available at*:

http://www.wired.com/politics/security/magazine/15-09/ff_estonia (detailing a rogue computer network's assault on Estonia).

[iii] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (LONDON), May 17, 2007, at 1.

[iv] *See* Brian Krebs, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, WASH. POST, Oct. 16, 2008, *available at*: http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (discussing Russian officials' plausible connivance at the online assault on Georgia and the internet activities that led up to the assault).

[v] Marshall White, *Rural areas not immune to cyber attacks*, STJOENEWS.NET, Aug. 9, 2009, *available at*: http://www.stjoenews.net/news/2009/aug/09/rural-areas-not-immune-cyber-attacks/?local.

[vi] Warwick Ashford, *Risk of cyber attack high as firms cut IT budgets, say researchers*, COMPUTERWEEKLY.COM, Oct. 15, 2009, *available at*: http://www.computerweekly.com/Articles/2009/10/15/238147/risk-of-cyber-attack-high-as-firms-cut-it-budgets-say.htm.

[vii] Rob Bauder, *Cyber gang likely siphoned district's money*, BEAVER COUNTY TIMES, Oct. 20, 2009, *available at*: http://www.timesonline.com/bct_news/news_details/article/1373/2009/october/04/officials-cyber-gang-likely-siphoned-districts-money.html.

[viii] Wendell Minnick, *Singapore Beefs up Cyber Security*, DEFENSE NEWS, Oct. 5, 2009, *available at*: http://www.defensenews.com/story.php?i=4309920&c=ASI&s=TOP.

[ix] For a full length discussion of these and other issues surrounding cyber attacks, see Scott J. Shackelford, *From Net War to Nuclear War: Analogizing Cyber Attacks in International Law*, 25(3) BERKELEY J. INT'L L. (2009).

[x] Rex B. Hughes, *NATO and Cyber Defence: Mission Accomplished?*, NATO-OTAN, Apr. 2009, *available at*: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf.

[xi] PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURE x, 9 (1997), *available at* http://www.ihs.gov/misc/links_gateway/download.cfm?doc_id=327&app_dir_id=4&doc_file=PCCIP_Report.pdf.

[xii] The following is a list of common IW weapons: *Sniffer* –a program executed from a remote site by an intruder, which allows the intruder to retrieve user IDs and passwords or other information; *Trojan Horse* – a program remotely installed into the controlling switching centers of the Public Switched Network; *Trap Door* – a program used to gain unauthorized access into secured systems; *Logic bomb* – lies dormant and can be hidden within a Trojan Horse until a trigger condition causes it to activate and destroy the host computer's files; *Video-morphing* – makes broadcasts indistinguishable from normal transborder data flows; *Denial of service attack* – prevents networks from exchanging data; *Computer worm or virus* – travels from computer to computer across a hospitals network, damaging files; *Infoblockade* - blocks all electronic information from entering or leaving a state's borders; *Spamming* – floods military and civil email communications systems with frivolous messages, overloading servers and preventing field

communications; *IP spoofing* – fabricates messages whereby an enemy masquerades as an authorized command authority. Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 836-39 (2001) (arguing that assessing self-defense responses to cyber attacks and the role international institutions to attain these objectives need clear rules).

[xiii] Jim Wolf, *Hacking of Pentagon Persists*, WASH. POST, Aug. 9, 2000 at A23.

[xiv] Pamela Hess, *Pentagon Puts Hold on USAF Cyber Effort*, ASSOCIATED PRESS, Aug. 13, 2008, *available at* http://www.boston.com/news/nation/washington/articles/2008/08/13/pentagon_puts_hold_on_usaf_cyber_effort/ (reporting that during the Georgian conflict "The Russians just shot down the government command nets so they could cover their incursion…This was really one of the first aspects of a coordinated military action that had cyber as a lead force, instead of sending in air planes.").

[xv] Sgt. Sara Wood, *New Air Force Command to Fight in Cyberspace*, AMERICAN FORCES PRESS SERVICE, Nov. 3, 2006, *available at*: http://www.defenselink.mil/News/NewsArticle.aspx?id=2014.

[xvi] Jeff Schogol, *Official: No options 'off the table' for U.S. response to cyber attacks*, STARS AND STRIPES, May 8, 2009, *available at*: http://www.stripes.com/article.asp?section=104&article=62555.

[xvii] Kevin Poulsen, *'Cyberwar' and Estonia's Panic Attack*, WIRED, Aug. 22, 2007, *available at*: http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html.

[xviii] *Doomsday Fears of Terror Cyber-Attacks*, BBC NEWS, Oct. 11, 2001, *available at*: http://news.bbc.co.uk/2/hi/science/nature/1593018.stm.

[xix] Hughes, *supra* note x.

[xx] United States Computer Emergency Readiness Team (US-CERT), *About Us*, *available at:* http://www.us-cert.gov/aboutus.html.

[xxi] Hughes, *supra* note x.

[xxii] *Id*.

[xxiii] Tom Burghardt, *The Launching of U.S. Cyber Command*, GLOBALRESEARCH.CA, July 1, 2009, *available at*: http://www.globalresearch.ca/index.php?context=va&aid=14186.

[xxiv] Ed O'Keefe, *Lieberman lays out his cyber security plan*, Wash. Post, Oct. 30, 2009, *available at*: http://voices.washingtonpost.com/federal-eye/2009/10/lieberman_lays_out_his_cyber_s.html?hpid=topnews; Daniel Fleischman, *Online only: Cyber security*, IDS, Oct. 8, 2009, *available at*: http://www.idsnews.com/news/story.aspx?id=70817; Elizabeth Lee, *Department of Homeland Security Opens Cyber Security Center*, VOICE OF AMERICA NEWS, Oct. 31, 2009, *available at*: http://www.voanews.com/english/2009-10-31-voa3.cfm.

[xxv] John Markoff, *Old Trick Threatens the Newest Weapons*, N.Y. TIMES, Oct. 26, 2009, *available at*: http://www.nytimes.com/2009/10/27/science/27trojan.html?hpw.

[xxvi] McMillan, *supra* note xi.

[xxvii] Ben Worthen, *Wide Cyber Attack is Linked to China*, WSJ, Mar. 30, 2009, *available at*: http://online.wsj.com/article/SB123834671171466791.html.

[xxviii] James D. Zirin, *Abdicating on a cyber czar?*, L.A. TIMES, Oct. 14, 2009, *available at*: http://www.latimes.com/news/opinion/commentary/la-oe-zirin14-2009oct14,0,603775.story.
[xxix] *Id.*
[xxx] Larry Greenmeier, *China's Cyber Attacks Signal New Battlefield is Online*, SCIENTIFIC AMERICAN, Sep. 18, 2007, *available at*: http://www.scientificamerican.com/article.cfm?id=chinas-cyber-attacks-sign.
[xxxi] Mac William Bishop, *China's Cyberwarriors*, FOREIGN POLICY, Sep. 2006, *available at*: http://www.foreignpolicy.com/users/login.php?story_id=3553&URL=http://www.foreignpolicy.com/story/cms.php?story_id=3553.
[xxxii] Steve DeWeese, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, NORTHRUP GRUMAN, Oct. 9, 2009, *available at*: http://www.domain-b.com/defence/general/NorthropGrumman_domain-b.pdf.
[xxxiii] *See* FY2004 Report to Congress on PRC Military Power, *available at*: http://www.defenselink. mil/pubs/d20040528PRC.pdf. *See also* Clay Wilson, *Information Warfare and Cyberwar: Capabilities and Related Policy Issues*, CRS, July 19, 2004, *available at*: http://www.rtna.ac.th/article/Information%20Warfare%20and%20Cyberwar_Capabilities%20and%20Related%20Issues.pdf.
[xxxiv] Robert McMillan, *Report Says China Ready for Cyber-war, Espionage*, PC WORLD, Oct. 23, 2009, *available at*: http://www.pcworld.com/article/174210/report_says_china_ready_for_cyberwar_espionage.html.
[xxxv] Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, U.S. ARMY WAR COLLEGE, Nov. 2001, *available at*: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA397266&Location=U2&doc=GetTRDoc.pdf.
[xxxvi] John Leyden, *Russian Cybercrooks Turn on Georgia*, REGISTER, Aug. 11, 2008, *available at*: http://www.theregister.co.uk/2008/08/11/georgia_ddos_attack_reloaded/; *Russia Refused Legal Assistance in Cyber Attacks Investigation*, 17 EST.REV. 3, 4 (2007), *available a*t: http://www.estonia.com.au/pics/er_27.pdf; John Leyden, *Polish Government cyberattack blamed on Russia*, REGISTER, Oct. 13, 2009, *available at*: http://www.theregister.co.uk/2009/10/13/poland_cyberattacks/.
[xxxvii] Timothy I. Thomas, *Russia's information warfare structure: Understanding the roles of the security council, Fapsi, the state technical commission and the military*, 7(1) EUROPEAN SECURITY 156, 156 (Spring 1998).
[xxxviii] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.
[xxxix] Hughes, *supra* note x.
[xl] Davis, *supra* note ii.
[xli] *See generally* Gary Peach & Paul Ames, *Stung by Cyber Warfare, Estonia, NATO Allies to Sign Deal on Cyber Defense Center*, ASSOCIATED PRESS, Mar. 13, 2008, *available at*: http://www.iht.com/articles/ap/2008/05/13/europe/EU-GEN-Estonia-NATO-Cyberterrorism.php.
[xlii] Hughes, *supra* note x.

[xliii] *Id.* The lead up to the Bucharest Summit began with the 2002 Prague and the 2006 Riga Summits, both of which were geared towards putting in place information systems.
[xliv] Section 47, NATO Bucharest Summit Declaration (2008).
[xlv] *NATO opens new centre of excellence on cyber defence*, NATO NEWS, May 20, 2008, *available at*: http://www.nato.int/docu/update/2008/05-may/e0514a.html.
[xlvi] *Id.*
[xlvii] *Id.*
[xlviii] Ian Grant, *NATO sets up Cyber Defence Management Authority in Brussels*, COMPUTERWEEKLY.COM, Apr. 2008, *available at*: http://www.computerweekly.com/Articles/2008/04/04/230143/nato-sets-up-cyber-defence-management-authority-in-brussels.htm.
[xlix] Hughes, *supra* note x.
[l] *Defending against cyber attacks*, NATO NEWS, January 29, 2009, *available at*: http://www.nato.int/issues/cyber_defence/index.html.
[li] *NATO agrees on common approach to cyber defence*, EURACTIV.COM, April 4, 2008, *available at*: http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence/article-171377.
[lii] Hughes, *supra* note i.
[liii] *Id*.