Harvard Journal of Law & Technology
Volume 20, Number 2 Spring 2007

GETTING IT RIGHT: PROTECTING AMERICAN CRITICAL INFRASTRUCTURE IN CYBERSPACE

Sean M. Condron∗

TABLE OF CONTENTS

> THE DOGMAS OF THE QUIET PAST ARE INADEQUATE TO THE STORMY PRESENT. THE OCCASION IS PILED HIGH WITH DIFFICULTY, AND WE MUST RISE TO THE OCCASION. AS OUR CASE IS NEW, SO WE MUST THINK ANEW AND ACT ANEW.[1]

> WHERE ONCE OUR OPPONENTS RELIED EXCLUSIVELY ON BOMBS AND BULLETS, HOSTILE POWERS AND TERRORISTS CAN NOW TURN A LAPTOP COMPUTER INTO A POTENT WEAPON CAPABLE OF DOING ENORMOUS DAMAGE. IF WE ARE TO CONTINUE TO ENJOY THE BENEFITS OF THE INFORMATION AGE, PRESERVE OUR SECURITY, AND SAFEGUARD OUR ECONOMIC WELL-BEING, WE MUST PROTECT OUR CRITICAL COMPUTER-CONTROLLED SYSTEMS FROM ATTACK.[2]

∗ Judge Advocate, U.S. Army. Presently assigned as an Associate Professor, International and Operational Law Department, The Judge Advocate General's Legal Center and School, Charlottesville, Virginia. LL.M., 2006 (Commandant's List), The Judge Advocate General's Legal Center and School; J.D., 1998 (*cum laude*), Duke University School of Law; B.S., 1992 (Honor Graduate), United States Military Academy. The views expressed in this article are those of the author and do not reflect the views of the Department of Defense or the Department of the Army.

1. Letter from Abraham Lincoln, U.S. President, to U.S. Congress (Dec. 1, 1862), *available at* http://www.presidency.ucsb.edu/ws/print.php?pid=29503.

2. THE WHITE HOUSE, DEFENDING AMERICA'S CYBERSPACE: NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION, at ii (2000), *available at* http://chnm.gmu.edu/cip-digitalarchive/files/522_WhiteHouseNationalPlanInvitationtoDialogue.pdf.

I. INTRODUCTION

The attacks of September 11, 2001 highlight the deadly intent of our adversaries and the nation's vulnerability to "different, unorthodox, and unimaginable" threats.[3] Due to the low cost and wide availability of computers, cyber attacks[4] are an attractive method of warfare.[5] Unlike traditional military weapons, an adversary can use a personal computer, which can be purchased almost anywhere for a few hundred dollars, to accomplish a military objective.[6] In 2003, the Computer Emergency Response Team Coordination Center received reports of 137,529 "incidents."[7] Attacks against network systems have become so common that, in 2004, the Computer Emergency Response Team stopped maintaining statistics showing the number of "incidents."[8] In 2004, the Congressional Research Service estimated that the economic impact of cyber attacks in the United States was $226 billion.[9]

Cyber attacks can originate from a number of sources. Michael Vatis, former head of the Institute for Security Technology Studies at Dartmouth College, has identified four categories of threats: terrorists, nation-states, terrorist sympathizers, and thrill seekers.[10] Of these threats, nation-states likely have the greatest capabilities and resources. For example, in the years ahead, the United States will

---

3. JAMES KIRAS ET AL., UNDERSTANDING "ASYMMETRIC" THREATS TO THE UNITED STATES 15 (2002), *available at* http://www.nipp.org/Adobe/Asymmetry%20%20final%2002.pdf.

4. This Article uses the phrases "cyber attack," "cyber defense," "cyber warfare," "cyberspace," and other derivatives of the root word "cyber" to refer to activities centered on the use of a computer system or computer network. For example, a cyber attack would refer to an attack using a computer system or network or an attack against a computer system or network.

5. PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROT., CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES 17 (1997), *available at* http://chnm.gmu.edu/cipdigitalarchive/files/5_CriticalFoundationsPCCIP.pdf.

6. *See id.* at 17–18.

7. Carnegie Mellon Software Engineering Institute, CERT/CC Statistics 1988–2005, http://www.cert.org/stats/cert_stats.html (last visited Apr. 14, 2007) ("An incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time."). The website does not further define the word "incident," but a discussion implies that it is some type of suspected attack on a computer system. *Id.*

8. *See id*. The Chief Information Officer and Assistant Secretary for Networks and Information Integration at the Department of Defense stated, "Our networks are under constant cyberattacks." Ian Martinez, *Cybersecurity at Center Stage for Advisory Committee*, WASH. INTERNET DAILY, Dec. 20, 2006.

9. Eric Chabrow, *Homeland Security Tries to Get its Cybersecurity House in Order*, INFORMATIONWEEK, Oct. 2, 2006, at 56, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=193100332&cid=RSSfeed_IWK_All.

10. MICHAEL A. VATIS, INST. FOR SEC. AND TECH. STUDIES AT DARTMOUTH COLL., CYBER ATTACKS DURING THE WAR ON TERRORISM: A PREDICTIVE ANALYSIS 1 (2001), *available at* http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

probably face an evolving cyber threat from China. In particular, China is integrating "information warfare units" into its military operations that have the capabilities for "first strikes against enemy networks."[11] In August 1999, China launched several cyber attacks against Taiwan, initiating a "public hacking war" with the disputed island.[12] China may have attacked United States federal government computer systems in the past.[13] Nation-states, however, probably will not attempt major cyber attacks, unless it is a precursor to military action, because of the potential severity of the response. Nation-states have territory, property, and citizens to protect, all of which would be jeopardized if it were to conduct a major cyber attack.

Thrill seekers are a minor threat because they are generally driven by a desire to show off their skills, rather than a desire to destroy.[14] While they are certainly capable of causing some serious problems, both the media and self-promoters from this group have overstated their actual menace.[15]

Cyber terrorists may not have a robust ability to conduct large cyber attacks on critical infrastructure, but they are probably far more likely to try than other actors.[16] Cyber terrorists do not face the repercussions that nation-states would and probably have more destruction-oriented agendas than thrill seekers. Despite this concern, there have been no known attempts to stage such an attack by any major terrorist group.[17] According to Dorothy Denning, a professor of computer science at the Naval Postgraduate School, "[t]errorists have not yet integrated information technology into their strategy and tactics, and significant barriers between hackers and terrorists may prevent their integration into one group."[18] There are indications, however, that Al Qaeda and other terrorist groups are seeking to expand their capabilities in this area, perhaps by forging connections with hacker groups.[19]

---

11. DEP'T OF DEFENSE, ANNUAL REPORT TO CONGRESS: MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA 35–36 (2006).

12. Peter Warren, *China Fires First Shots in Cyber War*, SCOT. ON SUNDAY, Aug. 22, 1999, at 8.

13. Bill Gertz, *Chinese Hackers Raid U.S. Computers*, WASH. TIMES, May 16, 1999 at C1. Following the errant bombing of the Chinese embassy in Belgrade, Chinese hackers launched cyber attacks on computers at the White House, State Department, and other federal agencies. *Id.*

14. VATIS, *supra* note 10, at 14.

15. GABRIEL WEIMANN, TERROR ON THE INTERNET 158–59 (2006) (quoting *Cyber Terrorism and Critical Infrastructure Protection: Hearing Before the Subcomm. on Gov't Efficiency, Fin. Mgmt., and Intergov'tal Relations*, 107th Cong. (2002) (statement of Douglas Thomas, Professor, Univ. of S. Cal.)).

16. VATIS, *supra* note 10, at 12.

17. WEIMANN, *supra* note 15, at 165.

18. *Id.* at 167.

19. *Id.* at 169–70. "U.S. troops searching the caves in Afghanistan found plans by al Qaeda to attack computer systems after sending al Qaeda recruits to train in high tech systems." *Id.* at 170.

Michael Vatis argues that terrorist sympathizers are the most likely group to launch a cyber attack.[20] Unlike the other groups, these individuals do not necessarily lack the technological ability or incentives. As a demographic, they are hackers with not only the knowledge and ability to conduct a cyber attack, but also a cause shared by terrorist groups like Al Qaeda.[21]

The United States federal government has focused an unprecedented amount of attention, time, and financial resources on the threat from weapons of mass destruction[22] and terrorism.[23] The White House, recognizing the growing threat of cyber attacks and the importance of protecting cyberspace,[24] has designated the Department of Homeland Security as the lead agency for addressing this threat.[25]

The government's approach to protecting cyberspace focuses on the concept of "critical infrastructure." The USA PATRIOT Act of 2001 defines critical infrastructure as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[26] Critical infrastructure includes the following sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, and postal and shipping.[27]

---

20. *See* VATIS, *supra* note 10, at 13–14.

21. *Id.* at 13.

22. *See* Robert Joseph, U.S. Under Sec'y for Arms Control and Int'l Sec., Dep't of State, Meeting the Challenges of Weapons of Mass Destruction Proliferation, Remarks at the University of Virginia Miller Center (Dec. 9, 2005), *available at* http://www.state.gov/t/us/rm/57874.htm.

23. *See* EXECUTIVE BRANCH OF THE U.S. GOV'T, NATIONAL STRATEGY FOR COMBATING TERRORISM 19 (2003), *available at* http://www.whitehouse.gov/news/releases/2003/02/counter_terrorism/counter_terrorism_strategy.pdf; *see also* THE PRESIDENT OF THE U.S., THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 12 (2006), *available at* http://www.whitehouse.gov/nsc/nss/2006/nss2006.pdf.

24. EXECUTIVE BRANCH OF THE U.S. GOVERNMENT, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, at iv (2003) [hereinafter SECURE CYBERSPACE], *available at* http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

25. *Id.* at 54.

26. USA PATRIOT Act of 2001 § 1016, 42 U.S.C. § 5195c (Supp. II 2002); *see also* U.S. DEP'T OF HOMELAND SECURITY, NATIONAL INFRASTRUCTURE PROTECTION PLAN 103 (2006) [hereinafter NIPP], *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (defining critical infrastructure to include networks vital to the nation). There is a related but distinct concept of key resources, defined as "publicly or privately controlled resources essential to the minimal operations of the economy or government." Homeland Security Act of 2002 § 2(9), 6 U.S.C. § 101(9) (Supp. II 2002); *see also* NIPP, *supra*, at 104.

27. THE PRESIDENT OF THE UNITED STATES, NATIONAL STRATEGY FOR HOMELAND SECURITY 30 (2002) [hereinafter HOMELAND SECURITY], *available at* http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf. Homeland Security Presidential Directive 7 suggests an expansion of critical infrastructure sectors when it assigns roles and responsibilities of sector-specific federal agencies. *See* PRESIDENT OF THE UNITED

Both government and private entities own and operate the critical infrastructure in the United States.[28]

Critical infrastructure is by definition essential for the survival of the nation.[29] Networked computer systems form the nerve center of the country's critical infrastructure.[30] The private sector is largely unable to adequately protect these computer systems and networks from major military and terrorist threats.[31] Civilian networks are often more vulnerable to attack than the Department of Defense network.[32] However, military networks are also vulnerable because they depend extensively on civilian networks for connectivity and transferability of information.[33] The well-being of the nation depends on a safe and secure cyber environment for its critical infrastructure.[34] Therefore, protection of the computer systems and networks supporting critical infrastructure in the United States should be the federal government's responsibility.[35]

Despite the magnitude of this threat, the United States currently operates under the presumption that a cyber attack constitutes a criminal activity, not a threat to national security.[36] Because law enforcement investigations that require the methodical collection of evidence are often protracted and resource-intensive, typically taking days, weeks, or even months, this presumption may result in a very slow response that may come too late to confront a cyber attack successfully.[37] A delayed response to a cyber attack on the nation's critical

---

STATES, HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 7 (2003), *available at* http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

28. *See* EXECUTIVE BRANCH OF THE U.S. GOV'T, THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS 8 (2003) [hereinafter PHYSICAL PROTECTION], *available at* http://www.whitehouse.gov/pcipb/physical_strategy.pdf. In 2003, the private sector owned and operated about eighty-five percent of the critical infrastructure in the United States. *Id*.

29. *See* 42 U.S.C. § 5195c (Supp. II 2002).

30. *See* SECURE CYBERSPACE, *supra* note 24, at vii.

31. *See generally* PHYSICAL PROTECTION, *supra* note 28, at 8 (discussing the insufficiency of private sector protection of critical infrastructure).

32. *See* Arthur K. Cebrowski, *CNE and CNA in the Network-Centric Battlespace: Challenges for Operators and Lawyers*, 76 INT'L L. STUD. 1, 4 (2002).

33. *See id.*; *see also* Charles J. Dunlap, Jr., *Meeting the Challenge of Cyberterrorism: Defining the Military Role in Democracy*, 76 INT'L L. STUD. 353, 354 (2002).

34. *See* SECURE CYBERSPACE, *supra* note 24, at vii.

35. *See* Chabrow, *supra* note 9, at 56.

36. *See* Dunlap, *supra* note 33, at 365; Kenneth A. Minihan, *Defending the Nation Against Cyber Attack: Information Assurance in the Global Environment*, U.S. FOREIGN POL'Y AGENDA, Nov. 1998, at 5, 7; Walter Gary Sharp, Sr., *Balancing Our Civil Liberties with Our National Security Interests in Cyberspace*, 4 TEX. REV. L. & POL. 69, 70 (1999); *see also* SECURE CYBERSPACE, *supra* note 24, at 28 (stating that "[l]aw enforcement plays the central role in attributing an attack through the exercise of criminal justice authorities").

37. *See* Sharp, *supra* note 36, at 71.

infrastructure may result in lives lost and massive damage.[38] For these reasons, the response should be nearly simultaneous with the attack itself.[39]

It may thus be preferable to approach cyber security as a threat to national security rather than as a criminal matter. This change would raise at least three issues. First, it may be necessary to revisit and clarify the government's current distinction between homeland security and homeland defense as applied to cyberspace. Second, this change requires consideration of the *jus ad bellum* paradigm that controls a state's self-defense response against a cyber attack. Finally, the delicate balance between national security interests and civil liberties should be considered in developing a strategy for responding to cyber attacks. This Article presents a framework for addressing these issues.

II. DEFENSE AND SECURITY: A BLURRED DISTINCTION

Following September 11, 2001, the executive branch made a policy decision to distinguish homeland security from homeland defense.[40] Homeland security has been defined as a "concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[41] In contrast, "[h]omeland defense is the protection of US sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression, or other threats as directed by the President."[42] The Department of Homeland Security is the federal agency in charge of homeland security while the Department of Defense is the lead federal agency for homeland defense.[43]

Such a distinction between defense and security poses several problems in the context of cyberspace. The first problem is that the distinction relies on a poor choice of words: defense and security are commonly understood to be synonymous.[44] Applying synonymous terms to two different concepts can lead to confusion. The Department of Homeland Security's National Response Plan exacerbates this con-

---

38. *See* Eric Talbot Jensen, *Computer Attacks on Computer National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 232 (2002).

39. *See* Sharp, *supra* note 36, at 71–72.

40. *See* HOMELAND SECURITY, *supra* note 27, at 13; U.S. DEP'T OF DEF., STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT 5 (2005) [hereinafter HOMELAND DEFENSE], *available at* http://www.defenselink.mil/news/Jun2005/d20050630homeland.pdf.

41. 6 U.S.C.A. § 111(b)(1)(A)–(C) (West 2002); *see also* HOMELAND SECURITY, *supra* note 27, at 2.

42. HOMELAND DEFENSE, *supra* note 40, at 5.

43. See HOMELAND SECURITY, *supra* note 27, at 13; HOMELAND DEFENSE, *supra* note 40, at 5.

44. ROGET'S II: THE NEW THESAURUS 248 (3d ed. 1995).

fusion by creating categories that imply a distinction between cyber security of the United States and cyber defense of the United States without delineating the difference between the two.[45]

The second problem is that the executive branch has failed to clearly distinguish between defense and security. As previously defined, homeland security focuses on terrorist attacks within the United States, while homeland defense focuses on external threats and aggression towards the sovereignty, territory, domestic population, and critical defense infrastructure of the United States.[46] It is easy to envision threats that span both concepts. Consider, for example, a cyber terrorist attack perpetrated from outside the United States where the effects of the cyber attack are felt within the United States. Under the current definitions of security and defense, it is not clear which agency would be responsible for preventing or responding to this threat.

The most serious problem with these definitions is their reliance on the concept of geographical borders. Geographical borders are almost meaningless in cyberspace[47] because cyberspace has no borders or boundaries in the traditional sense.[48] The Internet relies on "packet switching" by which packets travel the shortest electronic route to their destination.[49] However, the shortest electronic route does not necessarily correspond to the shortest geographical route.[50] Data transfer on the Internet "considers existing network traffic loads," and therefore "shortest" relates to time more than to geographic distance.[51] That route may cross physical borders during transmission, even when transmission is between domestically-situated entities.[52] This creates, in essence, a border-free space. Although the Department of Homeland Security has a definition for cyber security,[53] the definition does nothing to clarify this issue. Under the current formulation, differentiating between homeland security and homeland defense in cyberspace is essentially impossible.

---

45. *See* U.S. DEP'T OF HOMELAND SEC., NATIONAL RESPONSE PLAN, at CYB-6 (2004) [hereinafter NRP], *available at* http://www.dhs.gov/xlibrary/assets/NRP_FullText.pdf.

46. *See* HOMELAND SECURITY, *supra* note 27, at 2; HOMELAND DEFENSE, *supra* note 40, at 5.

47. *See* David R. Johnson & David Post, *Law and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996).

48. *Id.* at 1367.

49. David Tubbs et al., *Technology and Law: The Evolution of Digital Warfare*, 76 INT'L L. STUD. 7, 10 (2002).

50. *Id.*

51. *Id.*

52. *See* Johnson & Post, *supra* note 47, at 1372–73.

53. *See* NIPP, *supra* note 26, at 108 (defining cyber security as "[t]he prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and services (and the information contained therein) to ensure confidentiality, integrity, and availability").

Notwithstanding these definitional problems, government policy distinguishes between security and defense. With these distinctions, the government emphasizes security over defense with regard to cyberspace. The agency hierarchy is evidence of this priority. Under the National Strategy to Secure Cyberspace, the Department of Homeland Security assumes the lead role for cyber security,[54] with the Department of Defense relegated to a minor, supporting role.[55] Yet there is no comparable national strategy for cyber defense. This oversight has left a gaping hole in the protection of United States critical infrastructure because the Department of Homeland Security bases its concept of "security" on prevention and repair,[56] whereas the concept of defense has traditionally entailed a wider range of options. This section will outline some preliminary ideas about possible components that could be used to craft a cyber defense strategy.

Generally, defensive military operations consist of two types: active measures and passive measures.[57] Computer network defense can also be classified using these categories. Computer network defense protects from both domestic and foreign threats.[58] Passive measures of computer network defense include encryption, firewalls, and automated detection.[59] Generally, active measures include some type of in-kind response,[60] in which "the entity attacked launches an offensive operation against the perpetrator using a method that is similar in nature to the one used against them."[61] For the most part, the federal government has classified the specifics of active measures of computer network defense.[62] A good example of an active defense is the counter-strike philosophy of an Internet security company, which of-

54. SECURE CYBERSPACE, *supra* note 24, at 54.

55. *See* NRP, *supra* note 45, at CYB-6.

56. *See* NIPP, *supra* note 26, at 108.

57. *See generally* CARL VON CLAUSEWITZ, PRINCIPLES OF WAR 16–17 (Hans W. Gatzke trans., 1942).

58. *See* JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS, at II-5 (Feb. 13, 2006) [hereinafter JOINT PUB. 3-13], *available at* http://www.fas.org/irp/dodder/dod/jp3_13.pdf.

59. Jensen, *supra* note 38, at 230. Encryption is the process of producing ciphertext by scrambling the text in such a way that only individuals with the secret key can read and understand the text. DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 286 (1999). A firewall is "a network monitor or collection of monitors placed between an organization's internal network and the Internet or between two local area networks. The objective is to keep intruders, malicious code, and unwanted information out and proprietary or sensitive data in. A firewall is essentially a gateway between two networks." *Id*. at 353. Automated detection involves programs that "can scan computer records or on-line computer activity for patterns that indicate or suggest the presence of unauthorized activity." *Id*. at 361.

60. *Id.* ("[A]ctive responses may involve some in-kind rejoinder or 'hack-back' feature, either reflecting similar damage back to the sender or causing some other responsive action.").

61. DENNING, *supra* note 59, at 392.

62. Jensen, *supra* note 38, at 231.

fers counter measures including "flooding the attacking computers with data [and] rendering them Internet-blind."[63]

Computer network defense within the United States' Department of Defense "involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks."[64] The Department of Defense does not have an organization dedicated to and focused on the cyber defense of critical infrastructure.[65]

III. THE CYBERSPACE THREAT AND INTERNATIONAL LAW

The threats in cyberspace run the gamut from the teenager curious about what she can accomplish with her own personal computer[66] to a foreign military service separate and distinct from that nation's army, navy, and air force, devoted exclusively to information warfare.[67] That, indeed, is one of the challenges of this threat — a cyber attack could originate from any number of potential actors.[68] The attacker could be an isolated individual, a member of some organized group,

---

63. Matthew Fordahl, *Networks Lash Back at Cyber Hacks*, CBS NEWS, June 18, 2004, http://www.cbsnews.com/stories/2004/06/18/tech/main624875.shtml (noting that customers for such active defense programs include government and military entities).

64. JOINT PUB. 3-13, *supra* note 58, at II-5. The U.S. government defines the computer network defense mission as the coordination and direction of defense operations of "computer networks from unauthorized activity employing communications, law enforcement, counterintelligence and Intelligence Community (IC) capabilities in response to specific or potential threats." JOINT CHIEFS OF STAFF, INSTR. 6510-01D, INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND) at A-5 (June 15, 2004), *available at* http://www.dtic.mil/cjcs_directives /cdata/unlimit/6510_01.pdf.

65. *See* U.S. STRATEGIC COMMAND, JOINT TASK FORCE — GLOBAL NETWORK OPERATIONS, http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html (last visited Apr. 14, 2007). Joint Task Force — Global Network Operations protects the Global Information Grid. *Id.* The Global Information Grid is the network and computer systems supporting "warfighters, policymakers, and support personnel." JOINT CHIEFS OF STAFF, JOINT PUB. 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 225 (Apr. 12, 2001 as amended through Mar. 1, 2007), *available at* http://www.dtic.mil/doctrine/jel/ new_pubs/jp1_02.pdf. This represents, at most, only a fraction of the nation's critical infrastructure.

66. In July 2005, a teenager in Germany "admitted creating the Sasser and Netsky internet worms which forced airlines to ground their fleets and the British coastguard to work with pen and paper." Hannah Cleaver, *Teenager Admits Virus Attacks*, DAILY TELEGRAPH, July 6, 2005, at 16. In a 2000 attack, a Canadian boy known only as Mafiaboy shut down several major websites including CNN.com, Amazon.com, and Yahoo.com. DeNeen L. Brown, *Teen Admits Attacking Web Sites*, WASH. POST, Jan. 19, 2001, at E1. In 1998, two California teenagers who wanted to test their computer skills "penetrated Pentagon computers and briefly disrupted the movement of troops participating in military exercises in the Persian Gulf." Chris Mondics, *Rep. Andrews Leads Charge for Cyber Security*, PHILA. INQUIRER, Dec. 26, 2002, at A25.

67. Bill Gertz, *U.S. Set to Take Warfare On-Line*, WASH. TIMES, Jan. 6, 2000, at A3.

68. *See* SECURE CYBERSPACE, *supra* note 24, at 6.

or a state actor.[69] It is even possible that an attack could involve multiple actors, each with a slightly different intent.[70]

A. Use of Force in Cyber Self-Defense

The United Nations Charter and customary international law both govern the use of force by states and form the basis of the current *jus ad bellum* paradigm.[71] This paradigm prohibits the use or threat of force, except in limited circumstances.[72] The legal basis for the *jus ad bellum* paradigm is Article 2(4) of the United Nations Charter,[73] which states that "[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[74] There are two exceptions to the prohibition on the use of force in the United Nations Charter: Security Council action pursuant to Article 42[75] and individual or collective self-defense under Article 51.[76]

Legal scholars disagree on the current state of customary international law as it relates to the use of force in self-defense and the proper interpretation of Article 51. Some scholars interpret Article 51 strictly, arguing that a state may not act in self-defense until that state has suffered an armed attack.[77] According to this school of thought, a state could not act in anticipation of an armed attack.[78] Other legal scholars argue that Article 51 incorporates customary international

69. *See generally id.* at 6–7 (concluding that technology allows increasing numbers of actors to launch attacks on critical infrastructure in cyberspace).

70. *See* Barbara Demick, *Teenage Hacker Inspires Awe in Some Israeli Officials*, MIAMI HERALD, Mar. 26, 1998, at 2F (stating that teenage hackers in California joined with a teenager in Israel to attack Pentagon computer systems).

71. Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 99 (2002).

72. *See* U.N. Charter art. 2, para. 4; *id.* art. 51; Dinstein, *supra* note 71, at 99.

73. Dinstein, *supra* note 71, at 99. Professor Dinstein and others argue that "there exists in international law today 'an absolute prohibition of the use or threat of force, subject only to the exceptions stated in the Charter itself.'" *Id.* (quoting Josef Mrazek, *Prohibition of the Use and Threat Force: Self-Defence and Self-Help in International Law*, 27 CANADIAN Y.B. INT'L L. 81, 90 (1989)).

74. U.N. Charter art. 2, para. 4.

75. *Id.* art. 42 (authorizing the Security Council to "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security").

76. *Id.* art. 51 (stating that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations").

77. *See, e.g.*, Horace B. Robertson, *Self-Defense Against Computer Network Attack*, 76 INT'L L. STUD. 121, 123 (2002).

78. *Id.*

law as articulated by the *Caroline* standard, allowing anticipatory self-defense.[79]

It is important to note that the United Nations Charter was written before the Internet existed. There is no specific provision in the United Nations Charter that addresses cyber warfare, but the International Court of Justice has ruled that Article 2(4) and Article 51 apply to "any use of force, regardless of the weapons employed."[80] Although a question arises as to whether certain cyber attacks amount to a use of force under Article 2(4) or an armed attack under Article 51, many legal scholars would probably agree that a cyber attack *could* amount to a use of force or an armed attack.[81] More importantly, most legal scholars would probably agree that the United Nations Charter system and customary international law bind state actions engaging in cyber warfare.[82]

B. Conditions for the Use of Force in Cyber Self-Defense

Under the *jus ad bellum* paradigm, a state response to an armed attack must meet three conditions to qualify as self-defense: necessity, proportionality, and immediacy.[83] To fulfill the principle of necessity

---

79. Jason Barkham, *International Warfare and International Law on the Use of Force*, 34 NY.U. J. INT'L L. & POL. 57, 75 (2002); Jensen, *supra* note 38, at 218–19. The *Caroline* case involved a British attack on a United States ship in 1837. 2 JOHN BASSET MOORE, A DIGEST OF INTERNATIONAL LAW § 217, 409–10 (1906). Several years after the attack, United States Secretary of State Daniel Webster accepted a British apology for the attack and concluded that a state may attack in self-defense when the "necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation." *Id.* at 412 (quoting Letter from Daniel Webster, U.S. Sec'y of State, to Alexander Ashburton, Gr. Brit. Plenipotentiary (Aug. 6, 1842)). This quote is the *Caroline* standard of anticipatory self-defense.

80. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244 (July 8).

81. Jensen, *supra* note 38, at 222; Robertson, *supra* note 77, at 135–37; Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 934–35 (1999); Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4)*, 76 INT'L L. STUD. 73, 92–93 (2002).

82. *See* Dinstein, *supra* note 71, at 99, 102–03; Schmitt, *supra* note 81, at 929–30. *But see* Silver, supra note 81, at 93 ("The notion that the Charter represents the sole legal structure under which coercive force can be exerted by one State against another largely has been discredited."). An unusual problem arises when a state reacts in self-defense to a cyber attack; due to the nature of the Internet, a cyber attack and any cyber response to that attack may implicate the territorial integrity of a neutral nation. *See* George K. Walker, Neutrality and Information Warfare, 76 INT'L L. STUD. 233, 244–47 (2002); George K. Walker, Information Warfare and Neutrality, 33 VAND. J. TRANSNAT'L L. 1079, 1175–76 (2000).

83. *See* Dinstein, *supra* note 71, at 109; *see also* Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, 103 (June 27) (concluding that a self-defense response must fulfill the principles of necessity and proportionality under customary international law); YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 183–84 (3d ed. 2001) (discussing a third principle of immediacy that must be fulfilled for a lawful self-defense response under customary international law). *But see* Oscar Schachter, *The Right of States to Use*

generally, "non-forcible remedies must either prove futile *in limine* or have in fact been exhausted in an unsatisfactory manner."[84] Furthermore, the state must attribute the attack to a specific source, characterize the intent behind the attack, and conclude that the state must use force in response.[85] The principle of proportionality requires that the force used in the response be proportional to the original attack.[86] Lastly, immediacy prohibits the response from being "too tardy."[87] Under customary international law, the principle of immediacy is broad,[88] allowing a response days, weeks, or even months later.[89]

Attribution and characterization are especially important in the context of cyber warfare. A state must attribute an attack for two reasons. First, attribution helps to ensure that a state does not target an innocent person or place.[90] Second, a state must attribute an attack because the laws governing a permissible response vary depending on whether the attacker is a state actor or a non-state actor.[91] A state actor includes state employees, such as members of the military, as well as independent contractors, such as hackers hired to launch a cyber attack. A non-state actor is someone acting individually or a member of a terrorist organization.[92] If the attacker is a state actor, the response must comply with the United Nations Charter[93] and customary international law.[94] On the other hand, if the attacker is a non-state actor,

---

Armed Force, 82 MICH. L. REV. 1620, 1635, 1637 (1984) (arguing the anticipatory self-defense under customary international law requires necessity, proportionality, and imminency). Because this issue is not germane to the discussion, immediacy is used as the third condition to maintain consistency with the cited source.

84. Dinstein, *supra* note 71, at 109.

85. *Id.*; *see also* Jensen, *supra* note 38, at 231 (arguing that any active defense to a cyber attack must meet three longstanding limitations: attribution, characterization of the intent, and respect for the neutrality of other states).

86. Dinstein, *supra* note 71, at 109. There is some dispute about whether a state may aggregate many smaller attacks when determining the amount of counter-force authorized by law. *Id.* Professor Dinstein concludes that there is some support for the theory that suffering from many small attacks should permit a state to respond with one large counter-measure. *Id.*

87. *Id.* at 110.

88. Kevin C. Kenny, *Self-Defence*, 2 UNITED NATIONS: LAW, POLICIES AND PRACTICE 1162, 1167 (Rüdiger Wolfrum ed., 1995).

89. Dinstein, *supra* note 71, at 110.

90. *See id.*

91. *See* Jensen, *supra* note 38, at 232–33.

92. Non-state actors also include international criminal organizations that specialize in areas such as drug trafficking, human trafficking, money laundering, fraud, computer crimes, and many other illegal activities. *Cf.* CarrieLyn Donigan Guymon, *International Legal Mechanisms for Combating Transnational Organized Crime: The Need for a Multilateral Convention*, 18 BERKELEY J. INT'L L. 53, 94 (2000).

93. U.N. Charter art. 2, para. 4; *id.* art. 51.

94. Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, 94 (June 27).

domestic criminal law will likely govern the response.[95] In addition, international law requires a state to characterize an attack to avoid using force against an entity that inadvertently launched a cyber attack.[96] A state may be able to use force against a hostile attack under its own laws, but international law prohibits the use of force against an inadvertent attack.[97]

When a state defends itself using an active defense measure, additional international law implications arise. The principles of necessity and proportionality forbid "retaliatory or punitive actions. . . . [I]n particular, the means employed for the defence have to be strictly necessary for repelling the attack."[98] Yet the principle of proportionality does not limit "a state, victim of an armed attack . . . to expelling the foreign troops from its territory in exercising its right to self-defence, but [also allows pursuit] across the border into their territory."[99]

The current *jus ad bellum* paradigm does not offer adequate safeguards from cyber attacks.[100] The problem with cyber warfare is that technology makes it nearly impossible to attribute the attack to a specific source or to characterize the intent behind it. Moreover, a cyber attacker can launch her assault with the push of a key, completing the attack almost instantaneously.[101] A legal system that requires a determination of the attacker's identity and intent does not account for these features of the digital age.[102] The current international paradigm therefore ties a state's hands, making it difficult to effectively respond without risking a violation of international law.[103]

To address the unique nature of cyber warfare, international law should provide a safe harbor for states who initiate a good-faith response to an attack, thus acting in cyber self-defense, without first attributing and characterizing the attack.[104] State survival may depend on an immediate, robust, and aggressive response; therefore, interna-

---

95. *See* Daniel M. Creekman, Note, *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, 661 (2002); Jensen, *supra* note 38, at 232–33.

96. Dinstein, *supra* note 71, at 109.

97. *See* Jensen, *supra* note 38, at 235; *see also supra* note 82 and accompanying text.

98. *See* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 805 (Bruno Simma ed., 2d ed. 2002).

99. *Id*.

100. *See* Barkham, *supra* note 79, at 112; Creekman, *supra* note 95, at 680; Jensen, *supra* note 38, at 239; Schmitt, *supra* note 81, at 886. *But see* James P. Terry, *Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?*, 46 NAVAL L. REV. 170, 185 (1999).

101. *See* Jensen, *supra* note 38, at 232.

102. *See* Creekman, *supra* note 95, at 680; Jensen, *supra* note 38 at 239. *But see* Terry, *supra* note 100, at 185.

103. *See* Barkham, *supra* note 79, at 112; Creekman, *supra* note 95, at 680; Jensen, *supra* note 38, at 240; Schmitt, *supra* note 81, at 886.

104. *See* Creekman, *supra* note 95, at 681; Jensen, *supra* note 38, at 240; Schmitt, *supra* note 81, at 936.

tional law should not always require a state to fully satisfy the traditional necessity requirements when acting in self-defense of critical infrastructure.[105] A preferable governing principle would be: when the attack targets the state's critical infrastructure, the state should be able to exercise active defense measures or launch a cyber attack in response without incurring liability.[106] In order to avoid an exception that swallows the rule, states should be required to maintain a publicly available list of critical infrastructure, which a state may protect with active defense measures and, if the identified critical infrastructure were subjected to a cyber attack, a state could respond in cyberspace without first attributing or characterizing the attack.[107] In these circumstances, such an exception would not fundamentally alter the *jus ad bellum* framework, but would instead allow the state to exercise its inherent right of self-defense.

IV. CYBER WARFARE AND CIVIL LIBERTIES

The anonymity of cyber attackers is not only a practical problem. It also raises civil liberties concerns. While cyber attacks by a foreign nation launched from abroad are unlikely to implicate constitutional liberties, the same cannot be said for cyber attacks originating on United States soil. The possibility of employing active defense measures against United States citizens may infringe certain civil liberties normally enjoyed by Americans. Although a cyber attack on critical infrastructure may threaten national security, the United States should take into account the civil liberties of the individual American citizen when determining the proper response. The law must therefore adjust traditional understandings of the right to privacy,[108] the right to protection against an unreasonable search,[109] and the right to due process,[110] given the practical necessity of responding to cyber attacks before determining the attacker's identity and intent. In considering this balance, policymakers should keep in mind Justice Goldberg's statement: "[W]hile the Constitution protects against invasions of individual rights, it is not a suicide pact."[111]

---

105. Jensen, *supra* note 38, at 239–40.

106. *See id.*

107. *Cf.* Sharp, *supra* note 36, at 74.

108. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 484–86 (1965).

109. *See* U.S. CONST. amend. IV.

110. *See* U.S. CONST. amend. V.

111. Kennedy v. Mendoza-Martinez, 372 U.S. 144, 160 (1963); *see also* Terminello v. City of Chicago, 337 U.S. 1, 37 (1949) (Jackson, J., dissenting) ("There is danger that, if the Court does not temper its doctrinaire logic with a little practical wisdom, it will convert the constitutional Bill of Rights into a suicide pact.").

In responding to those attacks originating on U.S. soil, passive defense measures like encryption and firewalls are not problematic. However, active defense measures and response actions may gather intelligence from information stored on a person's computer system, alter information on that computer system, or destroy the computer system. All of these actions could threaten the constitutional rights of that person. An additional complication is that cyber attacks often use the computers of unsuspecting users as vessels.[112] This makes attribution simultaneously more difficult and more important. While it may be possible to attribute an incident to a specific computer system, it may not be possible to attribute the incident to the specific person coordinating the attack. This raises the possibility of the government inadvertently infringing upon the civil liberties of innocent individuals.

The United States takes pride in the protection of civil liberties. The Constitution, and more specifically the Bill of Rights, was an attempt to protect the most fundamental civil liberties of a democratic society. Yet these liberties are not necessarily absolute. In times of armed conflict, the government may be forced to limit them in the interest of national security. As Chief Justice Rehnquist pointed out:

> [I]n any civilized society the most important task is achieving a proper balance between freedom and order. In wartime, reason and history both suggest that this balance shifts to some degree in favor of order — in favor of the government's ability to deal with conditions that threaten the national well-being.[113]

While Chief Justice Rehnquist was referring to declared wars, he referred in his argument to *Youngstown Sheet & Tube Co. v. Sawyer*,[114] which took place during the undeclared Korean War, and discusses the power of the President to restrict civil liberties outside a state of declared war.[115] It could also be argued that the formal declaration of war is obsolete, serving little or no purpose in international law.[116] "[I]t appears that no nation has declared war since the late 1940s," in spite of hundreds of armed conflicts during this same pe-

112. Fordahl, *supra* note 63.

113. WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 222 (1998).

114. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952).

115. REHNQUIST, *supra* note 113, at 218–19.

116. Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 HARV. L. REV. 2047, 2061 (2005).

riod.[117] The relevant paradigm is now "armed conflict";[118] its existence should be the relevant question in determining whether the balance should potentially shift. While a cyber attack may use different means than a traditional armed conflict, it is no less threatening to national security, and it thus requires policymakers to balance liberty and security as in a conventional armed attack.

A. Reversing the Presumption

The current U.S approach to cyber attacks can be understood to favor civil liberties at the expense of national security. The United States operates under the presumption that a cyber attack is a criminal act.[119] Pursuant to this presumption, law enforcement investigates a cyber attack in the same fashion and by following the same rules as any other criminal matter.[120] This process respects the civil liberties of a suspected cyber attacker.[121] Only if the perpetrator of a cyber attack has been determined to be a non-U.S. citizen operating outside United States territory may law enforcement pass the incident on to another agency for a responsive measure.

This presumption of a criminal act applies regardless of the cyber attacker's target.[122] A cyber attack on a computer system that is part of our critical infrastructure is subject to the same presumption as an attack on a local business.[123] The problem with this presumption should be clear from the previous discussion concerning the threats in cyberspace: it may take days or even months to investigate the attack.[124] Even if a law enforcement agency can attribute the source of the attack, which may not be possible, doing so days or months later makes it impossible to prevent the resulting damage.[125] In choosing whether to treat a cyber attack as a criminal matter rather than a national security matter, policymakers should balance the protection of civil liberties against the ability to immediately, robustly, and aggressively respond to a cyber attack against critical infrastructure.

One example of how our current presumption has led to unsatisfactory results occurred in February 1998, when three teenagers, two

---

117. *Id.* at 2061–62.

118. *Id*. at 2061.

119. *See* Dunlap, *supra* note 33, at 365; Minihan, *supra* note 36, at 7; Sharp, *supra* note 36, at 70; *see also* SECURE CYBERSPACE, *supra* note 24, at 28 (stating that "[l]aw enforcement plays the central role in attributing an attack through the exercise of criminal justice authorities").

120. *See* Minihan, *supra* note 36, at 7; Sharp, *supra* note 36, at 71–72.

121. *See* Sharp, *supra* note 36, at 69.

122. *Id.* at 70.

123. *See id.*

124. *See id.* at 71.

125. *See id*.

located in California and one in Israel, hacked into eleven unclassified computer systems of the Navy and Air Force.[126] The ensuing interagency law enforcement operation took nearly a month to identify and arrest the perpetrators.[127] Were it not for the presumption that a cyber attack is a criminal activity requiring a response in accordance with the criminal justice system, federal authorities could have immediately launched an aggressive defense that would have quickly ended the attack. Although this attack had a benign purpose and the time lag did not result in catastrophic consequences, it highlights the potential difficulties that might arise when attempting to respond to a more serious attack.

This Article argues that the only effective way to mount an immediate, robust, and aggressive response to a cyber attack on critical infrastructure is to reverse the current presumption.[128] The nation should initially presume any cyber attack on the critical infrastructure of the United States is a national security threat rather than a criminal activity, at least until federal authorities neutralize the threat and determine that the activity is actually criminal in nature. Such a new presumption would make room for the response necessary to protect critical infrastructure.[129]

B. Impact of the Posse Comitatus Act

Viewing cyber attacks as national security threats suggests that the Department of Defense should play a much greater role, if not the lead role, in the cyber protection of critical infrastructure. Department of Defense involvement in cyber protection within the domestic United States, however, may have Posse Comitatus Act implications that should be considered. The Posse Comitatus Act restricts federal military assets from performing traditional law enforcement functions absent separate authority.[130]

Congress passed the Posse Comitatus Act in 1878 in response to the alleged excesses of federal troops in the South during the Reconstruction Era.[131] The current version of the Posse Comitatus Act states that "[w]hoever, except in cases and under circumstances expressly

---

126. Lisa Hoffman, *Pentagon Confronts Challenge to Computer System Security*, PATRIOT LEDGER, Apr. 8, 1998, at 16.

127. *See* Sharp, *supra* note 36, at 71.

128. *But see* Dunlap, *supra* note 33, at 366–67 (cautioning that the "the true threat is not what damage cyberterrorists can inflict upon our digital systems, but what freedoms they can force us to forfeit").

129. *See* Sharp, *supra* note 36, at 72.

130. *See* 18 U.S.C. § 1385 (2000).

131. *See* Brian L. Porto, Annotation, *Construction of Application of Posse Comitatus Act (18 U.S.C.A. § 1385), and Similar Predecessor Provisions, Restricting Use of United States Army and Air Force to Execute Laws*, 141 A.L.R. FED. 271, 281 (1997).

authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws" will be punished pursuant to the Act.[132] There are two Constitutional exceptions to the Act:

> (i) *The emergency authority.* Authorizes prompt and vigorous Federal action, including use of military forces, to prevent loss of life or wanton destruction of property and to restore governmental functioning and public order when sudden and unexpected civil disturbances, disasters, or calamities seriously endanger life and property and disrupt normal governmental functions to such an extent that duly constituted local authorities are unable to control the situations.
>
> (ii) *Protection of Federal property and functions.* Authorizes Federal action, including the use of military forces, to protect Federal property and Federal governmental functions when the need for protection exists and duly constituted local authorities are unable or decline to provide adequate protection.[133]

While on its face the Posse Comitatus Act appears to preclude a major role for the Department of Defense in cyber protection, any response to an attack on the computer systems of United States critical infrastructure would fall under one of the two Constitutional exceptions to the Act. The exact exception would depend on the nature of the critical infrastructure being targeted. An attack on private, state or local critical infrastructure would fall under the emergency authority exception, while an attack on federal critical infrastructure would fall under the protection of the federal property and functions exception. By definition, critical infrastructures are national systems and assets.[134] If, as this Article advocates, a cyber attack against critical infrastructure is presumed to be a national security threat, it can be dealt with by federal rather than local authorities and trigger one of the two Constitutional exceptions to the Act.

If at some point during a cyber attack it became clear that local authorities were more capable of responding to the attack, the Department of Defense could hand the action over to them for a continued response. The military could also passively assist the local

132. 18 U.S.C. § 1385.
133. 32 C.F.R. § 215.4 (2006).
134. 42 U.S.C. § 5195c (Supp. II 2002).

authorities without violating the Posse Comitatus Act regardless of the presumption applied.[135] For example, the military could continue to coordinate and exchange information with the local authorities, but could not participate in the ensuing law enforcement functions.[136] Therefore, the Posse Comitatus Act should not exclude the Department of Defense from playing a major role in protecting cyberspace.

V. CONCLUSION

Each day the connectivity of the world increases. This increased connectivity in turn improves our standard of living, expands the speed and sophistication of our decision-making abilities, and fuels the global economy. However, these benefits come at a cost. The United States is more vulnerable now than it has ever been before. For the first time in history, an individual armed with nothing more than technical expertise, a computer system, and a network connection could theoretically bring our nation to its knees. At no more than the cost of an AK-47, a terrorist could cause large-scale death and destruction by launching a cyber attack on the critical infrastructure of our nation. We owe it to ourselves to avoid an attack of this magnitude in the future. The possibility of a substantial cyber attack requires policymakers to fundamentally rethink the way in which they approach protection of the networks and computer systems underlying the nation's critical infrastructure.

A cyber attack is not merely a criminal matter that the nation can effectively address under the rubric of the justice system, but rather is an issue of national security. As such, the federal government must resolve the blurred distinction between cyber security and cyber defense. In cyberspace we cannot distinguish between defense and security. In addition, international law must evolve to account for the nature of the cyber threat to critical infrastructure. The *jus ad bellum* paradigm must permit active self-defense of critical infrastructure and allow a self-defense response to an attack on critical infrastructure in cyberspace without first requiring attribution or characterization of the attack. However, *jus ad bellum* should only allow use of these measures in defense of critical infrastructure that a nation has pre-selected and publicly disseminated prior to the incident. Lastly, policymakers must strike the proper balance between civil liberties and national security interests as we confront this cyber threat. The nature of the

---

135. *See* Porto, *supra* note 131, at 283 (explaining that military personnel would only violate the Posse Comitatus Act if they "assisted in civilian law enforcement by making arrests, searching persons and/or property, seizing evidence, investigating crimes, interviewing witnesses, pursuing escaped civilian prisoners, and searching an area for suspects.").

136. *See id.*

threat requires a reversal of the presumption that a cyber attack on critical infrastructure is a criminal matter. The new presumption must be that a cyber attack on critical infrastructure is a national security threat.

The United States cannot afford to get this wrong. Failure to properly protect the computer systems and networks of the nation's critical infrastructure could result in catastrophic consequences for the United States.[137] As Leonardo da Vinci put it, "[i]t is easier to resist at the beginning than at the end."[138]

137. *See* SECURE CYBERSPACE, *supra* note 24, at 6.

138. JOHN BARTLETT, FAMILIAR QUOTATIONS 135 (Justin Kaplan ed., 16th ed. 1992).