THE BATTLEFIELD OF CYBERSPACE: THE INEVITABLE NEW MILITARY BRANCH— THE CYBER FORCE

I. INTRODUCTION

"Information is now a place . . . . It is a place where we must ensure American security as surely as . . . [l]and, sea, air and space."[1]

Air Force Lt. Gen. Michael Hayden

With all the technical wonders and benefits associated with cyberspace,[2] few understand that cyberspace is also a new global battlefield that encompasses households, corporations, universities, governments, militaries, and all categories of critical infrastructures. While sipping a low-fat, no foam, soy latte at a café, a cyber warrior[3] of a nation state or a cyber terrorist[4] may access the Internet and unleash attacks within cyberspace. Indeed, in contrast to a suicide bomber, a cyber terrorist is not limited to just one act of terrorism within cyberspace ("cyber terrorism"). In order to protect the health, wealth, and safety of the United States and its citizens from cyber attacks, presidential directives, executive orders, legislation, agency policies, and warnings have been issued.[5] As a result, for several years, the United States Air Force, the Secret Service, the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), the Homeland Security Council, the Department of Defense (DOD), the Office of Management and Budget (OMB), and other federal agencies have operated to secure cyberspace.[6] In fact, in 2006, the Air Force officially elevated its cyberspace operations' profile by assigning the 8th Air Force as the new Air Force Cyberspace Command.[7] Consequently, this article argues that, inevitably, the United

---

[1] Jim Wolf, *U.S. Spy Chief: Cyberspace Is Potential Battlefield*, Oct. 17, 2000, http://cndyorks.gn.apc.org/yspace/articles/cyberwar3.htm.

[2] Cyberspace is defined as "[t]he electronic medium of computer networks, in which online communication takes place." THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 452 (4th ed. 2000).

[3] A solider under the command of a nation state who acts within and through cyberspace.

[4] A person plotting and executing terrorist acts within cyberspace.

[5] *See infra* apps. A & B.

[6] *See generally* JOHN MOTEFF, COMPUTER SECURITY: A SUMMARY OF SELECTED FEDERAL LAWS, EXECUTIVE ORDERS, AND PRESIDENTIAL DIRECTIVES (Cong. Research Serv. 2004), *available at* http://www.fas.org/irp/crs/RL32357.pdf (discussing the various entities that operate to secure cyberspace).

[7] C. Todd Lopez, *8th Air Force to Become New Cyber Command*, AIR FORCE LINK, Nov. 3, 2006, *available at* http://www.af.mil/news/story_print.asp?id=123030505.

States Congress will have to consider elevating United States cyberspace operations to more than a command within the Air Force, but rather, a new military branch: the Cyber Force. For a couple of years, cyber operations may hatch and be fed within the Air Force's nest, but in the future, the Air Force will need to push cyber operations from its nest so it can fly as the Cyber Force.

II. THE DOMAIN OF CYBERSPACE

"[C]yberspace is neither a mission nor an operation. . . . [It] is a strategic, operational and tactical warfighting domain . . . ."[8]

Dr. Lani Kass, Director of the Air Force Cyberspace Task Force

A. The Interconnectedness of Cyberspace

In October of 2006, the Joint Chiefs of Staff of the U.S. Armed Forces officially defined cyberspace as "[a] domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[9] Cyberspace users—households, corporations, universities, governments, and the military—travel in cyberspace to build and reach destinations of information, which is shared, acquired, and controlled through networked systems connected by "ordinary telephone lines, microwave relays, satellite uplinks and downlinks[,]" fiber optics, cables, transistors, and microchips.[10] These networks use an agreed upon computer language to communicate.[11] For example, the Internet, which is the most accessed and well-known

[8] C. Todd Lopez, *Senior Leaders Discuss Fighting in Cyberspace*, INTERCOM, Nov. 2006, at 18–19, *available at* http://public.afca.af.mil/shared/media/document/AFD-061220-041.pdf (emphasis added).

[9] Michael W. Wynne, Sec'y of the Air Force, Remarks as Delivered to the C4ISR Integration Conference: Cyberspace as a Domain in Which the Air Force Flies and Fights (Nov. 2, 2006), *available at* http://www.af.mil/library/speeches/speech.asp?id=283.

[10] Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 135–36 (2005) (citing George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1094–95 (2000)).

[11] *See* Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 252 (2005) (citing Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 821 (2004)) (discussing how networks communicate).

networked system,[12] uses the Internet Protocol as its language.[13]

Through the skillful use of computer language, networks become accessible. The extent of a network's vulnerability to infiltration is directly proportional to the extent of a network's accessibility.[14] As a result, the United States should be greatly concerned about the breadth of a cyber attack, because of the interconnectedness of the military, civilian, and business sectors. DOD relies heavily on civilian technology, much of which is made by foreign companies whose knowledge and expertise concerning our systems contributes to American vulnerability.[15] Additionally, ninety-five percent of the United States military's information transfers,[16] and ninety percent of large companies' information transfers, depend upon the less secure civilian networks.[17] The national vulnerability to cyber attack, which is a result of this interconnectedness, emphasizes that cyberspace—like land, sea, air, and space—must be defended.

B. International Recognition of Cyberspace as a Battlefield

States, criminal organizations, terrorist organizations, and specific individuals are using the developed networks to transverse cyberspace and launch cyber attacks. The United States Government Accounting Office has announced that "information warfare systems" are being developed and used by at least "[one hundred twenty] countries or groups."[18] Peru, Iran,

---

[12] *See* Antolin-Jenkins, *supra* note 10, at 135 (explaining that the Internet is "the primary means for information transmission today . . . ").

[13] *Id.* at 136.

[14] Rob Nazzal, *The Evolving Network Demands Improved Security*, CUSTOMER INTERACTION SOLUTIONS, Apr. 1, 2005, http://www.allbusiness.com/technology/computer-software-security/472056-1.html.

[15] *See* CLAY WILSON, COMPUTER ATTACK AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 8, 11–13, 16 (Cong. Research Serv. 2005), *available at* http://usinfo.state.gov/infousa/government/overview/docs/RL32114.pdf [hereinafter COMPUTER ATTACK] (discussing the ability of foreigners to access civilian technology used by the DOD and the vulnerability of U.S. systems).

[16] Antolin-Jenkins, *supra* note 10, at 133 (citing Ronald Knecht & Ronald A. Grove, *The Information Warfare Challenges of a National Information Infrastructure*, http://webarchive.og/web/2001107174401/htp://infowar.com/mil_c4i//iwchall.hyml-ssi (last visited May 12, 2003)).

[17] *Id.* at 132 (citing Frank J. Cilluffo, Paul Byron Pattak & George Charles Salmoiraghi, *Bad Guys and Good Stuff: When and Where Will the Cyber Threats Converge?,* 12 DEPAUL BUS. L.J. 131, 139 (1999–2000)).

[18] John Christensen, *Bracing for Guerrilla Warfare in Cyberspace: 'There Are*

United Arab Emirates, Saudi Arabia, Croatia, Vietnam, and Russia have launched cyber attacks on American financial, power, and utility infrastructures via cyberspace.[19] More disturbing is the fact that China and North Korea have integrated the employment of cyber attacks into their military strategy and doctrine. [20] North Korea, under the auspices of national defense, may be training more than one hundred new cyber warriors per year for cyber operations.[21] China has considered developing a fourth military branch focused on cyber warfare.[22] In fact, "[s]everal commentators . . . speculated" that in 2001, "Hack the USA" week, in which multiple United States government websites were shut down or altered and the content of one United States government website was replaced with China's national flag and anthem, was sponsored by the Chinese government.[23] Additionally, on April 27, 2007, Internet warfare broke out between Estonia and Russia, leaving Estonia defending "denial of service" cyber attacks.[24] If four countries, including the United States, are "openly" building a cyber military presence, six countries are blatantly launching cyber attacks against

Lots of Opportunities; That's Very Scary', CNN.COM (Apr. 6, 1999), http://www.cnn.com/TECH/specials/hackers/cyberterror/.

[19] *Id.*; Erik Stakelbeck, *Cyber Terror: Defusing the Timebomb*, CBNNEWS.COM, Apr. 2, 2007, http://www.cbn.com/CBNnews/84460.aspx?option=print.

[20] South Korea, in fear of what is believed to be North Korea's cyber prowess, has increased its defense budget to fund information warfare and has built centers to train information warriors. Brian McWilliams, *North Korea's School for Hackers*, WIRED, June 2, 2003, *available at* http://www.wired.com/print/politics/law/news/2003/06/59043.

[21] *Id.*; Associated Press, *North Korea May be Training Hackers*, REDORBIT.COM, May 16, 2003, http://redorbit.com/news/technology/3891/north_korea_may_be_training_hackers/index.html.

[22] Daniel M. Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China*, 17 AM. U. INT'L L. REV. 641, 652–53 (2001).

[23] *Id.* at 643–45 (citing Michelle Kessler, *China Troubles Linked to Attacks on Web Sites Run By U.S. Government,* USA TODAY, May 2, 2001, at 6B*;* Lauren W. Whittington, *Pro-China Hackers Hit House Clerk's Office*, ROLL CALL, May 3, 2001, at 1; Craig S. Smith, *May 6-12; The First World Hacker War*, N.Y. TIMES, May 13, 2001, § 4 (Week in Review), at 2; *U.S./China Tit-for-Tat Hacks Escalate*, NEWSWIRE (VNU), May 1, 2001; Elizabeth Becker, *F.B.I. Warns That Chinese May Disrupt U.S. Web Sites*, N.Y. TIMES, Apr. 28, 2001, at A8; Ted Bridis, *U.S., Chinese Hackers Infiltrate Web Sites, Trade Insults Across Pacific in "Net War"*, WALL ST. J., May 1, 2001, at B6).

[24] *A Cyber-riot,* ECONOMIST, May 10, 2007, *available at* http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598.

American infrastructures, and other countries have already engaged in internationally recognized cyber attacks, it is certain that other countries will follow suit. The United States must dramatically increase its ability to respond to and engage an enemy combatant on the cyber battlefield with an organized cyber force.

United States cyber enemies are not confined to being only military-driven, but may be terrorism-driven, using cyber bombs instead of suicide bombs. Specific terrorist groups have been pinpointed as actively pursuing the capabilities of using cyberspace as a battlefield. Al-Qa'eda has been identified as building its cyber skills to use in battle against the West.[25] Al-Qa'eda uses the Internet to communicate and collaborate with its internationally-placed terrorist cells in order to unleash both physical and cyber attacks.[26] An article to which Reuters contributed affirmed al-Qa'eda's cyber-focus on November 30, 2006, by reporting an alert that al-Qa'eda may have called for cyber terrorist attacks against U.S. financial institutions during December 2006.[27] The anonymity and accessibility of cyberspace allows terrorist groups like al-Qa'eda to move and organize themselves within the confines of cafés and personal computers while planning physical and cyberspace attacks. Similar to al-Qa'eda, other international terrorist groups like the Armed Islamic Group, Aum Shinrikyo, Hizballah, and Hamas have been heightening their computer expertise.[28] Likened to a " 'cyber-jihad' war room," web sites, chat rooms, and e-mail are being used by these groups to fundraise, collaborate, and strategize future attacks.[29] For instance, in Japan, the Aum Shinrikyo cult secured access to eighty Japanese companies and ten government agencies by selling them, through a "legitimate" software

[25] *See* Barry Levine, *The Man Who Put Al-Qaeda on the Web*, NEWSFACTOR MAG. ONLINE (July 29, 2006), http://www.globalsecurity.org/org/news/2006/060729-alqaeda-web.htm (discussing two Internet innovations undertaken by al-Qa'eda, and noting that the Internet has become "invaluable" in al-Qa'eda's "war against the West").

[26] *See id.* (describing how al-Qa'eda uses the Internet to communicate and spread propaganda).

[27] Jeanne Meserve & Kelli Arena, *U.S. Warns Financial Firms of al Qaeda Threat*, CNNMONEY.COM, Nov. 30, 2006, http://money.cnn.com/2006/11/30/news/economy/al_qaeda/.

[28] *The Emergency of Cyberterrorism*, INTERNET BUS. L. SERVICES, May 1, 2005 (LEXIS).

[29] Stakelbeck, *supra* note 19; *see* Levine, *supra* note 25 (discussing al-Qaeda's use of the Internet for these purposes).

company, software laden with backdoors, which could have allowed the cult undetected cyber entry into these companies and agencies at any time.[30] Furthermore, four domestic terrorist organizations—the Hammerskin Nation, Stormfront, Aryan Nation, and National Alliance—are recognized as potentially having the technology to engage in cyber terrorism.[31]

Evidently, cyberspace is a place, a battlefield, where individuals acting on their own or in concert with a country, nation-state, or terrorist organization, may cause costly and devastating damage to the United States. Consequently, the United States needs a well-funded force that can protect its interconnected civilian and military computer networks and be victorious on the cyber battlefield. The Air Force has taken the lead in cyber battle preparations by working to form the new Air Force Cyberspace Command.[32] If this command is to be the lead military cyber force, it will need the proper resources and trained cyber warriors to defend from cyber attacks.

III. THE CYBER BATTLEFIELD

"[I] spend more time thinking about [hackers, 'cyber-vigilantes,' terrorists, and 'hostile nation-states'] in the middle of the night, than any other."[33]

Deputy Secretary of Defense Gordon England

A. Cyber Attacks Include Cyber Terrorism and Cyber Warfare, Not Cybercrimes.

A cybercrime is not a cyber attack; cyber terrorism and cyber warfare constitute cyber attacks. Within cyberspace, the intent and effects of individuals' cyber actions determine whether a

[30] *Cyberterrorism: Hearing Before the H. Comm. on Armed Services Spec. Oversight Panel on Terrorism*, 106th Cong. (2000) (statement of Dorothy E. Denning, Director, Georgetown Institute for Information Assurance at Georgetown University), *available at* http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html [hereinafter Denning].

[31] Adam Savino, *Cyber-Terrorism*, Dec. 13, 2006, *available at* http://native-resistance.blogspot.com/2006_05_23_archive.html (citing Beverly Ray & George E. Marsh II, *Recruitment by Extremist Groups on the Internet*, 6 FIRST MONDAY (2001), http://firstmonday.org/issues/issue6_2/ray/index.html).

[32] David Hendricks, *City Ideal for AF's Cyberspace Command*, SAN ANTONIO EXPRESS-NEWS, Aug. 30, 2007, at 1E.

[33] Gordon R. England, Deputy Sec'y of Def., Address at MILCOM 2006 Conference (Oct. 25, 2006), *available at* http://www.defenselink.mil/speeches/speech.aspx?speechid=1059.

terrorist, criminal, or war act has occurred. As reflected in cyber terrorism's definition—"the use of computers as weapons, or as targets, by politically motivated international, sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies"—the intent of a cyber terrorist is to force others to capitulate to demands through the acts and threats of violence.[34] Instead of promoting fundamental belief systems, in cyber warfare, the combatants are trying to achieve military objectives, and in cybercrime, the cyber criminals are fulfilling their desires for financial or psychological benefits. Rather than desiring, like a cyber terrorist, to achieve destabilization and wide-spread publicity, the cyber criminal desires to steal money or information, gain personal fame and attention, be intellectually challenged, and/or experience illicit pleasure.[35]

This difference in the participants' intentions and effects changes how these actors are dealt with. For example, some companies desire to employ, rather than imprison a hacker—a cyber criminal.[36] In fact, Panasonic hired convicted hacker Morty Rosenfeld to monitor security when he was released from prison.[37] A hacker may be recruited either to join the government's cyber warriors or to become a cyber security employee. By virtue of their "hack,"[38] hackers reveal their fighting expertise on the cyberspace battlefield. Whereas some promote a great hack as proof of expertise during a job interview for a prospective six-figure job, a large-scale act of terrorism does not attract employer interest.

Criminal law governs cybercrimes; however, as of yet, no

[34] CARLOS A. RODRIGUEZ, CYBERTERRORISM—A RISING THREAT IN THE WESTERN HEMISPHERE 7 (2006), *available at* http://library.jid.org/en/mono45/Rodriguez,%20Carlos.pdf.

[35] *See* Barry C. Collin, Inst. for Sec. and Intelligence, The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge, Remarks at the 11th Annual International Symposium on Criminal Justice Issues, http://afgen.com/terrorism1.html (last visited Apr. 11, 2008) (discussing the differences between cyber terrorists and cyber criminals).

[36] Jonathan B. Wolf, *War Games Meets the Internet: Chasing 21st Century Cybercriminals with Old Laws and Little Money*, 28 AM. J. CRIM. L. 95, 104 (2000) (citing Richard Behar, Amy Kover & Melanie Warner, *Who's Reading Your E-mail?*, FORTUNE, Feb. 3, 1997, at 56, 66).

[37] *Id.* at 104 (citing Richard Behar, Amy Kover & Melanie Warner, *Who's Reading Your E-mail?*, FORTUNE, Feb. 3, 1997, at 56, 66).

[38] "Hack" is defined as "surreptitiously break[ing] into the computer, network, servers, or database of another person or organization." BLACK'S LAW DICTIONARY (4th ed. 2004).

United States laws exist regarding response to cyber attacks, i.e., cyber warfare and cyber terrorism. The only United States guidelines, published in the National Security Presidential Directive 16, are classified.[39] Furthermore, even though the international community has acknowledged the need for some sort of regulation,[40] the international community has not implemented any such regulation.

Thus, in our post-September 11th world, although no laws exist concerning cyber attacks, the United States government is focused on thwarting not only military cyber attacks, but also cyber terrorism within cyberspace. Because cyberspace is connected to physical infrastructures, the United States government is focused on prohibiting cyber attacks against American physical infrastructures, specifically identified as "critical infrastructures" and key assets.[41]

B. Critical Infrastructures and Key Assets Connected With Cyberspace

Physical infrastructures are connected to the domain of cyberspace. Those physical infrastructures "whose incapacity or destruction would cripple the United States'[] defensive or economic security" are called critical infrastructures.[42] Critical infrastructures include: "agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and

[39] CLAY WILSON, INFORMATION WARFARE AND CYBERWAR: CAPABILITIES AND RELATED POLICY ISSUES 10 (2004), *available at* http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-6058:1 [hereinafter INFORMATION WARFARE].

[40] "In 1998 and 1999, Russia proposed that the First Committee of the U.N. explore . . . the need for arms controls for information warfare weapons." *Id.* at 11 n. 28 (citing Dorothy Denning, *Reflections on Cyberweapons Controls*, 16 COMPUTER SECURITY J. 43 (2000), *available at* http://www.cs.georgetown.edu/~denning/infosec/cyberweapons-controls.doc).

[41] JOHN ROLLINS & CLAY WILSON, CONGRESSIONAL RESEARCH SERVICE, TERRORIST CAPABILITIES FOR CYBERATTACK: OVERVIEW AND POLICY ISSUES 5 (CRS Report RL33123) (2005), *available at* http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-7633:1 [hereinafter TERRORIST CAPABILITIES].

[42] Creekman, *supra* note 22, at 655 (citing PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROT., CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES app. at A-1 (1997), *available at* http://www.fas.org/sgp/library/pccip.pdf).

postal and shipping."[43] The five most targeted critical infrastructures are information and communications, physical distribution, energy, banking and finance, and vital human services."[44] If an attack is waged against a network that is connected to one of these critical infrastructures, the security of our nation would be put at risk. For instance, in August 2003, the "Slammer" Internet computer worm was able to infiltrate via the Internet the computer systems of the Ohioan Davis-Besse power plant (an energy critical infrastructure) and to corrupt its computer control systems for approximately five hours.[45] Also, in 2002, an Australian sewage and water treatment plant was infiltrated, which resulted in "one million liters of sewage [being pumped] into the environment."[46] These particular effects attract cyber terrorists and military strategists to the cyber battlefield. If a cyber terrorist or a cyber warrior infiltrates a computer system that monitors water levels at a dam, they may alter the data to make the dam overflow, causing financial and structural damage and area-wide instability. However, a close look at these critical infrastructures reveals that mostly private entities, not the military or the government, control them.[47] As a result, Public-Private Partnerships ("PPP") regarding cyberspace are necessary in order to protect these critical infrastructures.

C. Public-Private Partnerships ("PPP") Within Cyberspace

The private sector owns and operates much of the nation's critical infrastructure.[48] "[C]ivilian high technology products and services (including communications systems, electronics, and computer software)" support the United States military "in

[43] Antolin-Jenkins, *supra* note 10, at 144 (quoting THE NATIONAL STRATEGY TO SECURE CYBERSPACE 1 (2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).

[44] Creekman, *supra* note 22, at 654–55 (citing PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROT., CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES app. at A-1 (1997), *available at* http://www.fas.org/sgp/library/pccip.pdf).

[45] Kevin Poulsen, *Slammer Worm Crashed Ohio Nuke Plant Network*, SECURITYFOCUS, Aug. 19, 2003, http://www.securityfocus.com/news/6767.

[46] JEFFREY F. ADDICOTT, TERRORISM LAW: MATERIALS, CASES, COMMENTS 278 (4th ed. 2007).

[47] Antolin-Jenkins, *supra* note 10, at 144 (citing THE NATIONAL STRATEGY TO SECURE CYBERSPACE 2 (2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).

[48] *Id.* (citing THE NATIONAL STRATEGY TO SECURE CYBERSPACE 2 (2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).

significant ways."[49] Currently, the relationship between the private and public sectors is a voluntary one. For instance, Microsoft has voluntarily created a special Security Response Center and collaborates with the Department of Defense and industry and government leaders to catch and resolve any software vulnerabilities and improve the DOD's new products.[50] Obviously, a good relationship between the private and public sectors augments national security. For example, the assurance of confidential communications encourages businesses to report cyber attacks because businesses do not have to fear monetary loss from negative publicity and public embarrassment.[51] Confidential communications between business and the government could allow the government to learn about new cyber techniques or vulnerabilities, and, if needed, to act promptly. Thus, victory on this battlefield of ones and zeros relies on a coordinated and balanced relationship between the private and public sectors, and on trained cyber warriors who know how to position themselves and engage in offensive and defensive maneuvers within cyberspace.

D. The Weapons of Cyber Warfare

Cyber warriors, in order to offensively and defensively maneuver in cyberspace, use cyber weapons. Cyber weapons are not traditional warfare weapons. Combatants within the cyber domain may choose between four types of cyber weapons: (1) syntactic, (2) semantic, (3) mixed, and (4) electromagnetic.[52]

---

[49] COMPUTER ATTACK, *supra* note 15, at 1 (citing Interview by Wanja Eric Naef with Dan Kuehl, Professor of Sys. Mgmt., Nat'l Def. Univ., in London, Gr. Brit. (July 2003), *available at* http://www.iwar.org.uk/infocon/print/io-kuehl.htm).

[50] *Information Technology in 21st Century Battlespace: Hearing Before the Subcomm. on Unconventional Threats and Capabilities of the H. Comm. on Armed Services*, 108th Cong. 22–23 (2003) (statement of Scott Charney, Chief Security Strategist, Microsoft), *available at* http://commdocs.house.gov/committees/security/has205260.000/has205260_0.HTM#24.

[51] *Cf.* Sam Costello, *FBI: Cybercrime on the Rise, But Few Victims Report It*, NETWORKWORLDFUSION, Apr. 8, 2002, http://www.networkworld.com/news/2002/0408cybercrime.html (reporting that thirty-four percent of the organizations surveyed in the Seventh Annual Computer Crime and Security Survey, which was conducted by the Computer Security Institute and the San Francisco Bureau of the FBI, had not reported security breaches to law enforcement, and, of these, "[seventy percent] cited negative publicity as a reason for their silence").

[52] Antolin-Jenkins, *supra* note 10, at 139 (citing Susan W. Brenner & Marc

Syntactic weapons include "malicious code[s]," such as viruses, worms, Trojan horses, and spyware, that target a computer's operating system.[53] On the other hand, semantic weapons "target . . . the accuracy of the information to which the computer user has access."[54] Since cyber warfare is data-dependent, misinformation may be undetectable and cause incalculable damage. For example, misinformation may indicate official withdrawal requests from accounts when none were actually submitted, causing losses of billions of dollars. Mixed weapons combine syntactic and semantic weapons to attack both information and the computer's operating system.[55] An example of a mixed weapon is a "'bot network'" or "'bot herd,'" which is a group of "bots." Bots are remote-controlled or semi-autonomous computer programs that infect computers.[56] The hacker who controls the bots may spy, copy and transmit sensitive data, and organize the bots in a swarm attack against targeted computers.[57] Finally, the electromagnetic weapon is used "to overload computer circuitry" with a blast of electromagnetic energy.[58] The tactics and goals of the combatant determine which of these weapons are used.

E. The Tactics of Cyber Warfare

Three specific time frames exist in reference to offensive and defensive tactical cyber operations: before, during, and after the attack. Throughout the "before" stage, combatants assess the vulnerabilities and risks of the cyber battlefield, usually with network meetings in cyberspace and extensive reconnaissance and pre-operative surveillance.[59] The combatant on the defensive searches for vulnerable points of entry so that protective measures may be prioritized.[60] The combatant on the offensive

D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 U. ILL. J.L. TECH. & POL'Y 1, 27–42 (2002)) (discussing the three types of attacks on computer systems); Rodriguez, *supra* note 34, at 8–9 (discussing methods of attacking computer systems, including use of electromagnetic energy).

53 Antolin-Jenkins, *supra* note 10, at 144.

54 *Id.* at 140.

55 *Id.* at 141.

56 COMPUTER ATTACK, *supra* note 15, at 13.

57 *Id.*

58 *Id.* at 3.

59 *Id.* at app. A at 36, app. C at 42.

60 *Cf.* Denning, *supra* note 30 (noting that it is "effectively impossible" for computer security programs to eliminate all computer system vulnerabilities).

scans for vulnerable points of entry in order to complete the mission.[61] "During" an attack, the combatants gain and maintain access to exploit vulnerabilities and may utilize swarming methods.[62] Then, "after" the battle, the combatants quickly attempt to restore or maintain their newly conquered cyber territory and cover their tracks.[63] These tactics can be applied regardless of the type of attack launched.[64]

F. The Attacks on the Cyber Battlefield

Cyber fighters may unleash at anytime one of three attacks on the cyber battlefield: a cyber attack, a physical attack, and/or an electromagnetic attack.[65] In a cyber attack, the cyber warrior or cyber terrorist, using syntactic or semantic cyber weapons, attacks computer networks "to disrupt equipment operations, change processing control[s], or corrupt stored data."[66] From mildest to most severe, these attacks may include web vandalism (the deactivation or defacing of government or military web pages); disinformation campaigns (the spreading of error or rhetoric in cyberspace to influence the public's beliefs or psychology); gathering secret data (cyber espionage); disruption in the field (blocking, intercepting, or polluting communications that endanger the lives of soldiers); and attacking critical infrastructure (physically endangering civilians via a cyber attack).[67] In a physical attack, the cyber warrior uses conventional weapons.[68] For example, cruise missiles may be used to "scatter carbon filaments [in order to] short circuit[] power supply lines."[69] In an electronic attack, the combatant uses "an electromagnetic pulse (EMP) to overload computer circuitry" or a syntactic weapon on a microwave radio

61 COMPUTER ATTACK, *supra* note 15, at app. A at 36–37, app. C at 42.

62 *Id.* at 13, app. A at 37–38, app. C at 42.

63 *See id.* at app. A at 37 (explaining that an attacker can control a computer or network, construct ways to keep other hackers out, and use programs to avoid detection).

64 *See generally id.* at 13, app. A at 36–37 (explaining that an attack on networked computers could be accomplished by following certain steps used by hackers, and describing these steps).

65 *Id.* at 2–3.

66 *Id.* at 2.

67 LINDA A. MOONEY, DAVID KNOX & CAROLINE SCHACHT, UNDERSTANDING SOCIAL PROBLEMS 491 (5th ed. 2005).

68 COMPUTER ATTACK, *supra* note 15, at 2.

69 *Id.* at 3 (noting that the U.S. military reportedly used cruise missiles for this purpose during Operation Desert Storm in 1991).

transmission.[70] These attacks are successful because of vulnerabilities within the cyber battlefield.

G. Vulnerabilities Within the Cyber Battlefield

The reason the cyber battlefield exists is because vulnerabilities exist and can be exploited. If no vulnerabilities existed, there would be no need for protection against cyber attacks. The following is a non-exhaustive laundry list of ten vulnerabilities of which combatants take advantage on the cyber battlefield. First, in many scenarios, the enemy remains unidentified.[71] As a result, the injured party does not know whom to exact recourse against. Second, many computer security incidents, as many as eighty percent, remain unreported.[72] Corporations or other entities refrain from reporting because the ramifications of public discovery of the cyber invasion may cause reputation and profit loss.[73] As of yet, no law mandates a private entity to report cyber security violations. Consequently, if the public and private sectors cannot collaborate when cyber invasions occur because of the lack of reporting, protective measures cannot be prioritized nor implemented. Third, anyone can obtain "[s]tep-by-step hacking instructions" on the Internet.[74] This indiscriminate availability of how-to-hack instructions empowers and entices more cyber combatants. Fourth, a hackers' black market exists wherein anyone may purchase information on computer vulnerability.[75] For instance, as early as 1998, a member of Harkat-ul-Ansar, a "militant Indian separatist group," attempted to purchase cyber

[70] *Id.*

[71] *Id.* at 5–7.

[72] *Id.* at 7 (citing *Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD: Hearing Before the Subcomm. on Terrorism, Unconventional Threats and Capabilities of the H. Comm. on Armed Services*, GAO-03-1037T (2003), at 6 (statement of Robert F. Dacey, Dir., Info. Sec. Issues), *available at* http://www.gao.gov/new.items/d031037t.pdf [hereinafter *Information Security*]).

[73] *See id.* (noting that attacks are unreported due to the "potential liability concerns" of commercial enterprises).

[74] Creekman, *supra* note 22, at 648 (citing Michael Specter, *The Doomsday Click: How Easily Could a Hacker Bring the World to a Standstill?*, THE NEW YORKER, May 28, 2001, at 101, 105).

[75] *See* Bob Francis, *Know Thy Hacker: the Dollars and Cents of Hacking*, INFOWORLD, Jan. 28, 2005, http://www.infoworld.com/article/05/01/28/05OPsecadvise_1.html (noting that hackers may exploit hacks for themselves or sell the information they obtain to others on the black market).

attack software from hackers.[76] Accordingly, cyber vulnerabilities are a commodity, which entices free-lance hackers to discover and sell cyber vulnerability information instead of, in good faith, notifying the proper authorities and desiring to work full-time in a cyber security field. As a result, many consider hackers to be the greatest cyber security threat.[77] Fifth, offshore outsourcing relating to computer technology and equipment has become a common trend with corporations.[78] Consequently, the nation's security may be jeopardized by foreigners knowing how our computer systems are built. Sixth, the cyber sophistication of terrorists groups has increased.[79] Seventh, poor design leaves a network exposed to attack.[80] A syntactic attack may be conducted against a computer that has a faulty system configuration, old to no antivirus protection, a mis-configuration, or a pre-existing system flaw.[81] In fact, delays in release or lack of security patches for these flaws heighten vulnerability because potential combatants may become aware of the vulnerability and attack before it may be patched.[82] Reportedly, on 199 occasions in 1994, hackers infiltrated the Department of Energy's computers because the security flaws had not been patched.[83]

---

[76] Denning, *supra* note 30.

[77] *See 2004 E-Crime Watch Survey Shows Increase in Electronic Crimes*, GOV'T TECH., May 26, 2004, http://www.govtech.com/gt/90400 (reporting that forty percent of the surveyed "security and law enforcement executives" regarded hackers as "the greatest cyber security threat" to their organizations).

[78] COMPUTER ATTACK, *supra* note 15, at 16 (citing Patrick Thibodeau, *Offshore Outsourcing is Relentless*, COMPUTERWORLD, June 27, 2003, http://www.computerworld.com/careertopics/careers/story/0,10801,82578,00.html).

[79] *See Information Security*, *supra* note 72, at 5–6 ("According to the FBI, terrorists . . . are quickly becoming aware of and using information exploitation tools . . . that can destroy, intercept, degrade the integrity of, or deny access to data.").

[80] *See* COMPUTER ATTACK, *supra* note 15, at 15 (citing *Cyber Security—Growing Risk from Growing Vulnerability: Hearing Before the Subcomm. on Cybersecurity, Science, and Research and Development of the H. Select Comm. on Homeland Security* (2003) (statement of Richard D. Pethia, Dir., CERT Centers), *available at* http://www.cert.org/congressional_testimony/Pethia_testimony_06-25-03.html) (noting the lack of improvement in the security features of many products).

[81] COMPUTER ATTACK, *supra* note 15, at 5.

[82] *See SANS Top-20 Internet Security Attack Targets (2006 Annual Update)*, SANS INSTITUTE, Nov. 15, 2006, http://www.sans.org/top20/ (citing specific examples of codes being exploited before patches were created for program vulnerabilities).

[83] COMPUTER ATTACK, *supra* note 15, at 22 (citing Wilson P. Dizard III, *DOE Hacked 199 Times Last Year*, GCN, Sept. 30, 2004,

Eighth, operator error creates vulnerabilities. If there are poor security practices and procedures or inadequate security training, obviously the computer system may be left exposed to an attack.[84] Ninth, uncontrollable circumstances such as physical destruction due to natural causes (e.g., earthquakes and lightening) may expose a nation to cyber harm. For example, an earthquake in Taiwan left millions in China, Hong Kong, Japan, South Korea, and Taiwan, without Internet services, vital to businesses, for two days.[85] Tenth, a cyber attack can be very inexpensive for the attacker. For example, a single university student in the Philippines built and unleashed the "Love Bug" virus, which cost computer users "billions of dollars."[86] The low entry cost of cyberspace appeals to nations, criminals, and terrorist organizations that cannot outmatch or inflict harm upon the United States in an alternative manner.[87] However, even after governmental acknowledgement of the danger of cyber attacks, some disagree as to whether a coordinated cyber attack against critical infrastructures would be harmful.

H. The Debate on the Effects of a Cyber Attack

Even though the government has recognized and supported the

http://www.gcn.com/online/vol1_no1/27489-1.html?topic=daily-updates; U.S. DEPT. OF ENERGY, OFFICE OF INSPECTOR GEN., OFFICE OF AUDIT OPERATIONS, DOE/IG-0662, EVALUATION REPORT: THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM—2004 6 (2004), *available at* http://www.ig.energy.gov/documents/CalendarYear2004/ig-0662.pdf).

[84] COMPUTER ATTACK, *supra* note 15, at 6, 14 (citing *The Top 20 Most Critical Internet Security Vulnerabilities*—(2003–2004 Archive), SANS INSTITUTE, Oct. 8, 2003, http://www.sans.org/top20/2003/).

[85] Donald Greenlees & Wayne Arnold, *Repairs on Network Cables in Asia Could Take Days*, N.Y. TIMES, Dec. 28, 2006, *available at* http://www.nytimes.com/2006/12/28/business/worldbusiness/28cnd-connect.html?ex=1324962000&en=14f330f05e287e6b&ei=5088&partner=rssnyt&emc=rss; *see also Taiwan Tremors Cripple Internet, Phone Services*, CBC NEWS, Dec. 27, 2006, http://www.cbc.ca/world/story/2006/12/27/taiwan-telecom-061227.html ("[C]onnections [were] cut off to China, Japan and other parts of Southeast Asia").

[86] *Philippine Officials Charge Alleged 'Love Bug' Virus Creator*, CNN.COM, June 29, 2000, http://archives.cnn.com/2000/TECH/computing/06/29/philippines.lovebug.02/index.html.

[87] *See* C. Todd Lopez, *Senior Leaders Discuss Fighting in Cyberspace*, INTERCOM, Nov. 2006, at 18, *available at* http://public.afca.af.mil/shared/media/document/AFD-061220-041.pdf (stating low cost makes cyberspace "extremely attractive to nations, criminal and terrorist organizations who could not possibly attack the United States symmetrically.").

identification and implementation of protective measures for the United States' cyber domain, some contend that a cyber attack would only produce a limited breadth of damage. One rationale is that the "cascade" effect of international economic interdependency would likely deter attacks on financial programs. For example, the fact that other world markets would be damaged if the United States' economy was damaged, via the cascade effect of international economic interdependency, deters cyber attacks against the United States' financial programs.[88] However, this reasoning does not correspond to the reality that there are enemies of the United States who reject the very notion of a global economy, and do not care about the possible cascade effect on other untargeted countries.[89] Another reason proposed for this "minimized effect" stance is that a cyber attack is not comparable to a physical attack because a cyber attack would only result in "inconvenience and inefficiency."[90] For example, some people reason that it is easier to inflict death on a large scale with a physical attack versus a cyber attack.[91] Yet, the unpredictable consequences and unexpected adversarial advantages achieved from a cyber attack may do more damage than a physical attack.[92] Finally, it is reasoned that nuclear,

[88] *See* COMPUTER ATTACK, *supra* note 15, at 7, n.26 (noting that China may be deterred from employing cyber-attacks against the United States, because "China is as dependent on the same financial markets as the United States, and could suffer even more from disruption."); *see also* Robert Lemos, *What Are the Real Risks of Cyberterrorism?*, ZDNET NEWS, Aug. 26, 2002, http://news.zdnet.com/2100-1009_22-955293.html (reporting that Stash Jarocki, Chairman of Financial Services ISAC, stated that financial services are interrelated, such that a cyberattack on one would effect them all).

[89] COMPUTER ATTACK, s*upra* note 15. at 7 n.26 (citing James A. Lewis, Center for Strategic & International Studies, *Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats*, Dec. 2002, at 8, http://chnm.gmu.edu/cipdigitalarchive/files/292_CSISAssessingtheRisksofCyberTerrorismLewis2002.pdf).

[90] Antolin-Jenkins, *supra* note 10, at 145 (citing James A. Lewis, Center for Strategic & International Studies, *Assessing the Risks of Cyberterrorism, Cyber War and Other Cyber Threats,* Dec. 2002, at 5–6, http://chnm.gmu.edu/cipdigitalarchive/files/292_CSISAssessingtheRisksofCyberTerrorismLewis2002.pdf).

[91] *E.g.*, Joshua Green, *The Myth of Cyberterrorism: There are Many Ways Terrorists Can Kill You—Computers Aren't One of Them*, WASH. MONTHLY, Nov. 2002, *available at* http://www.washingtonmonthly.com/features/2001/0211.green.html.

[92] *See, e.g.*, *id.* (quoting the cyber security czar, Richard Clarke, who stated that "if an attack comes today with information warfare . . . it would be much, much worse than Pearl Harbor.").

biological, and chemical threats are greater than cyber threats.[93] Regardless, these other threats do not eliminate the actuality of damage from a cyber attack; therefore, other threats, such as nuclear, biological, or chemical should not displace protective measures. Accordingly, since 1996, the United States government has taken a proactive stance toward establishing national cyber security,[94] and this organizational history confirms the support Congress would have in establishing the Cyber Force.

IV. CYBER SECURITY HISTORY

Pre- and post-September 11th cyber security history reveals actions the United States government has taken to protect the United States from cyber attacks. Presidential Directives, Executive Orders, Legislation, and agency policies have supported cyber security research and groups.[95] As a result, many government entities, such as the Department of Defense ("DOD"), Federal Bureau of Investigation ("FBI"), Department of Homeland Security ("DHS"), and the Secret Service, have cyber teams.[96] However, with the recent creation of the Air Force's Cyber Command,[97] Congress needs to ready itself for the next historical step that will pull all cyber resources into a separate military branch with which the other branches and other government entities will have an interdependent relationship.

V. THE AIR FORCE

"The Mission of the Air Force is to deliver sovereign options for the defense of the United States of America and its global interests— to fly and fight in Air, Space and Cyberspace." [98]

In the movement to establish national cyber security, the Air Force has emerged as a leader. The Air Force has earned a reputation as a pioneer of new territories over the years. Seventy years ago, it advanced into the air; fifty years ago, space; now,

[93] *See id.* (quoting Georgetown University Computer Science Professor Dorothy Denning, who stated that "[cyberterrorism] [does] not rank alongside chemical, biological, or nuclear weapons . . . ").

[94] *See infra* apps. A–B.

[95] *See infra* apps. A–B.

[96] *See infra* apps. A–B.

[97] Lopez, *8th Air Force to Become New Cyber Command*, *supra* note 7.

[98] Wynne, *supra* note 9.

cyberspace.[99] Admirably, the Air Force took President George W. Bush's *National Strategy to Secure Cyberspace*[100] seriously, and, recognizing that its activities are critically intertwined with cyberspace, it made significant internal structural changes.[101] The most apparent difference involves General Moseley and Secretary Wynne changing the Air Force Mission Statement, as of December 5, 2005, to read: "to deliver sovereign options for the defense of the United States of America and its global interests—to fly and fight in Air, Space and Cyberspace."[102] Accordingly, the cornerstone of the Air Force's military doctrine now includes computers: " 'Command', Control' [sic], 'Computers', . . . Communication',[sic] . . . 'Intelligence', 'Surveillance' and 'Reconnaissance'."[103] Thus, the Air Force has officially extended its military reach into cyberspace. This official expansion reveals that the Air Force understands that the same "[c]riminal, [p]irate, [t]ransnational, and [g]overnment-[s]ponsored" trouble the military "contend[s] with in the [d]omains of [l]and, [s]ea, [a]ir, and . . . [s]pace" exists within cyberspace and that internal institutional changes must reflect this revelation.[104]

Correspondingly, within a year of the release of its new mission statement, the Air Force made internal institutional changes. In January 2006, the Air Force formed "a Cyberspace Task Force . . . [to be] led by military strategist Doctor Lani Kass."[105] As the Cyberspace Task Force gathered and analyzed data concerning cyberspace, thirty-five college students ("[nineteen] Air Force cadets, three from the Army, two from the Navy, eight National Science Foundation Fellows and four civilians"), from twenty-eight states, graduated in August from a four-credit hour Advanced Course in Engineering Cyber Security Boot Camp offered through Syracuse University's L.C. Smith

---

99 David Thompson, *Cyber Command: The New Frontier*, SATELLITE FLYER, Nov. 22, 2006, available at http://www.csmng.com/images/satelliteflyer/satelliteflyer_2006-11-22.pdf.

100 THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE ix (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

101 *See* C. Todd Lopez, *Plan for Cyberspace Available in Near Future*, AIR FORCE PRINT NEWS, Sept. 5, 2006, *available at* http://www.af.mil/news/story_print.asp?id=123026382 (discussing changes made by the Air Force to comply with federal mandates).

102 Wynne, *supra* note 9.

103 *Id.*

104 *Id.*

105 *Id.*

College of Engineering and Computer Science.[106] Then, on November 2, 2006, the Secretary of the Air Force, Michael W. Wynne, announced the 8th Air Force as the new Cyberspace Command to be led by Lt. Gen. Robert J. "Bob" Elder Jr.[107] Within a year, the Air Force quickly made institutional changes to accommodate the need to have an official "24/7/365" military presence in cyberspace.[108] Without a doubt, the Air Force has officially claimed cyberspace as its territory. However, these pioneering actions do not preclude a separate military branch, but, in fact, reveal that the creation of the Cyber Force is inevitable.

A. A New Military Branch (the "Cyber Force") Should Be Formed

History, job security, and economics dictate that a new military branch, the "Cyber Force," should be formed. The U.S. Constitution grants Congress the express power to fund and raise an army.[109] As a result, in 1947, Congress passed, and the President signed into law, the National Security Act of 1947, which created the Department of the Air Force.[110] This legislation officially separated what used to be called the United States Army Air Corps from the United States Army into its own separate military branch and renamed it.[111] Congress did this after World War II, which demonstrated "the critical importance of air power to the defense of our Nation."[112] This reflects exactly what probably will happen concerning the new Cyberspace Command of the 8th Air Force. Congress, in recognition of "the critical importance of [cyber-power] to the defense of our Nation,"[113] could potentially rename and separate what used to

[106] Francis L. Crumb, *Cyber Security Boot Camp Graduates Class of 2006*, AIR FORCE PRINT NEWS, Aug. 14, 2006.

[107] Lopez, *8th Air Force to Become New Cyber Command*, *supra* note 7.

[108] Breanne Wagner, *Cyberspace Fly and Fight Made Clear*, AIR FORCE MAG., Sept. 26, 2006, *available at* http://dailyreport.afa.org/AFA/Features/organization/box092606cyber.htm?pf=true.

[109] U.S. CONST. art. 1, § 8, cl. 12.

[110] 50 U.S.C. § 401 (2006).

[111] Air Force Historical Studies Office, Evolution of the Department of the Air Force, https://www.airforcehistory.hq.af.mil/PopTopics/Evolution.htm (last visited Apr. 11, 2008); Army Air Forces Historical Association, http://www.aafha.org/ (last visited Apr. 11, 2008).

[112] Press Release, Bill Clinton, President, 50th Anniversary of the National Security Act of 1947 (Sept. 15, 1997), *available at* http://clinton4.nara.gov/WH/EOP/NSC/html/50thanniv.html.

[113] *Id.*

be called the Air Force's Cyberspace Command to its own separate military branch—the Cyber Force.

Additionally, the military, not just the Air Force, has the need, structure, and resources to build and maintain a permanent Cyber Force. There are six reasons (not exhaustive) that support this premise. First, the Army, Navy, Air Force, and Marines are interdependent.[114] This interdependency extends into cyberspace. "[D]efending and fighting in the Cyber Domain is absolutely critical to maintain operations in Ground, Sea, Air and Space."[115] As a result, every branch of the military needs specially trained cyber warriors to aid in attacks.[116] Instead of each branch creating its own cyber division, all cyber resources should be concentrated in one branch, which will provide cyber specialists to the other branches. Similar to the fact that the army specializes in land battles and the navy specializes in sea battles, and both aid the other branches when needed, the Cyber Force should be a separate military branch that specializes in cyberspace battles and aids the other branches when needed.

The military offers stability, which will hopefully strengthen the nation's cyber security. Since January 2003, within the DOH, three cyber security advisors to the President (Richard Clarke, Howard Schmidt, and Amit Yoran) have resigned.[117] This instability of leadership hurts the vision, effectiveness, and direction of the United States cyber security. Also, the stability of a military career in cyber warfare will attract talent. Free-lance hackers who live unstable "cloak and dagger" lifestyles with the law will enjoy being able to do legally what they love, and others will be able to specialize in cyber security and related fields, thereby countering the world-wide shortage of cyber experts.[118]

Third, the financial and technological resources of the military allow the military to be competitively up-to-date with computer

---

114 *See Review of the Defense Authorization Request for Fiscal Year 2008 and the Future Years Defense Program: Hearing Before the Personnel Subcomm. of the S. Comm. on Armed Services*, 110th Cong. (2007) (statement of David S. C. Chu, Undersecretary of Defense for Personnel and Readiness) (remarking upon the interdependency of the military branches).

115 Wynne, *supra* note 9.

116 *See id.*

117 COMPUTER ATTACK, *supra* note 15, at 28.

118 *See* James Kilner, *Bill Gates Says West Not Supplying Enough IT Talent*, REUTERS, Nov. 7, 2006, http://www.reuters.com/article/technologyNews/idUSL0779951320061107 (reporting that Microsoft Chairman Bill Gates stated, "There is a shortage of IT skills on a worldwide basis.").

technology's advances.[119] The generous funding of the military[120] would allow the Cyber Force to remain competitive with technological advances.

Fourth, the military has already both offensively and defensively engaged in cyber battles, and the number of cyber attacks has increased.[121] During the NATO air campaign over Kosovo, the United States attempted to launch electronic attacks on Serbian computer networks.[122] Apparently, the military needs cyber warriors, and creating a separate military force will help to concentrate expertise and funding in a branch formed for longevity.

Fifth, as the Air Force assesses what it needs to deter, guard, rescue, strike, and access in preparation for a 21st Century Cyber War, it will soon realize that the Cyber Force will need separate funds, warriors, facilities, and schooling in order to aid all the branches and wage war on the cyber battlefield.[123] Quite possibly, competition for personnel and funding will create infighting within the Air Force. As a separate branch, the Cyber Force's funding would be guarded and the cyber warriors' career paths would be clear. Additionally, the Cyber Force, in order "to detect, deter, deceive, disrupt, defend, deny, and defeat any signal or electron transmission,"[124] will require versatile cyber warriors who will be able to protect the other military branches. The branch will need "cultural experts, intelligence officers,

---

[119] *See* Joe Pavlat, *Telecom Technology and the Military: Initiatives and Standards*, *in* MILITARY EMBEDDED SYSTEMS RESOURCE GUIDE 6 (2005), *available at* http://www.mil-embedded.com/columns/industry_analysis/pdfs/MES.2005.May.Industry_Analysis.Pavlat.pdf (discussing the military's ability to adopt continuously advancing information technology).

[120] *See* Kei Koizumi, *R&D in the FY 2007 Department of Defense Budget*, *in* AAAS REPORT XXXI: RESEARCH AND DEVELOPMENT FY 2007 (2006), http://www.aaas.org/spp/rd/07pch6.htm.

[121] *See* COMPUTER ATTACK, *supra* note 15, at 8 (noting an increase in cyber attacks against military networks between 2001 and 2004).

[122] *U.S. Spy Chief: Cyberspace a Potential Battlefield*, CNN.COM (Oct. 17, 2000), http://archives.cnn.com/2000/TECH/computing/10/17/tech.Internet.security.reut/index.html.

[123] *See* C. Todd Lopez, *Air Force Leaders to Discuss New 'Cyber Command*,' AIR FORCE PRINT NEWS, Nov. 5, 2006, *available at* http://www.8af.acc.af.mil/news/story.asp?id=123031988 (describing the reasons behind the creation of the Cyber Command, and noting logistical considerations that need to be taken into account); *see also* Wynne, *supra* note 9 (discussing, *inter alia*, strategic responses to current threats in cyberspace and future steps to be taken).

[124] Lopez, *supra* note 123 (describing "the essence of fighting in cyberspace").

electronic warfare officers, and lawyers,"[125] who not only understand the different military branches' culture and objectives, but also are experts in their respective fields and cyberspace.

Sixth, the fact that other nations, such as China, may be building a separate military branch[126] indicates that the United States will have to have a specific military force, supplied with all resources necessary to battle another country's military. Obviously then, the Cyber Force is part of the United States' future. Because of the aforementioned reasons, the Cyber Force is best placed within the military as a separate branch. As a result, Congress should prepare to create a new military branch: the Cyber Force. "In the hands of a technologically advanced military, the Internet becomes a new weapon, potentially as powerful and disruptive as a nuclear explosion."[127]

B. Concerns of a Separate Military Branch

Even though a strong case exists for a separate military branch—the Cyber Force—concerns still exist in reference to its formation. One large concern is how an official military branch would affect the voluntary relationship between the private and public sectors. Of course, the military will work towards a coordinated and balanced relationship with the private sector, but most likely the FBI, with its INFRAGARD program,[128] and DHS with its National Cyber Security Division,[129] will handle the bulk of private sector issues. And just as the military may have to occupy land in times of war;[130] the Cyber Force may have to occupy a company's cyberspace in times of cyber war. The extent of this occupation will need to be determined in the next few years.

Another concern is that a military Cyber Force may invoke an analogous situation to that of the National Security Agency's ("NSA") wiretapping program.[131] Under the guise of national

---

[125] Wagner, *supra* note 108 (describing the needs of the Air Force's cyber command).

[126] Creekman, *supra* note 22, at 652–53.

[127] *Id.* at 680 (citing Warren P. Strobel et al., *A Glimpse of Cyberwarfare*, U.S. NEWS & WORLD REP., Mar. 13, 2000, at 32).

[128] *See infra* app. A.

[129] *See infra* app. B.

[130] *See* 10 U.S.C. § 2663 (2007) (providing that the military may petition to take land for use in war or preparation for war).

[131] *See* Bill Mears & Andrea Koppel, *NSA Eavesdropping Program Ruled*

security, the question remains: would our military be able to invade, without oversight, the privacy of United States citizens? A third concern is whether the Cyber Force would compromise national security because the military relies on foreign-owned businesses to provide critical defense expertise, products, and technology.[132] Other countries may not only purchase similar products and, therefore, test and practice on the same systems the United States has, but might also embed code within the systems that would allow them undetectable access.

As a result of the United States Government's cyber security history, not only the Air Force, but also different government entities—the Secret Service, FBI, DHS, DOD, the Homeland Security Council ("HSC"), the Office of Management and Budget ("OMB"), and other federal agencies—have cyberspace roles.[133] When considering whether to create a separate military branch, a concern exists over whether the roles of these government entities will clash with the separate military branch. Based upon the expressed purpose of these government entities, a clash should not exist. The Secret Service's role is to prevent, detect, and investigate electronic crimes, such as child pornography, not wage electronic attacks, such as a semantic attack against the coordinates of a target.[134]Similar to the Secret Service, the FBI deals with cyber crimes, as revealed by its four-fold cyber mission.[135] The DHS's National Cyber Security Division ("NCSD") works with public, private, and international entities

Unconstitutional, CNN.COM, Aug. 17, 2006, http://www.cnn.com/2006/POLITICS/08/17/domesticspying.lawsuit/index.html (reporting that the disclosure of the NSA's warrantless electronic surveillance led to widespread criticism).

[132] *Id.*

[133] *See infra* apps. A–B.

[134] United States Secret Service Mission Statement, http://www.secretservice.gov/mission.shtml (last visited Apr. 11, 2008); United States Secret Service: Criminal Investigations, http://www.secretservice.gov/criminal.shtml (last visited Apr. 11, 2008).

[135] The FBI's cyber mission is four-fold: first and foremost, to stop those behind the most serious

> computer intrusions and the spread of malicious code; second, to identify and thwart online sexual predators who use the Internet to meet and exploit children and to produce, possess, or share child pornography; third, to counteract operations that target U.S. intellectual property, endangering our national security and competitiveness; and fourth, to dismantle national and transnational organized criminal enterprises engaging in Internet fraud.

Federal Bureau of Investigation, Cyber Investigations, http://www.fbi.gov/cyberinvest/cyberhome.htm (last visited Apr. 11, 2008).

to secure cyberspace.[136] Additionally, the Cyber Force most likely will hold a position on the Homeland Security Council,[137] which will facilitate information sharing between the different government entities and direct contact with the President on cyber security issues. Similarly, the Cyber Force and the Department of Defense will help, rather than detract from, each other's objectives because the DOD's Joint Information Operations Center focuses on integrating "Information Operations (IO) into military plans and operations . . . ."[138] The Office of Management and Budget oversees the federal agencies' assessment and implementation of cyber security measures,[139] which does not overlap with military oversight. Consequently, the concerns regarding a separate military branch will be worked out over time as the legislative, executive, and judicial branches involve themselves in its creation.

VI. CONCLUSION

The United States does not want its own household and business computers to be used against it in a cyber attack. As a result, the government has prioritized the securing of cyberspace, an internationally acknowledged battlefield. During this process, the Air Force took the lead in developing an official cyber military force under its 8th Air Force division.[140] Just as the Air Force initially grew under the Army's umbrella,[141] the Cyber Force will grow under the Air Force's wings. Eventually, the Cyber Force will need to become a separate military branch because of cyberspace's international use as a battlefield that directly affects households, corporations, universities, governments, military, and critical infrastructures. Congress, get ready to create a new military branch: the Cyber Force.

---

[136] DHS: National Cyber Security Division, http://www.dhs.gov/xabout/structure/editorial_0839.shtm (last visited Apr. 11, 2008).

[137] *See infra* notes 148–150 and accompanying text.

[138] Service & Joint Information Operations, Air University, http://www.au.af.mil/info-ops/joint.htm (last visited Apr. 11, 2008).

[139] Exec. Order No. 13,231, 66 Fed. Reg. 53,063 (Oct. 16, 2001).

[140] Lopez, *8th Air Force to Become New Cyber Command*, *supra* note 7.

[141] *See generally*, *Air Force History Overview*, AIR FORCE LINK, http://www.af.mil/history/overview.asp (last visited Apr. 11, 2008) (providing a brief history of how the Air Force grew out of the U.S. Army).

VII. APPENDIX A: PRE-SEPTEMBER 11TH CYBER SECURITY HISTORY

A. July 1996: President's Commission on Critical Infrastructure Protection ("PCCIP")

The Clinton Administration acknowledged the need to protect the United States' critical infrastructure and began the process with PCCIP. President Clinton tasked the commission to report to the President

> the scope and nature of the vulnerabilities of, and threats to, [the nation's] critical infrastructures; determine what legal and policy issues are raised by efforts to protect critical infrastructures . . . ; recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures . . . ; [and] propose any statutory or regulatory changes necessary to effect its recommendations . . . .[142]

In 1997, the PCCIP released its report in which it found no immediate threat to the nation's critical infrastructure, but did support action concerning cybersecurity.[143] PCCIP's report influenced President Clinton's Presidential Decision Directive No. 63.

B. 1998: Presidential Decision Directive No. 63 ("PDD-63")

President Clinton's PDD-63 Directive focused on protective measures against both physical and cyber attacks. It was an ambitious plan that set the year 2003 as a national deadline for the United States to be able to protect its critical infrastructures.[144] However, after September 11th, the Bush administration established the Department of Homeland Security, which either dissolved or adopted what PDD-63 created.[145]

---

142 Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 15, 1996).

143 PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROT., CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES x (1997), *available at* http://chnm.gmu.edu/cipdigitalarchive/files/5_CriticalFoundationsPCCIP.pdf.

144 Press Release, Office of the Press Sec'y, Fact Sheet: Protecting America's Critical Infrastructures: PDD 63 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd-63.htm.

145 *See Hearing Before the H. Energy & Commerce Subcomm. on Oversight and Investigations* 107th Cong. (July 9, 2002) (statement of John S. Tritak, Dir.,

C. The FBI's INFRAGARD Program

Certain programs already established within departments/agencies, such as the FBI's INFRAGARD Program still exist, even after September 11th. The FBI's INFRAGARD program serves both the government and the private sector as a source of warning and information regarding cyberattacks.[146] It works with DHS in order to protect the nation's critical infrastructures.[147]

VIII. APPENDIX B: POST-SEPTEMBER 11TH CYBER SECURITY HISTORY

A. October 8, 2001: Executive Order 13228 ("EO-13228")—Office of Homeland Security

President Bush, through EO-13228, established the Office of Homeland Security ("OHS") and the Homeland Security Council ("HSC").[148] The purpose of OHS was to secure the United States' critical infrastructure and ensure a rapid restoration after a terrorist threat or attack.[149] The HSC still exists as an advisory council to the President concerning homeland security.[150]

B. October 16, 2001: Executive Order 13231 ("EO-13231")—Defined U.S. Policy

In EO-13231, President Bush defined United States policy as "to protect against disruption of the operation of information systems for critical infrastructure . . . , and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible."[151] Subsequent amendments abolished the President's Critical Infrastructure Protection Board and minimized the influence of

Critical Infrastructure Assurance Office, Bureau of Indus. and Sec., U.S. Dep't of Commerce), *available at* http://www.ogc.doc.gov/ogc/legreg/testimon/107s/tritak0709.htm.

146 The History of InfraGard, http://www.infragardphl.org/resources/InfraGard_History.pdf (last visited Apr. 11, 2008).

147 *Id.*

148 Exec. Order No. 13,228, 66 Fed. Reg. 51,812, 51,816 (Oct. 8, 2001).

149 *Id.* at 812–14.

150 JOHN D. MOTEFF, CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY, AND IMPLEMENTATION 9–10 (2007), *available at* http://www.fas.org/sgp/crs/homesec/RL30153.pdf.

151 Exec. Order No. 13,231, 66 Fed. Reg. 53,063 (Oct. 16, 2001).

the National Infrastructure Advisory Council, which this executive order created.[152]

C. October 25, 2001: USA Patriot Act

The USA Patriot Act empowered the United States Secret Service "to develop a national network of electronic crime task forces."[153] By using the New York Electronic Crimes Task Force, which had, since 1995, "charged over 800 people with electronic crimes valued at more than $500 million[,]"[154] as a model, the United States Secret Service was to build a force for "preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."[155]

D. July 2002: National Strategy for Homeland Security

In July 2002, the Office of Homeland Security released the National Strategy for Homeland Security, which focused on protecting the nation against terrorist attacks.[156] It reiterated the importance of protecting critical infrastructures and grooming a solid relationship between the public and private sectors.[157]

E. November 25, 2002: Homeland Security Act of 2002 (P.L. 170-296)

Congress passed, and President Bush signed the Homeland Security Act of 2002 into law, thereby establishing the Department of Homeland Security.[158] The Department of Homeland Security is a cabinet-level department charged with the protection of the homeland of the United States.[159]

---

152 MOTEFF, *supra* note 150, at 10.

153 USA Patriot Act of 2001, Pub. L. No. 107-56, § 105, 115 Stat. 272, 277 (2001).

154 Press Release, Office of the Press Sec'y, Secretary Ridge Announces New Financial Investigations Initiatives (July 8, 2003), *available at* http://www.dhs.gov/xnews/releases/press_release_0206.shtm.

155 § 105, 115 Stat. at 277.

156 OFFICE OF HOMELAND SEC., NATIONAL STRATEGY FOR HOMELAND SECURITY vii (2002), *available at* http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

157 *Id.* at ix.

158 Homeland Security Act of 2002, Pub. L. No. 107-296, § 101, 116 Stat. 2135, 2142 (2002) (codified at 6 U.S.C. § 111).

159 § 101, 116 Stat. at 2142; *see also* President Bush's Cabinet,

F. November 27, 2002: Cyber Security Research and Development Act (P.L. 107-305)

Congress passed, and President Bush signed the Cyber Security Research and Development Act into law.[160] In conjunction, millions of dollars were allocated for computer and network security research, and development and research fellowship programs.[161] Specifically, "$903 million [was allocated] over five years for new research and training programs by the National Science Foundation (NSF) and the National Institute for Standards and Technology (NIST) to prevent and respond to terrorist attacks on private and government computers."[162]

G. December 17, 2003: Homeland Security Presidential Directive 7 ("HSPD-7")

Concerning cyber security, HSPD-7 clearly emphasized the roles of the Department of Homeland Security ("DHS") and the Office of Management and Budget ("OMB").[163] As a result, a cyber security unit is currently maintained by DHS, while the Director of OMB supports DHS's incident response center and oversees the government-wide information security programs by coordinating information security standards and guidelines developed by federal agencies.[164] HSPD-7 stressed that all federal agencies are responsible for developing plans to protect their own critical infrastructures, and the Director of OMB acts as a check and balance to their policy decisions.[165] Also, the "National Cyber Security Division (NCSD), within . . . [DHS] oversees a Cyber Security Tracking, Analysis and Response Center (CSTARC), tasked with conducting analysis of cyberspace threats and vulnerabilities, issuing alerts and warnings for

http://www.whitehouse.gov/government/cabinet.html (last visited Apr. 11, 2008) (listing the Secretary of Homeland Security as a member of President Bush's cabinet).

160 Cyber Security Research and Development Act, Pub. L. No. 107-305, 116 Stat. 2367 (2002).

161 §§ 4–5, 116 Stat. at 2368, 2370, 2372 (codified at 15 U.S.C. §§ 7403–7404); § 11, 116 Stat. at 2379 (codified at 15 U.S.C. § 7407).

162 COMPUTER ATTACK, *supra* note 15, at 34.

163 *See* MOTEFF, *supra* note 150, at 12.

164 Exec. Order No. 13,231, 66 Fed. Reg. 53,063 (Oct. 16, 2001); *see also* MOTEFF, *supra* note 150, at 12.

165 *See* MOTEFF, *supra* note 150, at 12 (noting that HSPD-7 requires federal agencies to submit their plans to the Director of OMB).

cyberthreats, improving information sharing, responding to major cybersecurity incidents, and aiding in national-level recovery efforts."[166] Even though DHS's main focus is on physical infrastructures, it is reasoned that DHS holds NCSD because the physical infrastructures and cyberspace are interdependent in cyber operations.[167]

H. February 2003: National Strategy to Secure Cyberspace

The *National Strategy to Secure Cyberspace*, "an implementing component of the *National Strategy for Homeland Security*,"[168] was published "to encourage the private sector to improve computer security for the U.S. critical infrastructure . . . ."[169] In part, the significance of this document is that it explicitly defines the federal role concerning privately-owned critical infrastructures as being "only justified when the benefits of intervention outweigh the associated costs."[170] Also, it officially pronounced that, if attacked in cyberspace, the United States would "respond in an appropriate manner," which could include the use of cyber weapons. [171]

I. 2004: National Cyber Alert System ("NCAS")

In 2004, the National Cyber Security Division (NCSD) within DHS formed "the National Cyber Alert System (NCAS), a coordinated national cybersecurity system that distributes information to subscribers to help identify, analyze, and prioritize emerging vulnerabilities and cyberthreats."[172] The United States Computer Emergency Readiness Team (US-CERT) manages NCAS, which exemplifies a public-private partnership in which private entities sign up to receive cyber informational updates and warnings from NCAS.[173] Additionally, the DOD manages information warfare and electronic warfare activities

166 COMPUTER ATTACK, *supra* note 15, at 21.

167 *See id.* at 29.

168 DHS: National Strategy to Secure Cyberspace, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (last visited Apr. 11, 2008).

169 *Id.* at 21.

170 OFFICE OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE ix (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

171 *Id.* at 50; *see also* COMPUTER ATTACK, *supra* note 15, at 24.

172 COMPUTER ATTACK, *supra* note 15, at 21.

173 *Id.* at 21–22.

through its Joint Information Operations Center (JOIC).[174] The JIOC serves under the United States Strategic Command (USSTRATCOM), one of nine unified combat commands of the DOD.[175] Through the Joint Task Force-Global Network Operations (JTF-GNO), which is within the JOIC, DOD's computer systems and networks are defended "in support of combatant commanders' and national objectives."[176]

J. September 2006: The National Strategy for Combating Terrorism

The most recent national strategy published by the United States Government purposely supports the creation of an expert community of counterterrorism professionals.[177] It determines four priorities, including: to prevent attacks by terrorist networks, i.e. cyber attacks; to deny terrorists the support and sanctuary of rogue states; and to deny terrorist control of any nation they would use as a base and launching pad for terror, i.e. cyber safe havens.[178] Again, this national strategy highlights the role of DHS. It marks DHS as the federal center of excellence for cyber security and the focal point for federal outreach to state, local, and nongovernmental organizations, including the private sector, academia, and the public. Without question with regard to cyber security, DHS has become the mediator between the private and public sectors.

---

[174] *Id.* at 24.

[175] *Id. see also U.S. Strategic Command Center for Combating WMD Achieves IOC*, USSTRATCOM NEWS, Feb. 1, 2006, http://www.stratcom.mil/News/WMD_IOC.html (noting USSTRATCOM's position with the DOD).

[176] COMPUTER ATTACK, *supra* note 15, at 24.

[177] *See generally* THE PRESIDENT OF THE U.S., THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 43 (2006), a*vailable at* http://www.whitehouse.gov/nsc/nss/2006/nss2006.pdf (discussing the reorganization of government and the integration of government and private entities to promote counterterrorism).

[178] *Id.* at 11–12.