

Cyber Warfare and Precautions Against the Effects of Attacks

Eric Talbot Jensen*

Ninety-eight percent of all U.S. government communications travel over civilian-owned-and-operated networks. Additionally, the government relies almost completely on civilian providers for computer software and hardware products, services, and maintenance. This near-complete intermixing of civilian and military computer infrastructure makes many of those civilian objects and providers legitimate targets under the law of armed conflict. Other civilian networks, services, and communications may suffer collateral damage from legitimate attacks on government targets. To protect those civilian objects and providers from the effects of attacks, the law of armed conflict requires a state to segregate its military assets from the civilian population and civilian objects to the maximum extent feasible. Where segregation is not feasible, the government must protect the civilian entities and communications from the effects of attacks. The current integration of U.S. government assets with civilian systems makes segregation impossible and therefore creates a responsibility for the United States to protect those civilian networks, services, and communications. The U.S. government is already taking some steps in that direction, as illustrated by a number of plans and policies initiated over the past decade. However, the current actions do not go far enough. This Article identifies six vital actions the government must take to comply with the law of armed conflict and to ensure not only the survivability of military communication capabilities during times of armed conflict, but also the protection of the civilian populace and civilian objects.

I.	Introduction.....	1522
II.	Cyber “Attacks”	1524
III.	Interconnectivity, Targeting, and Feasibility Under Article 58(a) and (b)	1530
IV.	Alternative Responsibilities Under Article 58(c).....	1540
V.	U.S. Practice in Protecting Civilians and Civilian Cyber Objects.....	1543
VI.	Recommendations	1551
VII.	Conclusion	1556

* Visiting Assistant Professor, Fordham Law School. Previously Chief, International Law Branch, Office of The Judge Advocate General, U.S. Army; Military Legal Advisor to U.S. forces in Baghdad, Iraq and in Tuzla, Bosnia; Legal Advisor to the U.S. contingent of U.N. forces in Macedonia. Thanks to Sean Watts for his comments on an earlier draft and SueAnn Johnson for her invaluable research assistance.

I. Introduction

From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.

—President Barack Obama¹

In a recent address to open the 2010 Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology, former Director of National Intelligence Admiral Michael McConnell estimated that 98% of U.S. government communications, including classified communications, travel over civilian-owned-and-operated networks and systems.² The U.S. government does not control or protect these networks. The lack of effective security and protection of these and most other civilian computer networks led Admiral McConnell to predict that the United States will suffer an “electronic Pearl Harbor.”³ He further predicted that at some point the U.S. government is going to have to “reinvent” itself to better incorporate and account for advancing cyber technology.⁴ Finally, he predicted that the Internet is going to have to move from “dot com” to “dot secure.”⁵ Coming from his prior position,⁶ these remarks should cause those who read them to pause and wonder at the inevitability of these predictions.

In fact, the United States and other governments are very aware of the problem and are making efforts to combat their vulnerabilities.⁷ However,

1. Barack Obama, U.S. President, Remarks on Securing Our Nation’s Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure; see also Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 123 (2009) (quoting NATO’s Chief of Cyber Defense as stating that “cyber terrorism [and] cyber attacks pose as great a threat to national security as a missile attack”).

2. Michael McConnell, Former Dir. of Nat’l Intelligence, Keynote Address at the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology (Feb. 4, 2010). The Symposium was sponsored by the Texas Law Review in partnership with the Strauss Center for International Security and Law.

3. *Id.* Others have similarly predicted an electronic Pearl Harbor. See *Bush’s War Room: Richard Clarke*, ABC NEWS, Sept. 30, 2004, <http://abcnews.go.com/Politics/story?id=121056&page=1> (indicating that former Special Adviser for Cyberspace Security Richard Clarke became well-known for using the phrase “electronic Pearl Harbor”).

4. McConnell, *supra* note 2.

5. *Id.* The reference here is presumably to a move to an Internet architecture that provides a much more secure platform than the current system.

6. See Shane Harris, *The Cyberwar Plan*, NAT’L J., Nov. 14, 2009, available at http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (describing how McConnell “established the first information warfare center at the NSA in the mid-1990s”).

7. See *infra* notes 36–46 and accompanying text.

many of the current efforts do not go far enough in addressing these vulnerabilities. The efforts also do not fully respond to legal requirements under the law of war. One example of this shortcoming in current government action, and the topic of this Article, is the lack of preparedness to comply with the law-of-armed-conflict requirement to protect civilians and civilian objects from the effects of attacks. The law of war requires states to either segregate their military assets from civilians and civilian objects, or where segregation is not feasible, to protect those civilians and civilian objects.⁸ The pervasive intermixing of U.S. Department of Defense (DOD) networks with civilian networks,⁹ the vast percentage of DOD communications that travel over civilian lines of communication,¹⁰ the near-complete reliance on commercially produced civilian hardware and software for DOD computer systems,¹¹ and the reliance on civilian companies for support and maintenance of U.S. government computer systems¹² make segregation of military and civilian objects during an armed attack unfeasible. This interconnectedness also makes these civilian companies, networks, and lines of communication legitimate targets to an enemy during armed conflict. Therefore, the United States and other similarly situated countries have a duty to protect the civilian networks and infrastructure, and key civilian companies, from the effects of potential attacks.

Part II of this Article will briefly document the current state of cyber affairs with a focus on the pervasiveness of cyber “attacks.” This Part will also briefly highlight the complicating problem of the inability to attribute attacks in cyberspace. Part III will discuss the significance of the interconnectivity of DOD cyber capabilities with civilian networks and systems, including potential enemy-targeting decisions. The Part will go on to establish that, at this point, it is not feasible for the United States to segregate its cyber operations from civilian objects and infrastructure as required by Article 58,

8. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 58, *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 3 [hereinafter API].

9. McConnell, *supra* note 2.

10. *Id.*

11. See ROBERT H. ANDERSON & RICHARD O. HUNDLEY, RAND CORP., THE IMPLICATIONS OF COTS VULNERABILITIES FOR THE DOD AND CRITICAL U.S. INFRASTRUCTURES: WHAT CAN/SHOULD THE DOD DO? 1 (1998), <http://www.rand.org/pubs/papers/2009/P8031.pdf> (“Critical systems on which the security and safety of the United States depend are increasingly based on commercial off-the-shelf (COTS) software systems.”); cf. ENTERPRISE SOFTWARE INITIATIVE, DEP’T OF DEF., ESI OVERVIEW & HISTORY (2009), <http://www.esi.mil/LandingZone.aspx?id=101&zid=1> (explaining the DOD’s ESI mission to reduce the cost of commercial software and hardware, which the DOD is relying on “more than ever to run the business of the DoD”).

12. See, e.g., Press Release, IBM, IBM Awarded National Security Agency High Assurance Platform (HAP) Contract to Improve Secure Information Sharing (Feb. 7, 2008), <http://www-03.ibm.com/press/us/en/pressrelease/23460.wss> (explaining the NSA’s High Assurance Platform (HAP) program, in which the NSA works with privacy companies, like IBM, to develop next-generation computers and networking technology).

paragraphs (a) and (b), of Additional Protocol I to the 1949 Geneva Conventions (API).¹³ Part IV will analyze the alternative requirement of paragraph (c) of Article 58, which requires states that are unwilling or unable to segregate their military and civilian objects to protect the endangered civilians and civilian objects under their control from the effects of potential attack.¹⁴ Part V will review specific steps already taken by the United States in an attempt to protect civilian infrastructure and systems. Part VI will advocate further measures that should be taken to not only ensure compliance with Article 58, but to also better meet the stated goals of protecting the U.S. cyber networks and infrastructure.

II. Cyber “Attacks”

The recent attack¹⁵ on the massive search engine Google¹⁶ is indicative of the pervasive nature of the threat that exists in cyberspace. A recent report claimed that at least thirty other companies were subjects of the same attack,¹⁷ and it was further discovered that “[m]ore than 75,000 computer systems at nearly 2,500 companies in the United States and around the world ha[d] been hacked in what appear[ed] to be one of the largest and most sophisticated attacks by cyber criminals to date.”¹⁸ Experts assert that “thousands of companies” are currently compromised by cyber invasions.¹⁹ In many of these cases, the companies do not even know they are compromised until law enforcement authorities tell them.²⁰ By that time, they have already been victimized.

These attacks are not only pervasive, but also cheap to execute and expensive to detect, defend, and remediate.²¹ As President Obama noted in

13. API, *supra* note 8, art. 58.

14. *See id.* (mandating that the parties to a conflict take all necessary precautions to protect civilians and their objects from dangers resulting from military operations).

15. *See* NAT’L RESEARCH COUNCIL OF THE NAT’L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1–2 (William A. Owens et al. eds., 2009) (describing the nature of cyber attack and its potential use); Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT’L L. 391, 399–405 (2010) (detailing the anatomy of a cyber attack); Paul A. Walker, Rethinking Computer Network “Attack” (Dec. 31, 2009) (unpublished manuscript), available at http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=paul_walker (discussing what amounts to an “attack” with computer-network operations).

16. Ellen Nakashima et al., *Google Threatens to Leave China*, WASH. POST, Jan. 13, 2010, at A1.

17. Ellen Nakashima, *Google to Enlist NSA to Ward off Attacks*, WASH. POST, Feb. 4, 2010, at A1.

18. Ellen Nakashima, *Large Worldwide Cyber Attack Is Uncovered*, WASH. POST, Feb. 18, 2010, at A3.

19. Kim Zetter, *Report Details Hacks Targeting Google, Others*, WIRED, Feb. 3, 2010, <http://www.wired.com/threatlevel/2010/02/apt-hacks/>.

20. *Id.*

21. *See* Siobhan Gorman et al., *Insurgents Hack U.S. Drones*, WALL ST. J., Dec. 17, 2009, available at <http://online.wsj.com/article/SB126102247889095011.html>; PAUL ROSENZWEIG, AM.

his speech quoted at the beginning of this Article, “America’s economic prosperity in the 21st century will depend on cybersecurity.”²² According to Ty Sagalow, Chairman of the Internet Security Alliance Board of Directors, “An estimated \$1 trillion was lost in the United States in 2008 through cyber attacks.”²³ The cost of downtime alone from major attacks to critical national infrastructure “exceeds . . . \$6 million per day.”²⁴ And the frequency and cost of cyber attacks are increasing.²⁵

A recent report published by the Center for Strategic and International Studies (CSIS) and McAfee, Inc. surveyed 600 security and IT executives from critical infrastructure in fourteen countries and detailed their anonymous responses about their “practices, attitudes and policies on security—the impact of regulation, their relationship with government, specific security measures employed on their networks, and the kinds of attacks they face.”²⁶ Their responses portray a state of continual attack on critical national infrastructure by high-level and technologically capable adversaries.²⁷ One of the most telling statistics gathered from this survey was that the United States was perceived as “one of the three countries ‘most vulnerable to critical infrastructure cyberattack’”²⁸ For all countries, but particularly for the United States, this is a problem that has the potential to dramatically affect civil life.²⁹

BAR. ASS’N STANDING COMM. ON LAW & NAT’L SEC., NATIONAL SECURITY THREATS IN CYBERSPACE 1–3 (2009), http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf (arguing that the unique features of cyberspace generally make traditional risk management ineffective and, even when possible, impractical because of the significant costs necessary for implementation).

22. Obama, *supra* note 1.

23. William Matthews, *Cyberspace May Be Locale of Next War, Group Warns*, FED. TIMES, Dec. 7, 2009, available at 2009 WLNR 25655353.

24. STEWART BAKER ET AL., CTR. FOR STRATEGIC & INT’L STUDIES, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 3 (2010), <http://csis.org/event/crossfire-critical-infrastructure-age-cyber-war>.

25. *Id.* at 5.

26. *Id.* at 1, 41 n.1.

27. *Id.* at 3–11; see also Mark Clayton, *US Oil Industry Hit by Cyberattacks: Was China Involved?*, CHRISTIAN SCI. MONITOR, Jan. 25, 2010, <http://www.csmonitor.com/layout/set/print/content/view/print/275786> (describing recent cyber attacks on major U.S. oil companies that “may have originated in China and that experts say highlight a new level of sophistication in the growing global war of Internet espionage”).

28. BAKER ET AL., *supra* note 24, at 30; see also Ellen Messmer, *DDoS Attacks, Network Hacks Rampant in Oil and Gas Industry, Other Infrastructure Sectors*, NETWORKWORLD, Jan. 28, 2010, <http://www.networkworld.com/news/2010/012710-ddos-oil-gas.html?page=1> (reviewing various statistics generated in the CSIS survey, including one listing the United States as one of the three countries perceived as most vulnerable to cyber attack).

29. See Matthews, *supra* note 23 (“By targeting the systems that control [U.S.] manufacturing plants, power generators, refineries and other infrastructure, attackers may be able to take control of—and even crash—power, water, traffic control and other critical systems”); BAKER ET AL., *supra* note 24, at 30 (“Some experts suggested that the U.S. was seen as more vulnerable because it was more advanced—and more reliant than almost any other nation on computer networks.”).

The attacks on Google and others also highlight another significant problem that plagues cybersecurity, or at least responses to cyber invasions—the inability to attribute cyber attacks.³⁰ Attribution is the ability to know who is actually conducting the attacks. As one former U.S. law enforcement official stated, “Even if you can trace something back to a [computer], that doesn’t tell you who was sitting behind it.”³¹ This lack of ability to attribute an attack gives attackers “plausible deniability.”³² While “most owners and operators [of critical national infrastructure] believe that foreign governments are already engaged in attacks on critical infrastructure in their country,”³³ there is no way to positively establish that.³⁴ For example, one computer-security expert claims that “the majority of the data that gets exfiltrated [from the United States] ultimately finds its way to IP addresses in China, and that’s pretty much all anybody knows.”³⁵

The commercial world is not the only target of cyber attack. Indeed, “politically-motivated attacks are becoming more frequent and sustained.”³⁶ In its 2009 Virtual Criminology Report, McAfee, Inc. noted that there has been an increase in politically motivated cyber attacks, including attacks against the White House, Department of Homeland Security (DHS), U.S. Secret Service, and DOD.³⁷ A recent report stated that in 2007,

[T]he Departments of Defense, State, Homeland Security, and Commerce; NASA; and National Defense University all suffered major intrusions by unknown foreign entities. The unclassified e-mail of the secretary of defense was hacked, and DOD officials told us that the department’s computers are probed hundreds of thousands of times each day. A senior official at the Department of State told us the department had lost “terabytes” of information. Homeland Security

30. Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. REV. 1, 31 (2009).

31. BAKER ET AL., *supra* note 24, at 6.

32. *Id.* at 1; see also *Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace: Hearing Before the Subcomm. on Terrorism and Homeland Security of the S. Comm. on the Judiciary*, 111th Cong. (2009) (statement of Larry M. Wortzel, Vice Chairman, U.S.–China Economic and Security Review Commission), available at http://judiciary.senate.gov/hearings/testimony.cfm?id=4169&wit_id=8316 (emphasizing that one of the most important objectives in preparing for future cyber attacks should be “developing reliable attribution techniques to determine the origin of computer exploitations and attacks”).

33. BAKER ET AL., *supra* note 24, at 3.

34. See *The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade: Hearing Before the H. Comm. on Foreign Affairs*, 111th Cong. (2010) (statement of Larry M. Wortzel, Comm’r, U.S.–China Economic and Security Review Commission), available at <http://www.internationalrelations.house.gov/111/wor031010.pdf> (arguing that “even if the attacks can be traced to China, it is not clear who ordered the attacks”).

35. Zetter, *supra* note 19 (quoting Kevin Mandia, president–CEO of Mandiant, a computer-security firm).

36. Jeffrey Carr, *Under Attack from Invisible Enemies*, INDEP. (U.K.), Jan. 20, 2010, available at 2010 WLNR 1165835.

37. Press Release, McAfee, Inc., McAfee Inc. Warns of Countries Arming for Cyberwarfare (Nov. 17, 2009), http://newsroom.mcafee.com/article_display.cfm?article_id=3594.

suffered break-ins in several of its divisions, including the Transportation Security Agency. The Department of Commerce was forced to take the Bureau of Industry and Security off-line for several months, and NASA has had to impose e-mail restrictions before shuttle launches and allegedly has seen designs for new launchers compromised.³⁸

U.S. government computers and networks are constantly being probed,³⁹ and protection is a formidable task. In any twenty-four-hour period, DOD computers access the Internet “over one billion times.”⁴⁰ The DOD “operates 15,000 networks across 4,000 installations in 88 countries. [They] use more than 7 million computer devices. It takes 90,000 personnel and billions of dollars annually to administer, monitor and defend those networks.”⁴¹ DHS recently received funding to hire up to one thousand cybersecurity experts to help “the nation’s defenses against cyberthreats,”⁴² and DOD “ordered all troops and officials involved in protecting computer networks from enemy hackers to undergo training in computer hacking” under the premise that “to beat a hacker, you must think like one.”⁴³ At a recent Senate subcommittee hearing, Senator Thomas R. Carper stated that in the last year “federal agencies have spent more on cyber security than the entire Gross Domestic Product of North Korea.”⁴⁴ It is estimated that “more than 100 foreign intelligence organizations are trying to break into U.S. systems”⁴⁵ and known cyber attacks against U.S. computers rose to 37,258 in 2008 from 4,095 in 2005.⁴⁶ Terrorist organizations such as al Qaeda are transitioning many of

38. COMM’N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, CTR. FOR STRATEGIC & INT’L STUDIES, *SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 12–13* (2008), http://csis.org/files/media/isis/pubs/081208_securingcyberspace_44.pdf.

39. See Schapp, *supra* note 1, at 141–42 (providing two examples of recent incidents in which hackers penetrated U.S. government computer systems).

40. Joshua E. Kastenberg, *Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DOD to Take Time-Sensitive Action on the NIPRNET*, 64 A.F. L. REV. 175, 183 (2009).

41. William J. Lynn III, Deputy Sec’y of Def., Remarks at the USAF–TUFTS Institute for Foreign Policy Analysis Conference (Jan. 21, 2010), <http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1410>.

42. Carol Cratty, *DHS to Hire up to 1,000 Cybersecurity Experts*, CNN POLITICS.COM, Oct. 2, 2009, <http://www.cnn.com/2009/POLITICS/10/02/dhs.cybersecurity.jobs/index.html> (quoting Secretary of Homeland Security Janet Napolitano).

43. Bill Gertz, *Inside the Ring*, WASH. TIMES, Mar. 4, 2010, at A8.

44. *More Security, Less Waste: What Makes Sense for Our Federal Cyber Defense: Hearing Before the Subcomm. on Fed. Financial Management, Government Information, Fed. Servs., and International Security of the S. Comm. on Homeland Security and Governmental Affairs*, 111th Cong. (2009) (statement of Sen. Thomas R. Carper, Chairman, Subcomm. on Fed. Financial Management, Government Information, Fed. Servs., and International Security), available at http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=8505fb0f-bf9b-4bb4-9e25-e71154391202.

45. Lynn, *supra* note 41.

46. Siobhan Gorman, *Bush Looks to Beef Up Protection Against Cyberattacks*, WALL ST. J., Jan. 28, 2008, at A9.

their efforts to the Internet,⁴⁷ causing FBI Director Robert S. Mueller to state that “Al-Qaeda’s online presence has become as potent as its physical presence.”⁴⁸

Attacks are not focused solely on the United States. Countries such as Tatarstan, Kyrgyzstan, Iran, Zimbabwe, Israel, and South Korea have been the targets of attacks within the last two years.⁴⁹ Additionally, there are the famous cases of Estonia in 2007⁵⁰ and Georgia in 2008⁵¹ where cyber attacks severely degraded the government’s ability to govern. The attacks in Estonia targeted not only government Web sites but also included many of the country’s banks and other civilian infrastructure.⁵² Even more telling for the topic of this Article, “[h]ackers mounted coordinated assaults on Georgian government, media, banking and transportation sites in the weeks before Russian troops invaded.”⁵³ These recent historical examples show not only the propensity to attack governments but also the natural integration of cyber attacks with future kinetic attacks. This is almost certainly a trend that will increase.⁵⁴ As demonstrated by the attacks on Georgia and Estonia,

47. See Toby Harnden, *Al-Qa’eda Plans Cyber Attacks on Dams*, DAILY TELEGRAPH, June 28, 2002, <http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1398683/Al-Qa'eda-plans-cyber-attacks-on-dams.html> (“Al-Qa’eda have been investigating how to carry out devastating attacks through cyberspace by seizing control of dam gates or power grids using the internet.”); Pauline Neville-Jones, Statement on Governments and Cyber Warfare (Mar. 11, 2010), http://www.conservatives.com/News/Speeches/2010/03/Pauline_Neville-Jones_Governments_and_Cyber_Warfare.aspx (noting that terrorists rely on the Internet for recruiting and planning purposes).

48. Ellen Nakashima, *FBI Director Warns of ‘Rapidly Expanding’ Cyberterrorism Threat*, WASH. POST, Mar. 4, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html>.

49. Carr, *supra* note 36.

50. Anne Applebaum, *For Estonia and NATO, a New Kind of War*, WASH. POST, May 22, 2007, at A15; Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at A1; *US Warns Cyber-Attacks Will Increase*, FIN. TIMES, May 18, 2007, at 12; Toomas Hendrik Ilves, President, Republic of Estonia, Remarks at the International Cyber Conflict Legal and Policy Conference in Tallinn (Sept. 9, 2009), http://www.president.ee/en/media/press_releases.php?gid=130312. The attacks on Estonia prompted NATO to fund and create a new research center designed to boost their cooperative defenses against cyber attacks. *Cyberterrorism Defense*, WASH. POST, May 14, 2008, at A13.

51. James R. Asker, *Cyber Zap*, AVIATION WK. & SPACE TECH., Sept. 7, 2009, at 24; Siobhan Gorman, *Cyberwarfare Accompanies the Shooting*, WALL ST. J., Aug. 12, 2008, at A9.

52. BAKER ET AL., *supra* note 24, at 17.

53. Brandon Griggs, *U.S. at Risk of Cyberattacks, Experts Say*, CNN, Aug. 18, 2008, <http://www.cnn.com/2008/TECH/08/18/cyber.warfare/index.html>; see also Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 4–5 (2009) (“In July 2008, shortly before armed conflict broke out between Russia and Georgia, hackers barraged Georgia’s Internet infrastructure with coordinated cyberattacks. The attacks overloaded and shut down many of Georgia’s computer servers, and impaired Georgia’s ability to disseminate information to its citizens during its armed conflict with Russia.”).

54. See Jaak Aaviksoo, Minister of Defense, Republic of Estonia, Strategic Impact of Cyber Attacks, Address at the Royal College of Defense Studies (May 3, 2010), <http://www.irl.ee/en/Media/Articles/1927/strategic-impact-of-cyber-attacks> (discussing the threat of

attribution continues to be a problem in the case of attacks against state-computer systems.⁵⁵ Without the ability to attribute, it is difficult to equate these attacks to acts of armed conflict.⁵⁶

It is clear that states, in conjunction with upgrading their cyber defenses, are also developing cyber-offensive capability.⁵⁷ As mentioned previously,⁵⁸ many of the IT and security professionals who responded to the CSIS survey believed that foreign governments were behind at least some of the attacks on their networks.⁵⁹ The United Nations has collected statements by a number of nations concerning their views on cyberspace,⁶⁰ but few clear answers have emerged.

“coordinated cyber attacks towards [a] country’s critical information infrastructure . . . organized together with physical attacks”).

55. See Schaap, *supra* note 1, at 144–46 (recounting the cyber attacks that were mounted against Estonian and Georgian computer systems and noting that “there is no conclusive proof of who was behind the attacks”); Watts, *supra* note 15, at 397–98 (elaborating on the difficulty of identifying the “precise source” of the Russian attacks on Georgian and Estonian computer networks).

56. See Sklerov, *supra* note 53, at 6–10 (explaining that “because the law of war forbids states from responding with force unless an attack can be attributed to a foreign state or its agents,” the attribution problem forces governments to treat cyber attacks as criminal matters rather than as traditional armed assaults).

57. BAKER ET AL., *supra* note 24, at 5 (“In 2007, McAfee’s annual Virtual Criminology Report concluded that 120 countries had, or were developing, cyber espionage or cyber war capabilities.”); see also RAY WALSER, HERITAGE FOUND., STATE SPONSORS OF TERRORISM: TIME TO ADD VENEZUELA TO THE LIST (2010), <http://www.heritage.org/Research/Reports/2010/01/State-Sponsors-of-Terrorism-Time-to-Add-Venezuela-to-the-List> (warning of Cuba’s developing capacity for cyber warfare, aided by the Russians and Chinese).

58. See *supra* notes 26–27 and accompanying text.

59. BAKER ET AL., *supra* note 24, at 3.

60. See The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–13, delivered to the General Assembly, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–17, delivered to the General Assembly, U.N. Doc. A/64/129 (July 8, 2009); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–8, delivered to the General Assembly, U.N. Doc. A/63/139 (July 18, 2008); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 1–3, delivered to the General Assembly, U.N. Doc. A/62/98/Add.1 (Sept. 17, 2007); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–14, delivered to the General Assembly, U.N. Doc. A/62/98 (July 2, 2007); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–8, delivered to the General Assembly, U.N. Doc. A/61/161 (July 18, 2006); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 3, delivered to the General Assembly, U.N. Doc. A/60/95 (July 5, 2005); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–13, delivered to the General Assembly, U.N. Doc. A/59/116 (June 23, 2004); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–17, delivered to the General

The ubiquity of cyber attack cannot be questioned. However, each state's response to the problem is certainly an open question. While issues of attribution complicate a state's response, every state has to be prepared to protect itself and its citizens from the consequences of cyber attack. It is on this issue that this Article focuses next.

III. Interconnectivity, Targeting, and Feasibility Under Article 58(a) and (b)

As mentioned in the introduction to this Article, 98% of U.S. government communications travel over civilian-owned-and-operated networks.⁶¹ This includes both unclassified and classified messaging and would presumably include communications that are military orders and directions for conducting military operations. It would likely also include current intelligence and information reports coming from the battlefield to update strategic decision makers in the Pentagon and other headquarters.⁶²

These communications are military objectives and would be targetable by an enemy during armed conflict. The definition of military objectives is contained in Article 52 of the API.⁶³ Article 52 is titled "General protection

Assembly, U.N. Doc. A/58/373 (Sept. 17, 2003); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 1–3, delivered to the General Assembly, U.N. Doc. A/57/166 (July 2, 2002); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–6, delivered to the General Assembly, U.N. Doc. A/56/164/Add.1 (Oct. 3, 2001); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–5, delivered to the General Assembly, U.N. Doc. A/56/164 (July 3, 2001); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–7, delivered to the General Assembly, U.N. Doc. A/55/140 (July 10, 2000); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–13, delivered to the General Assembly, U.N. Doc. A/54/213 (Aug. 10, 1999) (reporting responses from various countries expressing their appreciation of information-security issues and ideas about measures to strengthen information security in the future); see also The Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2, delivered to the General Assembly, U.N. Doc. A/60/202 (Aug. 5, 2005) (reporting on the communications between the governmental experts on information security); Sean Kanuck, Int'l Att'y and Senior Intelligence Analyst, *Sovereign Discourse on Cyber Conflict Under International Law*, Remarks at the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology (Feb. 6, 2010), *audio available at* <http://www.texaslrev.com/symposium/listen> (discussing various countries' responses to U.N. requests and the current group of governmental experts on information security).

61. See *supra* note 2 and accompanying text.

62. See Howard S. Dakoff, Note, *The Clipper Chip Proposal: Deciphering the Unfounded Fears That Are Wrongfully Derailing Its Implementation*, 29 J. MARSHALL L. REV. 475, 479 (1996) (noting that the types of military communications transmitted over private networks "include the designing of weapons, the guiding of missiles, the managing of medical supplies, the mobilization of reservists and the relaying of battle tactics to combat commanders").

63. API, *supra* note 8, art. 52 ("[M]ilitary objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization . . . offers a distinct military advantage.").

of civilian objects” and clarifies that civilian objects are not targetable.⁶⁴ It also contrasts civilian objects with military objectives.⁶⁵

A government’s military or intelligence-agency⁶⁶ computers, routers, networks,⁶⁷ cables, and other cyber assets are targetable because of their use facilitating military communications. If these objects were performing the same functions for a civilian company, rather than the government, they would be protected from attack as civilian objects. It is their use by the military or intelligence agencies that makes them targetable.⁶⁸ Though it concerned radio and television instead of cyber communication, this is apparently the analysis that NATO leaders applied before bombing a radio and television station in Belgrade during the Kosovo air campaign in 1999.⁶⁹ Such an action, though protested by Serbia, was not found to be unlawful.⁷⁰

Similarly, the government procures the vast majority of its hardware and software from commercial suppliers. Much of this software and hardware is also maintained by civilian companies.⁷¹ These companies that manufacture and service government hardware and software may be targetable. In the event of a sustained attack against the United States’ cyber capabilities, these civilian companies would likely be contacted for support and maintenance.⁷² Further, the U.S. government is the “single largest

64. *Id.*

65. *See id.* (“Civilian objects are all objects which are not military objectives as defined in paragraph 2.”).

66. There may be other government computers, routers, networks, cables, and other assets that would also be targetable based on their use.

67. *But see* Joshua E. Kastenber, *Non-intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43, 55 (2009) (recognizing a memorandum from the U.S. Air Force Operations and International Law division as taking the position that a network does not constitute a weapons system). This may affect an attacker’s analysis as to whether a network is targetable by its nature as opposed to its use.

68. *See* API, *supra* note 8, art. 52 (“[M]ilitary objectives are . . . those objects which by their . . . use make an effective contribution to military action . . .” (emphasis added)).

69. Justin Brown & Phil Miller, *Foreign Journalists Feel the Heat of Backlash*, SCOTSMAN, Apr. 24, 1999, available at http://findarticles.com/p/articles/mi_7951/is_1999_April_24/ai_n32632439/?tag=content; Paul Richter, *Milosevic Not Home as NATO Bombs One of His Residences*, L.A. TIMES, Apr. 23, 1999, at A34.

70. *See* Int’l Criminal Tribunal for the Former Yugo., June 13, 2000, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia*, ¶ 72, 39 I.L.M. 1257, 1283 (noting NATO’s stress of the civil television network’s “dual-use”).

71. *See, e.g.*, Press Release, Lockheed Martin, Lockheed Martin Awarded \$5.8M Contract to Maintain Pentagon Electronic Messaging Systems (Aug. 20, 2008), http://www.lockheedmartin.com/news/press_releases/2008/0820_pentagon-netcents-contract.html (reporting the selection of Lockheed Martin, a civilian company, “to operate and maintain the message routing infrastructure for the Pentagon’s command messaging systems”).

72. Civilians who work at these companies would be targetable to the extent that they take a “direct part in hostilities.” *See* API, *supra* note 8, art. 51 (“Civilians shall enjoy the protection afforded by this section, unless and for such time as they take a direct part in the hostilities.”). The meaning of this term is highly contested and beyond the scope of this Article. *See generally* NILS MELZER, INT’L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT

purchaser of information security products.”⁷³ These security products are purchased from civilian suppliers who presumably will supply security updates and assistance to maintain the security of government systems. This reliance on civilian cyber companies to maintain government cyber systems and update cyber products brings the premises and objects used by these civilian companies potentially within the targeting options of an attacking enemy as well. If a civilian computer company produces, maintains, or supports government cyber systems, it seems clear that an enemy could determine that company meets the test of Article 52 and is targetable.

Discrete electronic-military communications, such as an e-mail transmitting an attack order or delivering an intelligence report, are also targetable by their nature. Targeting and interrupting these communications would obviously be of great benefit to an enemy during an armed conflict. As will be discussed below, targeting specific electronic communications presents technological difficulties, but under the law, it is clear that these discrete communications are targetable.⁷⁴

Each of the military targets just listed is likely to be intermixed with civilian objects in the interconnected cyber world.⁷⁵ The surrounding civilian objects cannot be directly attacked. But the company that manufactures government computers or routers will likely also manufacture them for sale to civilians.⁷⁶ The software company that provides a “help desk” for government assistance will likely also have employees who work in the same area answering questions for civilians.⁷⁷ The company that produces security software and sends out “patches” to cover vulnerabilities will likely produce and send those patches to both government and civilians.⁷⁸ And fiber-optic

PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 41–68 (2009) (attempting to interpret “direct participation in hostilities” in a useful way with little guidance from the primary sources); Watts, *supra* note 15, at 392 (discussing the inadequacy of current law-of-war status determinations).

73. Daniel M. White, *The Federal Information Security Management Act of 2002: A Potemkin Village*, 79 *FORDHAM L. REV.* (forthcoming 2010).

74. *See supra* notes 63–65 and accompanying text.

75. *See Harris, supra* note 6 (noting that, in 2003, the United States decided against attacking Iraq’s military communications networks with a cyber attack because of intermixing with civilian systems).

76. Civilian objects that serve both civilian and military purposes are often termed “dual-use.” Jeanne M. Meyer, *Tearing Down the Facade: A Critical Look at the Current Law on Targeting the Will of the Enemy and Air Force Doctrine*, 51 *A.F. L. REV.* 143, 178 (2009). This term is somewhat misleading because at the point the civilian business or object serves a military purpose, it becomes a military object. The portions of that object that continue to provide services to civilians do not change the target back to a civilian object. Rather, they require the commander ordering the attack to consider that in his proportionality analysis discussed below.

77. *See, e.g.*, Microsoft Government, Contact Us, <http://www.microsoft.com/industry/government/products/contactus.mspx> (providing government users with contact information for support regarding Microsoft software).

78. *See, e.g.*, Microsoft Government, Microsoft Infrastructure Optimization Model, <http://www.microsoft.com/industry/government/solutions/itinfrastructureoptimization.mspx> (describing Microsoft services able to patch operating systems and desktops).

wires that carry military communications will also carry civilian communications. The portions of these companies or services that support the government may be legitimate targets under the law of war, while the portions that do not are protected from direct attack.⁷⁹ The civilian portions are not, however, preserved from the effects of attacks on legitimate military objectives. The case of a fiber-optic communication line is illustrative.

With 98% of day-to-day government communications routinely traveling over civilian communication lines, there will be many civilian lines of communication that will carry targetable electronic traffic intermixed with civilian traffic. Those specific military communications are still targetable, but the networks and lines would not be. However, because of the nature of electronic communications, it is very difficult to target a single communication once it is in transit.⁸⁰ The attacker may still be able to attack the military objective, such as the individual military communication, but he would have to determine that he could actually destroy or degrade the military communication and then weigh the military benefit of destroying that military communication against the incidental destruction to civilian networks and communications and ensure the destruction was not excessive compared to the benefit the attacker would receive. This analysis is known as the principle of proportionality, and it is contained in Article 57.2(a)(iii) of API.⁸¹

Article 57. Precautions in attack

1. In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.
2. With respect to attacks, the following precautions shall be taken:
 - (a) those who plan or decide upon an attack shall:
 - (i) do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them;
 - (ii) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event

79. See API, *supra* note 8, art. 52(2) (stating that attacks shall be limited to military objectives).

80. See E. Judson Jennings, *Carnivore: U.S. Government Surveillance of Internet Transmissions*, 6 VA. J.L. & TECH. 10, ¶¶ 8–9 (2001), <http://www.vjolt.net/vol6/issue2/v6i2-a10-Jennings.html> (describing the FBI's Carnivore program, which is used to intercept targeted communications, and explaining how “[a] single communication is broken into many smaller packets” when in transit).

81. API, *supra* note 8, art. 57(2)(a)(iii); E. L. Gaston, *Mercenarism 2.0? The Rise of the Modern Private Security Industry and Its Implications for International Humanitarian Law Enforcement*, 49 HARV. INT’L L.J. 221, 244 (2008).

to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects;

(iii) refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated⁸²

It is clear that these two fundamental law-of-war targeting provisions of military objective and proportionality apply to cyber attacks conducted during armed conflict.⁸³ Attackers can only target cyber elements that are military objectives, and any attacks against military objectives must comply with the principle of proportionality. There are many nuances to the application of these principles that are beyond the scope of this Article and have been amply covered elsewhere.⁸⁴ It is sufficient to establish that a state's cyber activities are targetable by an enemy and are likely to be attacked in times of armed conflict. Further, network and system operators who have military communications traversing their computers and networks may be opening themselves up to attack by an enemy that has performed a proportionality analysis and determined that the benefit of destroying these civilian networks and systems is not excessive considering the degradation to the U.S. government communications that would be achieved.

In addition to prescribing who and what an attacker can attack, the law of war also puts an affirmative obligation on the defender with regard to civilians and civilian objects.⁸⁵ This affirmative obligation is known as "precautions against the effects of attacks" and requires the defender to take certain precautions to protect civilians and civilian objects from the potential dangers of anticipated attacks.⁸⁶ This obligation to protect civilians and civilian objects has its modern foundation in the 1863 Lieber Code, which stated that "[c]lassical works of art, libraries, scientific collections, or precious instruments, such as astronomical telescopes, as well as hospitals, must be

82. API, *supra* note 8, art. 57.

83. See Eric Talbot Jensen, *Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1154–61 (2003) (reviewing the two-prong test that must be satisfied to overcome the preclusion against attacking civilian objects and issues related to its typical application and then applying those concepts to computer-networks attacks); Schaap, *supra* note 1, at 158 ("When analyzing the lawfulness of a cyber warfare operation one should conduct the same analysis as when determining the lawfulness of an aircraft targeting a military objective."). But see Watts, *supra* note 55, at 440–43, 446–47 (arguing that other principles of the law of war, such as the requirements for combat status, may need to be revised).

84. See Jensen, *supra* note 83, at 1154–61 (reviewing the requirements for attacking civilian objects where doing so serves military objectives and then applying those concepts to computer-networks attacks); Schaap, *supra* note 1, at 149–60 (analyzing the use of cyber-warfare operations in relation to the law of war).

85. API, *supra* note 8, art. 58.

86. *Id.*

secured against all avoidable injury, even when they are contained in fortified places whilst besieged or bombarded.”⁸⁷ While it is unclear from the text who had this responsibility, it presumably applied to whomever was in possession of the civilian objects, which would certainly have been the defender in many cases, such as in a siege or bombardment.

The affirmative obligation was clarified in the Annex to the 1907 Hague Convention IV.⁸⁸ In Article 27, it states that the besieged has the duty to indicate the presence of “buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected . . . by distinctive and visible signs, which shall be notified to the enemy beforehand.”⁸⁹ The same Article imposes a responsibility on the attacker to spare such marked buildings “provided they are not being used at the time for military purposes.”⁹⁰

This principle of a defender’s responsibility to protect civilians and civilian objects was revisited in the preparations for the 1977 conference that produced the Additional Protocols to the 1949 Geneva Conventions.⁹¹ The International Committee of the Red Cross (ICRC) proposed a text that became the basis for the conference’s negotiations.⁹² This draft contained a provision—originally Article 51, but it would eventually become Article 58—that concerned the defender’s responsibilities for its civilians and civilian objects. The obligation was basically set in the alternative: either

87. FRANCIS LIEBER, WAR DEP’T, INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD ¶ 35 (1863) [hereinafter LIEBER CODE], *reprinted in* 2 FRANCIS LIEBER, THE MISCELLANEOUS WRITINGS OF FRANCIS LIEBER: CONTRIBUTIONS TO POLITICAL SCIENCE 245, 254 (1881). Two other provisions allow for the protection of certain civilian objects but do not make it an affirmative obligation:

115. It is customary to designate by certain flags (usually yellow) the hospitals in places which are shelled, so that the besieging enemy may avoid firing on them. The same has been done in battles, when hospitals are situated within the field of the engagement.

....

118. The besieging belligerent has sometimes requested the besieged to designate the buildings containing collections of works of art, scientific museums, astronomical observatories, or precious libraries, so that their destruction may be avoided as much as possible.

Id. at 267, 268.

88. Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land art. 27, Oct. 18, 1907, 1 Bevans 631 [hereinafter Hague IV].

89. *Id.*

90. *Id.*

91. 1 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE ON THE REAFFIRMATION AND DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICTS, GENEVA (1974–1977), pt. 1, at 3 (1978) [hereinafter OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE].

92. *Id.*

protect the civilians under your control or segregate them from areas where they are endangered. The draft proposal initially stated:

Article 51. Precautions against the effects of attacks

1. The Parties to the conflict shall, to the maximum extent feasible, take the necessary precautions to protect the civilian population, individual civilians and civilian objects under their authority against the dangers resulting from military operations.
2. They shall endeavour to remove them from the proximity of military objectives, subject to Article 49 of the Fourth Convention, or to avoid that any military objectives be kept within or near densely populated areas.⁹³

Once the conference convened, the draft was sent to a working group where the discussion seemed to revolve around two key points: the practicability of the obligation and whether the obligation was *de facto* or *de jure*.⁹⁴ The representative from Canada, Brigadier General (BG) J.P. Wolfe, who was the Judge Advocate General for the Department of National Defense, proposed two changes that dealt with both of these concerns.⁹⁵ In the first proposal, BG Wolfe urged changing the language of paragraph one from “authority” to “control.” He argued that “use of the word ‘control’ would impose obligations on the parties which would not necessarily be implied by the use of the word ‘authority.’ It referred to the *de facto* as opposed to the *de jure* situation.”⁹⁶ It is clear from the negotiating record that this proposed amendment was viewed mostly in terms of geography, and that phenomena such as the Internet were not envisioned in the deliberations.⁹⁷ Therefore, control was thought of as a territorial term.⁹⁸ The proposed amendment was eventually accepted.⁹⁹

The second proposal by BG Wolfe was to have the limiting language, “to the maximum extent feasible,” apply generally to the Article, rather than to the first paragraph only.¹⁰⁰ His concern was reflected by several other delegations who were concerned that “countries would find it difficult to

93. *Id.* art. 51, at 17.

94. 14 *id.* at 198–99 (“[T]he use of the word ‘control’ would impose obligations on the parties which would not necessarily be implied by the use of the word ‘authority.’ It referred to the *de facto* as opposed to the *de jure* situation.”).

95. *Id.* at 198–99.

96. *Id.* at 198.

97. 1 *id.* pt. 1, art. 51, at 147; COMMENTARY TO THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 692 (Yves Sandoz et al. eds., 1987).

98. COMMENTARY TO THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, *supra* note 97, at 692. It is interesting to note here that the United States has recently begun to view cyberspace as a domain equal to air, land, and sea. See Ellen Nakashima, *Pentagon to Announce ‘Cyber Command,’* WASH. POST, June 13, 2009, at A5 (articulating the Pentagon’s “cyber-command” strategy).

99. API, *supra* note 8, art. 58.

100. 14 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE, *supra* note 91, at 199.

separate civilians and civilian objects from military objectives.”¹⁰¹ John Redvers Freeland, the United Kingdom head of delegation for the second, third, and fourth sessions, emphasized that protections such as those contemplated in Article 51 can “never be absolute” and that the words “to the maximum extent feasible” related to what was “workable or practicable, taking into account all the circumstances at a given moment, and especially those which had a bearing on the success of military operations.”¹⁰² This same idea was advocated by S.H. Bloembergen, a delegate from the Netherlands, who stated that “feasible” should be “interpreted as referring to that which was practicable or practically possible, taking into account all circumstances at the time.”¹⁰³

After modification in the working group to its present form, the Article was voted on and adopted by consensus¹⁰⁴ with George H. Aldrich, the head of the U.S. delegation, reporting that the modified text “had been the most generally acceptable”¹⁰⁵ to those involved in the negotiations. As amended and approved, the new Article 58 states:

The Parties to the conflict shall, to the maximum extent feasible:

- (a) Without prejudice to Article 49 of the Fourth Convention, endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;
- (b) Avoid locating military objectives within or near densely populated areas;
- (c) Take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.¹⁰⁶

Though modified and reordered, the two fundamental alternatives from the original Article 51 remain the gravamen of the Article: either protect the civilians under your control or segregate them from areas where they are endangered.¹⁰⁷ Reinforcing the understanding during the negotiations, many states added declarations upon signature of the API that these obligations were subject to the language, “maximum extent feasible,” and that such language required only that which was practicable, based on the conditions and situation prevailing at the time.¹⁰⁸

101. 15 *id.* at 353.

102. 6 *id.* at 214.

103. *Id.*

104. 14 *id.* at 304.

105. *Id.*

106. API, *supra* note 8, art. 58.

107. *See supra* note 93 and accompanying text.

108. *See* International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, <http://www.icrc.org/ihl.nsf/WebSign?ReadForm&id=470&ps=P>

The United States is a signatory to the API but not a party because the Senate has never given its advice and consent.¹⁰⁹ However, in his seminal article on the United States' position concerning the API, Mike Matheson stated that the United States "support[ed] the principle" in Article 58.¹¹⁰ Additionally, not only is there no record of any statements by the U.S. government against Article 58, but the U.S. Navy's military manual states the principle as applicable to U.S. operations.¹¹¹ Further, in its recent Customary International Humanitarian Law Study, the ICRC lists precautions against the effects of attacks as customary international law,¹¹² binding on all states whether or not they are parties to the API.¹¹³ While there has been no official statement, there is also no indication that the United States would not accept the provisions of Article 58 as an affirmative obligation during armed conflict.

Accepting Article 58's obligation to segregate or protect, either as binding on the United States or as a principle the United States would accede to in armed conflict, the following example is typical of an application of Article 58 to a non-cyber armed-conflict situation. Assume the military determined that it needed to establish a military-supply depot at a normally civilian seaport. Because of the military's use of the seaport, that part used by the military would become a military objective under Article 52 and would

(listing the state parties and signatories to the API). In particular, the declarations of Algeria, Australia, Austria, Belgium, Canada, Ireland, Italy, the Netherlands, New Zealand, Spain, and the United Kingdom describe this "practicable" framework. *Id.* (follow "text" hyperlink for each).

109. See Theodor Meron, Editorial Comment, *The Time Has Come for the United States to Ratify Geneva Protocol I*, 88 AM. J. INT'L L. 678, 678–80 (1994) (describing President Regan's request that the Senate give its advice and consent to the ratification of Protocol II alone); International Committee of the Red Cross, *supra* note 108 (noting that a state becomes a party by signing and ratifying a treaty).

110. See Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y 419, 426–27 (1987) ("We support the principle that all practicable precautions, taking into account military and humanitarian considerations, be taken in the conduct of military operations to minimize incidental death, injury, and damage to civilians and civilian objects . . ."). *But see* Memorandum for John H. McNeill, Assistant Gen. Counsel (International), OSD (May 9, 1986), in LAW OF WAR DOCUMENTARY SUPPLEMENT 399–401 (Porter Harlow ed., 2008) (describing the portions of API that law-of-war experts thought were either part of customary international law or supportable for inclusion as customary international law through state practice, and noting that Article 58 was not listed in the memorandum).

111. See U.S. DEP'T OF THE NAVY, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ¶ 8.3.2 (2007) ("A party to an armed conflict has an affirmative duty to remove civilians under its control (as well as the wounded, sick, shipwrecked, and prisoners of war) from the vicinity of objects of likely enemy attack."):

112. 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 68–71 (2005). The study lists Rule 22 as, "The parties to the conflict must take all feasible precautions to protect the civilian population and civilian objects under their control against the effects of attacks." *Id.* at 68.

113. See Source: Custom, 1 HACKWORTH DIGEST § 3, at 15–17 (explaining that a rule of international law can develop from the practice of states if it has been of "sufficient duration and uniformity").

be targetable. If an enemy decided to attack the seaport, it would have to conduct a proportionality analysis under Article 57 based on the potential injury or death to civilians and damage to the civilian portions of the port area.¹¹⁴

Anticipating the potential for attack, under Article 58(a), the defending military would be obligated to the “maximum extent feasible” to “endeavour” to remove the civilians and civilian-shipping concerns from that portion of the seaport so if the enemy decided to attack the military portion of the port, that attack would put the fewest number of civilians and civilian objects at risk.¹¹⁵ Additionally, under Article 58(b), if the seaport was in the midst of a densely populated area, the military would have to try to situate its portions of the seaport as far away from the civilian population as feasible.¹¹⁶

Applying this analysis to cyber warfare illustrates the immediate difficulties inherent in the interconnectedness of U.S. government and civilian systems and the near-complete government reliance on civilian companies for the supply, support, and maintenance of its cyber capabilities. The U.S. government cannot, at this point, segregate its cyber capabilities from civilians and civilian objects. Given that 98% of the government’s communications go through civilian networks and systems over civilian lines,¹¹⁷ such segregation would require the government to establish its own lines of communication throughout the world,¹¹⁸ connecting its dispersed military installations.¹¹⁹ The government would also have to create its own computer hardware and software companies that could produce, support, and maintain state-of-the-art computer capabilities. Further, the government would have

114. API, *supra* note 8, art. 57.

115. *Id.*

116. *Id.*

117. *See supra* note 2 and accompanying text.

118. While the government is working on the “Global Information Grid,” a part of which would include secure computing and communications infrastructure, the current vision is only of a future system that is not within today’s technological capabilities. *See* U.S. DEP’T OF DEF., GLOBAL INFORMATION GRID ARCHITECTURAL VISION 1–6 (2007), available at <http://cio-nii.defense.gov/docs/GIGArchVision.pdf> (“The current GIG is characterized by organizational and functional stovepipe systems with varying degrees of interoperability and constrained access to needed information. It does not sufficiently exploit the potential of information age technologies, and does not fully support the operational imperative for the right information at the right time.”); Chris Paine, *U.S. Military to Install Global Internet Architecture Giving a “God-Like” View of Planet*, INFOWARS.COM, July 13, 2009, <http://www.infowars.com/u-s-military-to-install-global-internet-architecture-giving-a-god-like-view-of-planet/> (“The GIG, or Global Information Grid is a worldwide surveillance network that will give anyone linked into it instant information, at the users request, about anything, anytime, anywhere in the world!”); *cf. State’s Fibre Optic Cable Raises Cost, Benefits Questions*, STABROEK NEWS, Feb. 7, 2010, <http://www.stabroeknews.com/2010/stories/02/07/state%E2%80%99s-fibre-optic-cable-raises-cost-benefits-questions/print/> (analyzing Guyana’s plan to create a fiber-optic cable exclusively dedicated to e-governance).

119. *See* Lynn, *supra* note 41 (stating that the DOD currently uses 15,000 networks across 4,000 military installations in eighty-eight different countries).

to establish its own system of routers, switches, and telecom hotels to manage and protect these communications.

While these options may be conceivably “feasible,” they are not “practicable,” to use the words from Bloembergen during the negotiations.¹²⁰ Rather, the current practice of governments, and certainly the U.S. government, appears to embrace the interconnectedness with civilian systems, making segregation under Article 58(a) and (b) infeasible.¹²¹ Even understanding the risk associated with the interconnectedness of military and civilian cyber systems, governments have not taken affirmative steps to segregate military and civilian systems. If anything, the tendency is to move toward more interconnectivity.¹²² Segregation is not the preferred option for meeting obligations under Article 58 to protect civilians and civilian objects against the effects of attack.

But that must not be the end of the inquiry. It is certainly not in keeping with the spirit of the law of armed conflict for government action to bring civilians and civilian companies within the scope of lawful attacks and then to allow those same governments to leave the civilians and civilian companies completely alone to defend themselves. In fact, this is not the state of the law. Rather, in the absence of the feasibility of segregation under Article 58(a) and (b), governments accept the obligation of protection under Article 58(c).¹²³

IV. Alternative Responsibilities Under Article 58(c)

While cyber segregation is an overwhelming task, effective cyber protection is only slightly less daunting.¹²⁴ Understanding what Article 58(c)

120. 6 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE, *supra* note 91, at 214.

121. See Harris, *supra* note 6 (relating fears that Iraqi military communications networks were potentially connected to French banking networks); *supra* notes 9–12 and accompanying text.

122. See ARNAUD DE BORCHGRAVE ET AL., CTR. FOR STRATEGIC & INT’L STUDIES, CYBER THREATS AND INFORMATION SECURITY: MEETING THE 21ST CENTURY CHALLENGE 7 (2000) (estimating that in 2000, the rate of interconnectedness was 95%).

123. See API, *supra* note 8, art. 58(c) (requiring the government to take all other necessary precautions to protect civilians from the dangers of military operations).

124. See Sklerov, *supra* note 53, at 26. In analyzing the effectiveness of U.S. cyber protection, Lieutenant Commander Sklerov observes,

Unfortunately, computer security in its present form is not enough to stop cyberattacks. Computer software frequently has design flaws that open systems to attack, despite system administrators’ best efforts to fully secure their computer systems. These design flaws are compounded by administrator and user carelessness in both system design and use, which often nullify the security measures put in place to defend a system. Furthermore, poor design of federal computer networks has left them with more entry points than U.S. early warning programs can effectively monitor at one time, leaving U.S. computer systems vulnerable to attack until the amount of entry points is reduced. These vulnerabilities highlight the fact that passive defenses alone are not enough to protect states from cyberattacks.

Id. Sklerov advocates for the use of “active defenses” to protect critical computer networks and systems against states that do not prevent attacks from within their territory. *Id.*

does and does not require is vital to complying with the obligation it imposes. Based on the negotiating history already discussed and the plain reading of the text, it appears that there are three key concepts in the Article: “to the maximum extent feasible,” “other necessary precautions,” and “under their control.”¹²⁵ The first and last of these act to limit the extent of required government action, while the second acts to force otherwise deferred action.

In analyzing Article 58(c)’s application to cyber warfare, it is important to note the negotiators were clear that the language of “to the maximum extent feasible” applied to the entire Article, making the obligation to protect subject to this same caveat.¹²⁶ As one cyber expert recently stated, it is not possible to protect all the networks all the time.¹²⁷ Recognizing that it is not feasible to protect everything all the time requires some decision methodology. While some have argued for protection of critical national infrastructure as a top priority,¹²⁸ this category may be broader than the contours of Article 58 require. Each state will have to make its own determination as to what is feasible, but it is important to note that the language is the “maximum” extent, not the minimum.¹²⁹

The second concept that acts to limit the required government action is the language concerning control of civilians and civilian objects. The Article only requires governments to protect those civilians and civilian objects that are “under their control.”¹³⁰ Returning to the non-cyber example of the military use of the seaport, under Article 58(c), if certain civilians or civilian objects came under the control of the military at the seaport, the military would be obliged to take necessary precautions to protect those civilians and civilian objects from the dangers resulting from military operations, including attacks by the enemy.¹³¹ This might include actions such as segregating civilians and civilian objects as much as possible within the military portions of the seaport, placing civilian work spaces in protected areas such as in buildings or bunkers, or creating evacuation plans that would quickly move civilians to a safer location in the event of attack.

125. API, *supra* note 8, art. 58(c).

126. 14 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE, *supra* note 91, at 199.

127. Colonel Guillermo R. Carranza, Remarks at the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology (Feb. 6, 2010).

128. See Sean M. Condrón, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 404, 407 (2007) (asserting that critical infrastructure is vital to a nation’s survival and that a safe and secure cyber environment is necessary to support the critical infrastructure); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense*, 38 STAN. J. INT’L L. 207, 229 (2002) (arguing that the United States must “establish a domestic practice of protecting its critical national infrastructure” against computer-network attacks); Sklerov, *supra* note 53, at 26 (arguing that current computer security is not enough to stop cyber attacks and, as a consequence, states will feel the need to build active defenses).

129. API, *supra* note 8, art. 58.

130. *Id.*

131. *Id.*

Similarly, any computers, networks, systems, routers, telecom hotels, etc., would have to be under the control of the government to come under this obligation. Recall that during the negotiations this provision was meant to be understood as a *de facto* standard, not *de jure*.¹³² One scenario where this provision gives meaning to the obligation would be a cyber attack launched by an enemy where the government determined it was necessary to take control of a particular computer network, securing the portions necessary to ensure continuity of government operations. The network would continue to be a civilian object, though discrete military communications would be targetable.¹³³ Once the government took control of the network, it would have to accept the obligation to protect the entire network, including the civilian communications traffic.¹³⁴

Another example might be a telecom hotel through which valuable military communications pass between the continental United States and Europe. During an armed conflict, the government might take physical and cyber control to ensure its military communications were uninterrupted. Countless civilian communications would pass through that same telecom hotel, and the U.S. government would have to accept the obligation to protect those communications as well.

Finally, Article 58(c) requires the government to take “other necessary precautions.”¹³⁵ This language is significant for at least two reasons. First, the word “other” seems to indicate that the required actions may involve more than just additional segregation. In other words, if segregating under the preceding two paragraphs of Article 58 were not feasible, the government cannot meet the obligation of paragraph (c) merely by segregating those civilian cyber activities “under their control” and then leaving them to fend for themselves. Once the government accepts the obligation to protect, other “feasible” precautions are required.

Second, the use of the term “precautions” is significant. Precautions note actions taken in advance, not just in response.¹³⁶ This is particularly appropriate in the context of cyber warfare where an attack can happen in the time it takes to make a keystroke, sending a destructive stream of electrons into an enemy’s computer system. With a damaging cyber attack so instantaneous, the government cannot take this obligation as a reactionary responsibility. Rather, the government has to act in advance of a potential attack. And since no one knows when that potential attack will come, the

132. *See supra* notes 93–99 and accompanying text.

133. *See supra* notes 74–81 and accompanying text.

134. *See* API, *supra* note 8, art. 58 (requiring governments to protect civilian objects under their control from the dangers of military operations).

135. *Id.*

136. Precaution is “a measure taken beforehand to prevent harm or secure good.” MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY 976 (11th ed. 2003).

government has to act now to ensure potential civilian cyber activities that either are or will come under its control will be adequately protected.

This, then, becomes the crux of the requirement for the government. It requires some forethought and immediate action. It requires the government to analyze which of its cyber capabilities it will want to guarantee functionality when an armed conflict occurs. Then, the government must determine what civilian systems, companies, networks, etc., are necessary to maintain that functionality. Having made that determination, the government must act now to put the necessary steps in place to protect those civilians and civilian objects which will likely come under its control. Waiting until these systems are under attack will not meet the obligations of Article 58 and the law of armed conflict.¹³⁷ Immediate action is required.

One complicating factor is that such actions will require specific legal authority and significant cooperation with the private sector. As one commentator recently noted concerning cyber protection, “[T]he list of powers granted to the President in carrying out his duties as Commander in Chief is devoid of any authority to defend private industry.”¹³⁸ The next Part will review steps already taken by the government to ensure continuing cyber functionality in the face of an armed attack.

V. U.S. Practice in Protecting Civilians and Civilian Cyber Objects

Beginning in the 1990s, as the U.S. government’s use of the Internet increased and its dependence on the Internet for communication and functionality expanded, the need for protection became more apparent. The actions taken over the ensuing two decades have been detailed elsewhere¹³⁹ and need not be repeated here. However, it is worth drawing attention to several specific provisions or actions that delineate the government’s plans on protecting civilians and civilian objects from the effects of potential attacks.

Initially, the government’s predominant focus for protection was critical national infrastructure.¹⁴⁰ In hindsight, this decision seems prescient, as re-

137. See API, *supra* note 8, art. 58 (prescribing various mechanisms to be taken by the parties to a conflict to protect individuals from the effects of attacks).

138. Todd A. Brown, *Legal Propriety of Protecting Defense Industrial Base Information Infrastructure*, 64 A.F. L. REV. 211, 220 (2009).

139. See *id.* at 219–20 (discussing the Homeland Security Act of 2002); Kastenber, *supra* note 67, at 48–50 (describing various executive and legislative initiatives taken to safeguard U.S. infrastructure); Sklerov, *supra* note 53, at 25–26 (outlining efforts to ensure that the private sector acts on both computer security and a government early-warning system for cyber attacks); U.S. DEP’T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 185 app. 2 (2009), http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf [hereinafter NIPP] (containing a comprehensive list of U.S. statutes, strategies, and directives dealing with infrastructure protection).

140. “Critical infrastructure” is defined in the relevant U.S. Code as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such

cent history has shown an ever-increasing focus of attacks on critical infrastructure.¹⁴¹ In 1997, President Clinton created the President's Commission on Critical Infrastructure Protection and followed in 1998 by issuing Presidential Decision Directive 63, concerning protection of U.S. critical infrastructure.¹⁴² The Directive made it the policy of the U.S. government to "take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."¹⁴³ The Directive recognized the need for strong public-private partnership and urged that "[s]ince the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector."¹⁴⁴

In 2002, Congress passed the Homeland Security Act, which authorized the President and the Secretary of Homeland Security to designate critical-infrastructure-protection programs.¹⁴⁵ As a result of this authority, the President "issued a number of directives designating critical infrastructure protection programs and describing responsibilities therein."¹⁴⁶ One of these directives was the Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection¹⁴⁷ (HSPD-7). Issued in December of 2003, HSPD-7 states very clearly the policy of the United States at least with regard to protection of critical infrastructure from terrorist attacks:

It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:

- (a) cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;
- (b) impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;
- (c) undermine State and local government capacities to maintain order and to deliver minimum essential public services;

systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e) (2006).

141. See Press Release, *supra* note 37 (noting cyber attacks on the White House, DHS, U.S. Secret Service, and DOD).

142. Memorandum on Critical Infrastructure Protection, Presidential Decision Directive/NSC-63 (May 22, 1998), available at <http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf>.

143. *Id.* at 2.

144. *Id.* at 3.

145. Homeland Security Act of 2002, Pub. L. No. 107-296, § 213, 116 Stat. 2135, 2152 (codified at 6 U.S.C. § 132 (2006)).

146. Brown, *supra* note 138, at 220.

147. 39 WEEKLY COMP. PRES. DOC. 1816 (Dec. 17, 2003).

- (d) damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
- (e) have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or
- (f) undermine the public's morale and confidence in our national economic and political institutions.¹⁴⁸

As directed in HSPD-7, the government created a National Infrastructure Protection Plan (NIPP) in 2006 and updated it in 2009.¹⁴⁹ Within the NIPP, the DOD was assigned as the Sector Specific Agency (SSA) for the Defense Industrial Base (DIB).¹⁵⁰ As the SSA for the DIB, DOD has the responsibility to "implement the NIPP sector partnership model and risk management framework; develop protective programs, resiliency strategies, and related requirements; and provide sector-level [critical infrastructure and key resources (CIKR)] protection guidance in line with the overarching guidance established by DHS pursuant to HSPD-7."¹⁵¹ Also, the NIPP discusses the National Infrastructure Inventory, a "national inventory of the assets, systems, and networks that make up the nation's CIKR."¹⁵²

As part of its responsibility under the NIPP, DOD issued its sector-specific plan for the DIB (DIB SSP) in May 2007.¹⁵³ One of the key points in the plan is that "[p]rivate sector participation in executing the NIPP is voluntary."¹⁵⁴ The DIB SSP acknowledges that "[c]urrently, there are no regulatory requirements for conducting formal risk assessments" within the DIB.¹⁵⁵ In fact, critical-infrastructure executives in the United States reported the "lowest levels" of government regulation across the fourteen countries surveyed.¹⁵⁶ In response, DOD has conducted risk assessments on portions of the DIB of its own accord.¹⁵⁷ However, DOD admits that it is not conducting comprehensive risk assessments on the DIB in the area of cyber assets. The DIB SSP states, "While cyber security is an issue that could affect any facility, DOD does not perform network- or system-level assessments."¹⁵⁸

148. *Id.* at 1817.

149. NIPP, *supra* note 139, at 7–8.

150. *Id.* at 19.

151. *Id.* at 18.

152. *Id.* at 29.

153. U.S. DEP'T OF DEF., DEFENSE INDUSTRIAL BASE: CRITICAL INFRASTRUCTURE AND KEY RESOURCES SECTOR-SPECIFIC PLAN AS INPUT TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN (2007), available at <http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf>.

154. *Id.* at 4.

155. *Id.* at 17.

156. BAKER ET AL., *supra* note 24, at 1.

157. U.S. DEP'T OF DEF., *supra* note 153, at 17.

158. *Id.*

In February 2003, the President issued the National Strategy to Secure Cyberspace.¹⁵⁹ While this strategy encourages public-private coordination on securing critical infrastructure, it also expands the scope of government concern to include “reduc[ing] our national vulnerabilities to cyber attack.”¹⁶⁰ Enlarging the aperture by which the government is directing policy from critical infrastructure to national vulnerabilities is laudable. However, the strategy also states that “[t]he federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector.”¹⁶¹

In 2008, President Bush also issued NSPD-54/HSPD-23 creating the Comprehensive National Cybersecurity Initiative.¹⁶² This NSPD takes a broader view than just critical infrastructure, though it is mostly focused on government networks.¹⁶³ Though the NSPD is not available to the public, one commentator recently stated,

President Bush, by means of a classified directive signed on 8 January 2008, authorized federal intelligence agencies, in particular the National Security Agency (NSA), to monitor the computer networks of all federal agencies, including those they had not previously monitored. Pursuant to this directive, a task force headed by the Office of the Director of National Intelligence (ODNI) will coordinate efforts to identify the source of cyber-attacks against government computer systems. The DHS and DOD will take ancillary roles in this effort—protecting systems and devising strategies for counterattacks.¹⁶⁴

In March of 2009, the GAO released a report on National Cybersecurity Strategy.¹⁶⁵ The report finds that “DHS has yet to fully satisfy its cybersecurity responsibilities designated by the [2003 National Strategy to Secure Cyberspace].”¹⁶⁶ The report does admit some progress in many areas,

159. WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf. In 2004, President Bush issued National Security Presidential Directive 38 (NSPD-38), also called the National Strategy to Secure Cyberspace. The 2004 document is not available to the general public due to its classification.

160. *Id.* at 14.

161. *Id.* at 11.

162. JOHN ROLLINS & ANNA C. HENNING, CONG. RESEARCH SERV., COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS 1 (2009).

163. *See id.* at 7 (“[T]he primary response and recovery activities associated with previous [private] network breaches have been addressed by the private sector entity that has been the victim of the attack.”).

164. Brown, *supra* note 138, at 240–41; *see also* Ellen Nakashima, *Bush Order Expands Network Monitoring*, WASH. POST, Jan. 26, 2008, at A3 (providing additional description of the directive issued by President Bush).

165. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-432T, NATIONAL CYBERSECURITY STRATEGY: KEY IMPROVEMENTS ARE NEEDED TO STRENGTHEN THE NATION'S POSTURE (2009).

166. *Id.* at 4.

but also contains twelve recommendations that still need attention.¹⁶⁷ One of those recommendations is to “[f]ocus more actions on prioritizing assets and functions, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.”¹⁶⁸ The report goes on to say,

[E]fforts to identify which cyber assets and functions are most critical to the nation have been insufficient [I]nclusion in cyber critical infrastructure protection efforts and lists of critical assets are currently based on the willingness of the person or entity responsible for the asset or function to participate and not on substantiated technical evidence.¹⁶⁹

Shortly after entering office, President Obama ordered a comprehensive review of the U.S. cyber strategy.¹⁷⁰ This review resulted in the Cyberspace Policy Review.¹⁷¹ The Review argued,

The Federal government cannot entirely delegate or abrogate its role in securing the Nation from a cyber incident or accident. The Federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and well-being of citizens. The private sector, however, designs, builds, owns, and operates most of the digital infrastructures that support government and private users alike. The United States needs a comprehensive framework to ensure a coordinated response by the Federal, State, local, and tribal governments, the private sector, and international allies to significant incidents.¹⁷²

In light of Article 58 obligations, this framework should include the protection of certain civilian networks and systems from the effects of attacks.

Among the many recommendations made in the Review, perhaps the most pertinent to this Article concerns the protection of private networks:

The Federal government should work with the private sector to define public-private partnership roles and responsibilities for the defense of privately owned critical infrastructure and key resources. The common defense of privately-owned critical infrastructures from armed attack or from physical intrusion or sabotage by foreign military forces or international terrorists is a core responsibility of the Federal government. Similarly, government plays an important role in protecting these infrastructures from criminals or domestic terrorists. The question remains unresolved as to what extent protection of these

167. *Id.* at 6–12.

168. *Id.* at 9.

169. *Id.* at 10.

170. *Id.* at 4.

171. WHITE HOUSE, CYBERSPACE POLICY REVIEW (2009), available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

172. *Id.* at iv–v.

same infrastructures from the same harms by the same actors should be a government responsibility if the attacks were carried out remotely via computer networks rather than by direct physical action. Most private network operators and service providers consider it to be their responsibility to maintain and defend their own networks, but key elements of the private sector have indicated a willingness to work toward a framework under which the government would pursue malicious actors and assist with information and technical support to enable private-sector operators to defend their own networks.¹⁷³

The DOD has also been actively pursuing its abilities to defend cyberspace, including civilian elements that are necessary to support military capabilities. In a recent address, Deputy Secretary of Defense William Lynn stated, “[T]he Defense Department has formally recognized cyberspace for what it is—a domain similar to land, sea, air and space. A domain that we depend upon and must protect.”¹⁷⁴ He continued,

Our defenses need to be dynamic. A fortress mentality will not work in cyber. We cannot retreat behind a Maginot line of firewalls. Cyber war is much more like maneuver warfare, and these new technologies help us find and neutralize intrusions. But we must also keep maneuvering. If we stand still for a minute our adversaries will overtake us.¹⁷⁵

It may be that the majority of cyber attacks against U.S. systems come from private individuals, but as CSIS reported in its report for the incoming President, “Our most dangerous opponents are the militaries and intelligence services of other nations.”¹⁷⁶ To help respond to the increasing capability and lethality of cyber attacks, Defense Secretary Robert Gates announced in June 2009 the creation of U.S. Cyber Command, which will be tasked with “protecting and coordinating the nation’s computer and defense networks and infrastructure.”¹⁷⁷ According to Deputy Secretary Lynn,

Cyber Command will bring together more than half a dozen intelligence and military organizations in support of three overlapping categories of cyber operations. First, CYBERCOM will lead the day to day defense and protection of all DoD networks, raising our situational awareness and control. Second, CYBERCOM will coordinate all DoD network operations providing full spectrum

173. *Id.* at 28.

174. Lynn, *supra* note 41.

175. *Id.*

176. COMM’N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, *supra* note 38, at 13; *see also* Elinor Mills, *Report: Countries Prepping for Cyberwar*, CNN, Nov. 16, 2009, <http://www.cnn.com/2009/TECH/11/17/cnet.cyberwar.internet/index.html?iref=allsearch> (suggesting that countries and nation-states are gearing up their offensive “cyberweapon” capabilities and may already be engaged in attacks on networks).

177. Ryan Justin Fox, *Fort Meade to Be Cyber Defense Home*, CAPITAL, Oct. 12, 2009, available at <http://www.hometownannapolis.com/news/top/2009/10/12-14/Fort-Meade-to-be-cyber-defense-home.html>.

support to military and counter-terrorism missions. Third, CYBERCOM will stand by to support civil authorities and industry partners on an as-needed basis.¹⁷⁸

The new Cyber Command falls under Strategic Command or STRATCOM, one of the unified and specified commands created by statute to conduct the nation's warfighting.¹⁷⁹ "Part of USSTRATCOM's mission is to ensure freedom of action in cyberspace and to deliver integrated kinetic and non-kinetic effects, including information operations, in support of Joint Force Commander operations."¹⁸⁰ This freedom of action would certainly include the ability to use certain civilian networks in times of armed conflict.

It is clear that the government is taking important steps to include critical civilian networks, systems, and infrastructure under its protective umbrella.¹⁸¹ However, there are three consistent problems with the government's approach. The first is that a majority of these plans and policies depend on the voluntary assent of the private sector. This includes relying on the civilian sector to assess vulnerabilities and execute solutions. Second, the consistent approach throughout these policies and plans is reactive, not proactive. Remediation and damage management are consistent themes, with only little attention to prevention, detection, and protection. Finally, these plans and policies do not assign the appropriate role for DOD, given the potential for cyber attack as part of armed conflict.

In the absence of a legal obligation, allowing the private sector to govern itself may be appropriate to some degree. However, given the government's legal obligation imposed by Article 58 to protect civilian objects under government control during times of armed conflict, a voluntary regime is not sufficient. In failing to make assessments mandatory, these plans and policies leave the government in the situation of not knowing the complete scope of the problem—who they need to protect and to what extent.¹⁸² HSPD-7's authorization for DHS to provide protection and guidance to the private sector¹⁸³ carries no mandatory compliance requirements and is insufficient to meet the United States' legal obligations. The 2003 National Strategy to Secure Cyberspace's statement that the government "should not" secure private-sector systems denotes a lack of acceptance

178. Lynn, *supra* note 41.

179. *See* 10 U.S.C. § 161 (2006) (authorizing the creation of commands to conduct military missions).

180. Schaap, *supra* note 1, at 130.

181. *See supra* notes 171–73 and accompanying text.

182. *See supra* note 169 and accompanying text.

183. *See* Homeland Security Presidential Directive 7, *supra* note 147, at 1817 ("Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective.").

of the responsibility under Article 58.¹⁸⁴ As long as participation in the government's cybersecurity plan is voluntary, the results will be uneven and insufficient. The Cyberspace Policy Review had it exactly right when it said that "[t]he common defense of privately-owned critical infrastructures from armed attack or from physical intrusion or sabotage by foreign military forces or international terrorists is a core responsibility of the Federal government."¹⁸⁵ The government needs to listen and respond.

Additionally, throughout the DIB SSP, it is clear that the government takes a reactive approach to asset protection. In laying out a strategy for layered defense, the federal government is the fifth (and last) level and is appropriate only after local authorities, state or local law enforcement, and the state's national guard or other federal agencies have all failed, and the President determines it is then appropriate to use military assets.¹⁸⁶ Though the DIB SSP states that it is DOD's goal to prevent and detect potential incidents,¹⁸⁷ there is no requirement for members of the DIB to support this goal or take any actions at all toward this end. This approach is insufficient in a technological age where the attack can be an instantaneous burst of electrons that will destroy or significantly degrade the cyber capabilities of a critical infrastructure that the United States may be obliged to protect. NSPD-54's requirement of monitoring is a step in the right direction, but it falls short of providing the protection required under Article 58.¹⁸⁸

Finally, while perhaps the focus on terrorist attacks can be overlooked since HSPD-7 was promulgated in the wake of the September 11 attacks,¹⁸⁹ the current government approach fails to recognize the central role DOD will have to play in response to a cyber attack. This sentiment is echoed in a 2007 GAO report, where the GAO found that "DOD relies so heavily on non-DOD infrastructure assets that their unavailability could critically hinder the DOD's ability to project, support, and sustain forces and operations worldwide."¹⁹⁰ The report's assumption that protection from armed attack, even of private critical networks, was the responsibility of the government is

184. See WHITE HOUSE, *supra* note 159, at 11. In reference to the government's responsibility in cybersecurity, the policy states,

The federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector. . . . Each American who depends on cyberspace, the network of information networks, must secure the part that they own or for which they are responsible.

Id.

185. WHITE HOUSE, *supra* note 171, at 28.

186. U.S. DEP'T OF DEF., *supra* note 153, at 23.

187. *Id.* at 24.

188. See *supra* text accompanying note 164.

189. See *supra* text accompanying notes 145–48.

190. Brown, *supra* note 138, at 234 (citing U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-461, DEFENSE INFRASTRUCTURE: ACTIONS NEEDED TO GUIDE DOD'S EFFORTS TO IDENTIFY, PRIORITIZE, AND ASSESS ITS CRITICAL INFRASTRUCTURE 1 (2007)).

a recognition of the same principles Article 58 enshrines, and DOD will be the primary government actor to provide that protection.¹⁹¹ When armed conflict begins and cyber attacks hit U.S. networks, the President is not going to turn to DHS and ask what it is doing about it. The responsibility is going to fall to DOD. The government needs to embrace that reality now and adjust its plans and policies accordingly.

VI. Recommendations

In his speech quoted at the beginning of this Article, which was given in response to the Cyberspace Policy Review, President Obama acknowledged the need for greater work to protect the United States' communications capabilities.¹⁹² The nature of the Internet prevents effective post-attack protection when facing the instantaneous degradation of cyber capabilities. To effectively protect civilian networks and systems in accordance with the United States' obligations under Article 58(c), the government must take affirmative steps now. The following six recommendations will do much to bring the United States in compliance with its Article 58 obligations.

First, the President, through DOD, should identify those civilian systems, networks, and industries that will become legitimate military targets in time of armed conflict because of their nature, location, purpose, or use. The President also needs to identify those that may come under the control of the government but not become military objectives.

President Obama's Cyberspace Policy Review has already recognized that "with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights. The government has a responsibility to address these strategic vulnerabilities."¹⁹³ Under the DIB SSP, DOD is already compiling information on critical infrastructure.¹⁹⁴ Additional analysis comparing military operations and plans against this information should yield a fairly accu-

191. See, e.g., U.S. DEP'T OF DEF., *supra* note 153, at 2 (noting that DOD is "the SSA responsible for collaboration with the DIB security partners, conducting or facilitating DIB vulnerability assessments, and encouraging risk management strategies to protect and mitigate the effects of attacks").

192. Obama, *supra* note 1. President Obama stated,

First, working in partnership with the communities represented here today, we will develop a new comprehensive strategy to secure America's information and communications networks. To ensure a coordinated approach across government, my Cybersecurity Coordinator will work closely with my Chief Technology Officer, Aneesh Chopra, and my Chief Information Officer, Vivek Kundra. To ensure accountability in federal agencies, cybersecurity will be designated as one of my key management priorities. Clear milestones and performance[] metrics will measure progress.

Id.

193. WHITE HOUSE, *supra* note 171, at i.

194. U.S. DEP'T OF DEF., *supra* note 153, at 23, 25.

rate assessment. This assessment will provide the baseline for specific actions required to comply with Article 58.

Second, Congress and the President should expand the current policy and authorities, such as HSPD-7, to include protection not just from terrorists, but from state parties in armed conflicts. Congress should provide the Executive specific authority to protect those privately owned industries, systems, and networks that are anticipated to come under the control of the government during times of armed conflict. Part of this authority should include methods to monitor, implement, and enforce cybersecurity and survivability measures in those specific networks, systems, and industries now.

Such action is not without precedent. Congress has authorized the President to take similar actions with communications systems in times of armed conflict in the past.¹⁹⁵ Current law is insufficient to do so in the current age against the current threats.¹⁹⁶ Former Clinton Deputy Attorney General Jamie S. Gorelick recently urged the Obama Administration to “seek legislation for comprehensive authority to deal with a cyber emergency” including monitoring or cutting off private cell phones and other communications devices.¹⁹⁷ President Obama has shown a reluctance to take steps that invade personal privacy.¹⁹⁸ These situations are not mutually exclusive. Monitoring those systems selected above and taking necessary steps to

195. WHITE HOUSE, *supra* note 171, at C-4 to C-5. According to the Review, Recognizing the pivotal importance of communications to support the execution of government functions during a crisis, Congress, by joint resolution in 1918, authorized the President to assume control of any telegraph, telephone, marine cable or radio system or systems in the U.S. and to operate them as needed for the duration of World War I. Relying on this Congressional authorization, President Wilson issued a proclamation asserting possession, control and supervision over every telegraph and telephone system within the United States. To preserve support for critical government communications needs during times of crisis, Congress later included in Section 706 of the Communications Act of 1934 authority for the President to control private communications systems within the United States during wartime.

Id.

196. *See id.* at 17 (“Current law permits the use of some tools to protect government but not private networks, and vice versa.”).

197. *See* Ellen Nakashima, *War Game Reveals U.S. Lacks Cyber-Crisis Skills*, WASH. POST, Feb. 17, 2010, at A3 (warning that Americans should not expect their “cellphone and other communications to be private—not if the government is going to have to take aggressive action to tamp down the threat”).

198. *See* Obama, *supra* note 1 (stressing the importance of maintaining personal privacy and net neutrality). President Obama remarked,

Let me also be clear about what we will not do. Our pursuit of cybersecurity will not—I repeat, will not include—monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans. Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be—open and free.

Id. But *see* Geoff Fein, *Effort Underway to Put Network Security Language into DFAR*, DEF. DAILY, July 8, 2009, available at 2009 WLNR 14424861 (stating that there is an effort to “define in both the [Defense Federal Acquisition Regulations] and the Federal Acquisition Regulations (FAR) what kind of network infrastructure is needed”).

ensure their protection does not have to include invasions of privacy. Congress can provide authority and the President can implement that authority in a way that will meet our legal obligations; protect the necessary networks, systems, and industries; and preserve our individual rights.

Third, the President, after identifying those industries, networks, and systems that will become targetable and using the additional authority granted by Congress, should establish memoranda of agreement with these private entities to ensure sufficient protection of these industries and networks. This does not mandate government intrusion in civilian networks, industries, or systems. The government can establish the standard, put in place necessary safeguards, and establish effective monitoring systems and then allow these civilian entities to provide their own protection or opt for some combination of government and private security. Whatever method is agreed upon, the government should determine the sufficiency of the protection and then monitor implementation of the protective measures and have the authority to enforce compliance if necessary.

Prior work in the public–private partnership area already has set an effective base for this action. IT and security executives in the United States reflected the highest confidence level (73%) in the ability of their government to deter cyber attacks of any of the surveyed countries.¹⁹⁹ But the current “voluntary” nature of this partnership does not go far enough. Former Assistant Secretary of DHS Stewart Baker believes that “the private sector [is] not prepared to defend against a cyber act of war and that the government need[s] to play a role.”²⁰⁰ Government involvement and regulation has proven to be one of the most effective means to incentivize the private sector to improve security.²⁰¹ In those specific areas where the government anticipates the obligation to protect civilian objects during armed conflict, the government has to be able to take a more proactive role to ensure the proper protections are in place before the attack occurs and the systems are degraded.

Again, President Obama has shown some reluctance to move in this direction. He recognizes the need for public–private partnership but hesitates to dictate specific standards for private companies.²⁰² This hesitation may be

199. See BAKER ET AL., *supra* note 24, at 26 (reporting that only 27% of U.S. IT and security executives think the U.S. government is “not capable or not very capable” of deterring cyber attacks).

200. Nakashima, *supra* note 197.

201. See BAKER ET AL., *supra* note 24, at 39 (“For owners and operators, . . . their relationships to governments are a key factor in how they handle security. For governments, that relationship is crucial for the defense of national assets. In the absence of technological silver bullets, many executives see regulation—despite its drawbacks—as a way of improving security.”).

202. See Obama, *supra* note 1. Indeed, the President has stated,

Third, we will strengthen the public/private partnerships that are critical to this endeavor. The vast majority of our critical information infrastructure in the United States is owned and operated by the private sector. So let me be very clear: My

well-placed generally, but in the face of a legal obligation to protect those limited civilian objects under the control of the government in times of armed conflict, and potential catastrophic consequences for failure, the current paradigm falls short.

Fourth, the government should establish and maintain a “hack back” or other technological solution that protects those systems and networks designated by the President that will come under government control during armed conflict. Many scholars agree that “[a]ctive defenses are the most appropriate type of force to use against cyberattacks in light of the principles of *jus in bello*.”²⁰³ A hack-back-type technology will serve as a “credible military presence in cyberspace to provide a deterrent against potential hackers”²⁰⁴ in an area where deterrents are few. There is evidence that many corporations are already using hack back as a defensive option, including many Fortune 500 corporations.²⁰⁵

Such technological solutions may be limited at present and will need to continue to evolve as attacks evolve. Nearly every panel or review commissioned in the area of cybersecurity has argued that the government needs to invest more heavily in defensive cyber-war capabilities.²⁰⁶ President Obama seems to have embraced the need for increased spending,²⁰⁷ but must also

administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity.

Id.

203. Sklerov, *supra* note 53, at 79; *see also* Jensen, *supra* note 83, at 232–39 (taking the position that in order to combat cyber attacks “the law should permit an active response based on the target of the attack”).

204. COMM’N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, *supra* note 38, at 23.

205. Ruperto P. Majuca & Jay P. Kesan, *Hacking Back: Optimal Use of Self-Defense in Cyberspace* 5–6 (Ill. Pub. Law & Legal Theory Papers Series, Research Paper No. 08-20, 2009), available at <http://papers.ssrn.com/abstract=1363932> (“[A] survey of 320 Fortune 500 corporations revealed that around 30% of the companies have installed software capable of launching counterattack measures.”). *But see* ROSENZWEIG, *supra* note 21, at 18 (speculating that a hack back response would probably violate domestic law).

206. *See, e.g.*, U.S. GOV’T ACCOUNTABILITY OFFICE, *supra* note 165, at 11 (“[E]xperts stated that the U.S. is not adequately focusing and funding research and development efforts to address cybersecurity or to develop the next generation of cyberspace to include effective security capabilities.”); WHITE HOUSE, *supra* note 159, at 34 (“Federal investment in research for the next generation of technologies to maintain and secure cyberspace must keep pace with an increasing number of vulnerabilities.”); COMM’N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, *supra* note 38, at 74 (lamenting as inadequate the government’s 2009 allocation of \$300 million toward research and development in cybersecurity); MARTIN C. LIBICKI, RAND CORP., CYBERDETERRENCE AND CYBERWAR 159 (2009), http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf (arguing that the DOD will need to spend far more on cybersecurity defense than offense).

207. *See* Obama, *supra* note 1. With respect to investing in cybersecurity, the President has stated,

Fourth, we will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time. And that’s why my administration is making major investments in our information infrastructure: laying broadband lines to every corner of America; building a smart electric grid to deliver energy more efficiently; pursuing a next generation of

make a commitment to the hack back technology as a deterrent and first line of protection for specifically designated networks and systems.²⁰⁸

Fifth, the government should create a strategic reserve of Internet capability, including bandwidth, routers, and other necessary means. This would be much like the strategic petroleum reserve whose purpose is to “provide[] the President with a powerful response option should a disruption in commercial oil supplies threaten the U.S. economy.”²⁰⁹ A “strategic cyber reserve” would ensure that critical cyber networks and systems have a place to go when they are being attacked.

In the armed conflict between Russia and Georgia, after the Georgian government sites were shut down by attackers, the Georgian government was able to reestablish itself on servers hosted outside its own borders.²¹⁰ Obviously, the scale of the cyber reserve would need to be sufficient to preserve vital U.S. interests and protect those civilian systems and networks that fall under Article 58.

Finally, the government should push the international community for greater recognition of each state’s requirement under international law to not allow its territory to be used for acts harmful to another state.²¹¹ This “no harm” principle places the responsibility to stop attacks on the country from which they originate or through which they are passed. In several recent attacks, countries from which the attacks have originated refused to accept responsibility and even refused to cooperate with investigations.²¹² That is unacceptable.²¹³

The Cyberspace Policy Review argued that “[i]nternational norms are critical to establishing a secure and thriving digital infrastructure. The United States needs to develop a strategy designed to shape the international

air traffic control systems; and moving to electronic health records, with privacy protections, to reduce costs and save lives.

Id.

208. Mike McConnell, *To Win the Cyber War, Look to the Cold War*, WASH. POST, Feb. 28, 2010, at B1; *see also* Neville-Jones, *supra* note 47 (arguing, in a statement for the United Kingdom Conservative Party, that passive defenses are not sufficient to adequately protect against cyber attack).

209. U.S. Department of Energy, U.S. Petroleum Reserves, <http://www.fossil.energy.gov/programs/reserves/> (last updated Apr. 11, 2010).

210. Gorman, *supra* note 51.

211. *See* Sklerov, *supra* note 53, at 12–13 (arguing that requiring a host state to “hunt down [cyber] attackers within its borders” would allow victim states to “impute state responsibility to host-states that neglected this duty, and respond in self-defense”). *But see* ROSENZWEIG, *supra* note 21, at 14–15 (suggesting that there are many potential problems with blaming states for the actions of cyber attackers, including determining whether the state had sufficient control over the cyber attackers and dealing with cyber attacks that originate from multiple states).

212. Sklerov, *supra* note 53, at 6–10.

213. *See* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1053–57 (2007) (advocating the need for international law to govern activities such as cyber attacks).

environment and bring like-minded nations together on a host of issues, including acceptable norms regarding territorial jurisdiction, sovereign responsibility, and use of force.²¹⁴ The acceptance of the no harm principle is one such norm that should be embraced and specifically applied to cyber operations.

The value of this final suggestion in relation to Article 58 may seem tenuous because Article 58 obligations are only triggered in armed conflict. However, it is clear from recent events that armed conflicts need not come only from nation-states. In fact, terrorist organizations and other non-state actors can create an armed conflict.²¹⁵ Attacks from non-state actors are going to be conducted through the territory of a nation-state. A recognized requirement or international agreement for neutral states to interrupt harmful cyber activities from within their borders will indirectly provide protections for those civilian objects covered by Article 58.

Embracing these six recommendations will cause the government to adapt its current approach to cybersecurity. It will generate some resistance from the private sector. But it will also bring the United States into compliance with its law-of-armed-conflict obligation to protect civilians and civilian objects from the effects of cyber attacks.

VII. Conclusion

In the face of an armed conflict, including a cyber attack, the government cannot allow the collapse of civilian communications infrastructure to prevent an adequately coordinated and effective response to that armed attack. The government will have to step in to ensure continued connectivity. In doing so, it will inevitably rely on civilian industry and use civilian networks and systems to carry its important communications and to accomplish many vital national-security tasks, making these same industries, networks, and systems targetable by the enemy. It will also endanger civilian systems, networks, and industries that are not legitimate military objectives but may be collateral damage from an enemy's attack of military objectives. Article 58(c) requires the government to protect those civilian networks and systems that come under its control to the maximum extent possible.²¹⁶

214. WHITE HOUSE, *supra* note 171, at 20. *But see* ROSENZWEIG, *supra* note 21, at 6 (“[T]he single greatest difficulty encountered thus far in the development of a legal response [to threats in cyberspace] lies in the transnational nature of cyberspace and the need to secure international agreement for broadly applicable laws controlling offenses in cyberspace.”).

215. In response to the attacks on the United States on September 11, 2001, the United Nations Security Council passed Resolution 1368, which recognizes the inherent right of self-defense that was triggered by the terrorist attacks. S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001); *see also* S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001); NATO, NATO and the Fight Against Terrorism, http://www.nato.int/cps/en/natolive/topics_48801.htm (last updated May 4, 2010) (discussing NATO's invocation of the collective-defense provision of the Washington Treaty, which can only be done in response to an armed attack).

216. *See supra* Part IV.

Article 58 of the API places an affirmative obligation on those facing attack to either segregate or protect civilians and civilian objects to the maximum extent feasible in order to spare them from the effects of attacks.²¹⁷ The application of Article 58 to cyber warfare was clearly not contemplated by the drafters who thought of this provision in territorial or geographic terms. However, in modern society, cyberspace has become not only an integral and necessary part of daily life but also a popular vehicle of both personal and military attack.

In applying Article 58 to cyber warfare, the near-complete interconnectedness of government and civilian cyber systems makes segregation under Article 58(a) and (b) impractical. Therefore, states must embrace the requirement under Article 58(c) to protect civilians and civilian objects under their control from the effects of attacks.

The United States has already taken steps to integrate the public- and private-sector defense strategies, particularly in the area of critical infrastructure. However, much more can and needs to be done. By following the six recommendations contained in Part VI, the government will not only bring itself into compliance with Article 58's obligations, but it will also be creating a safer and more resilient cyber world in the face of terrorist and other threats.

217. *See supra* notes 85–108 and accompanying text.