Brigham Young University Law School
BYU Law Digital Commons

Faculty Scholarship

12-31-2012

Cyber Deterrence

Eric Talbot Jensen
BYU Law, jensene@law.byu.edu

Follow this and additional works at: https://digitalcommons.law.byu.edu/faculty_scholarship

 Part of the Internet Law Commons, and the National Security Law Commons

Recommended Citation
Eric Talbot Jensen, *Cyber Deterrence*, 26 Emory Int'l L. Rev. 773, 773 (2012).
Available at: https://digitalcommons.law.byu.edu/faculty_scholarship/231

This Article is brought to you for free and open access by BYU Law Digital Commons. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of BYU Law Digital Commons. For more information, please contact hunterlawlibrary@byu.edu.

CYBER DETERRENCE

Eric Talbot Jensen[*]

ABSTRACT

Cyber operations by both state actors and non-state actors are increasing in frequency and severity. As nations struggle to defend their networks and infrastructure, their ability to apply the principles of deterrence to cyber activities correspondingly increases in importance.

Cyber deterrence offers much more flexibility and increased options from traditional deterrence methodologies developed in the Cold War's nuclear age. In addition to traditional retaliation, cyber deterrence includes options such as taking legal action and making networks invisible, resilient, and interdependent. It also presents new ways to view and apply accepted methodologies such as invulnerability.

As the United States continues to develop and implement cyber deterrence strategies and capabilities, there are important legal issues that require consideration, including international law, the law of armed conflict, and U.S. domestic law. This Article will identify and discuss six prominent theories of cyber deterrence and briefly analyze legal issues associated with this vital area of national security. The law not only provides important factors that must be considered as cyber deterrence doctrine is solidified, but it also provides significant insights into how these theories of cyber deterrence can best be utilized to support national strategic goals.

---

[*] Associate Professor, Brigham Young University Law School. The author wishes to thank Ryan Fisher and Brigham Udall for their exceptional research and editing assistance.

Deterrence is the art of producing in the mind of the enemy the fear to attack.

Dr. Strangelove[1]

INTRODUCTION

In July 2011, then-Deputy Secretary of Defense William J. Lynn III announced that a few months earlier, more than 24,000 Department of Defense (the "DoD") computer files had been stolen by hackers who had gained access to the DoD's computer systems.[2] A few months prior to that announcement, one of the U.S. Government's key scientific labs was hacked and large amounts of information were taken.[3] In neither case has the U.S. Government made any statement about the hackers' identity. However, in both cases, there was speculation that the origin of the attack was a foreign nation.[4]

These are just two examples in a long line of continuous and pervasive cyber "attacks"[5] on U.S. Government computer systems.[6] In any 24-hour period, roughly seven million DoD-owned computers access the Internet[7] and

---

[1] DR. STRANGELOVE OR: HOW I LEARNED TO STOP WORRYING AND LOVE THE BOMB (Hawk Films 1964) [hereinafter DR. STRANGELOVE].

[2] Karen Parrish, *Lynn: Cyber Strategy's Thrust is Defensive*, AM. FORCES PRESS SERV. (July 14, 2011), http://www.defense.gov/news/newsarticle.aspx?id=64682.

[3] Kim Zetter, *Top Federal Lab Hacked in Spear-Phishing Attack*, WIRED (Apr. 20, 2011 1:16 AM), http://www.wired.com/threatlevel/2011/04/oak-ridge-lab-hack.

[4] The 2011 Department of Defense Strategy for Operating in Cyberspace acknowledges that "many foreign nations are working to exploit DoD unclassified and classified networks, and some foreign intelligence organizations have already acquired the capacity to disrupt elements of DoD's information infrastructure." DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 1 (2011). The GAO reports that "[i]n February 2011, the Deputy Secretary of Defense said that more than 100 foreign intelligence agencies have tried to breach DOD computer networks and that one was successful in breaching networks containing classified information." U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-421, DEFENSE DEPARTMENT CYBER EFFORTS 1 (2011).

[5] Use of the word "attack" to describe a vast array of computer operations is extremely imprecise. It is used here only to parallel common usage. In legal terms, "attack" has significant meaning under international law. *See* Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 1 NAT'L SECURITY L. BRIEF 33, 34 (2011); Kim Taipale, *Cyber Deterrence*, *in* LAW, POLICY AND TECHNOLOGY: CYBERTERRORISM, INFORMATION WARFARE, DIGITAL AND INTERNET IMMOBILIZATION (Pauline C. Reich & Eduardo Gelbstein eds., 2012). The use of the word attack is also a matter of definitional debate for the argument of how to respond to cyber activities. *See* Oona Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 822–37 (2012) (proposing a definition of cyber attack).

[6] Duncan B. Hollis, *An e-SOS for Cyberspace,* 52 HARV. INT'L L.J. 373, 374–75 (2011).

[7] 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).

"Homeland Security counted 37,258 attacks on government and private networks [in 2008], compared with 4,095 in 2005."[8] A recent Center for Strategic and International Studies report stated:

> [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 email 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 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.[9]

The government is certainly not alone as a target for malicious computer operations. Private businesses are also being hacked at an alarming rate. In a recent incident targeting "proprietary corporate data, e-mails, credit-card transaction data and login credentials at companies in the health and technology industries," more than 75,000 computers at more than 2,500 businesses in 196 countries were targeted.[10] The presumed targets in these attacks were intellectual property and proprietary information that could be translated into economic gain for the attackers.[11] According to Ty Sagalow, chairman of the Internet Security Alliance board of directors, "[a]n estimated $1 trillion was lost in the United States in 2008 through cyber attacks."[12] This

---

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

[9] COMM'N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 12–13 (2008).

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

[11] *See id.*

[12] William Matthews, *Cyber War's 'Front Lines' May Be in Private Hands*, DEF. NEWS, Dec. 7, 2009, at 38, *available at* 2009 WLNR 25655553; *see* DEP'T OF DEF., *supra* note 4, at 4 (stating that "[e]very year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and governmental departments and agencies."). The United States is not alone in this area. According to recent reports, China is suffering from severe criminal activity that is causing serious domestic problems. "The annual worth of China's 'hacker industry' is now over 238 million yuan (about $34.8 million), causing upwards of 7.6 billion yuan (about $1.1 billion) in losses . . . . The number of computers in China controlled by 'botnets' tops the list worldwide." Tang Lan & Zhang Xin, *The View from China: Can Cyber Deterrence Work?*, *in* GLOBAL CYBER DETERRENCE: VIEWS FROM CHINA, THE U.S., RUSSIA, INDIA, AND NORWAY 1, 2 (Andrew Nagorski ed. 2010) [hereinafter GLOBAL CYBER DETERRENCE]. *But*

is more than the annual Gross Domestic Product of all but the top nineteen countries in the world.[13]

Among the most worrisome of hacking incidents are those focused on critical national infrastructure.[14] This infrastructure is the backbone of United States' transportation and economic systems.[15] The cost of downtime alone from major attacks on critical national infrastructure "exceeds . . . $6 million per day."[16] The attacks have caused President Barack Obama to recently state,

> 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.[17]

President Obama's recognition of the role and importance of deterring malicious cyber operations, including cyber attacks, incorporates the traditional notions of deterrence to this modern risk to national security.

---

see Robert Vamosi, *The Myth of that $1 Trillion Cybercrime Figure*, SECURITYWEEK (Aug. 3, 2012), http://www.securityweek.com/myth-1-trillion-cybercrime-figure.

[13] CIA, *Country Comparison: GDP (Purchasing Power Parity)*, CIA WORLD FACTBOOK, https://www.cia.gov/library/publications/the-world-factbook/rankorder/2001rank.html (based on 2011 estimates) (last visited Nov. 16, 2012).

[14] As defined in the Critical Infrastructures Protection Act of 2001, critical national infrastructure "means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e) (2006); *see also* DEP'T OF DEF., DEPARTMENT OF DEFENSE DIRECTIVE NO. 3020.40, DOD POLICY AND RESPONSIBILITIES FOR CRITICAL INFRASTRUCTURE 19, 20 (2010); EXEC. OFFICE OF THE PRESIDENT, PRESIDENTIAL DECISION DIRECTIVE 63, CRITICAL INFRASTRUCTURE PROTECTION (1998).

[15] 42 U.S.C. § 5195c(b).

[16] STEWART BAKER ET AL., IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 3 (2010).

[17] Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure. This sentiment was echoed by U.S. Cyber Command's General Alexander, "[t]his increased inter-connectedness of our information systems, combined with the growing sophistication of cyber criminals and foreign intelligence actors, has increased our risk. Our inter-connectedness is now a national security issue." *Budget Request for Information Technology and Cyber Operations Programs: Hearing on the National Defense Authorization Act for Fiscal Year 2013 and Oversight of Previously Authorized Programs, Before the Subcomm. on Emerging Threats and Capabilities of the H. Comm on Armed Services*, 112th Cong. 6 (March 20, 2012) [hereinafter *Budget Request for Information Technology and Cyber Operations Programs*] (statement of General Keith B. Alexander, Commander, United States Cyber Command).

Deterrence has been a part of Western political security doctrine since ancient Greece[18] and played a particularly key role in the post-World War II nuclear world.[19] It is equally important in today's world of cyber operations[20] and will continue to play a key role in the U.S. national security strategy.[21] In fact, just as cyber operations offer unique capabilities as tools to accomplish national goals,[22] they also present distinctive aspects of deterrence, both in line with traditional notions of deterrence and also some innovative and progressive ways of viewing deterrence.[23]

As the United States continues to develop and implement cyber deterrence strategies and capabilities,[24] there are important legal issues that require consideration, including international law, the law of armed conflict ("LOAC"), and U.S. domestic law. This Article will identify and discuss six prominent theories of cyber deterrence and analyze legal issues associated with this vital area of national security. The law not only provides important factors

---

[18] *See* ALEXANDER L. GEORGE & RICHARD SMOKE, DETERRENCE IN AMERICAN FOREIGN POLICY: THEORY AND PRACTICE 12 (1974).

[19] GREVILLE RUMBLE, THE POLITICS OF NUCLEAR DEFENSE 42, 71 (1985) (explaining mutually assured destruction in nuclear deterrence).

[20] M. Elaine Bunn, *Can Deterrence Be Tailored?*, STRATEGIC FORUM, Jan. 2007, at 1, 5; Elaine Grossman, *Top General: US Needs Fresh Look at Deterrence, Nuclear Triad*, NATIONALJOURNAL (July 15, 2011), http://www.nationaljournal.com/nationalsecurity/top-general-u-s-needs-fresh-look-at-deterrence-nuclear-triad-20110715.

[21] DEP'T OF DEF., *supra* note 14, at 2, 5 (outlining DoD policy and responsibilities for critical infrastructure).

[22] *See Budget Request for Information Technology and Cyber Operations Programs*, *supra* note 17, at 7 (statement of General Keith B. Alexander, Commander, United States Cyber Command) (stating that "our cyber capabilities represent key components of deterrence."); MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 125–26 (2009) (discussing the potential use of cyber attacks in offensive military operations).

[23] LIBICKI, *supra* note 22, at xvi–xix.

[24] As cyber capabilities have been developed and increased, the United States military has gone through an evolution of how to utilize and control these capabilities. Initially, cyber activities were placed under the U.S. military's Strategic Command, or STRATCOM. STRATCOM is the unified command tasked with maintenance and readiness of the United States' nuclear arsenal and was created in response to the Cold War with the Soviet Union. STRATCOM's mission is to "[d]etect, deter, and prevent attacks against the United States and our allies - join with the other combatant commands to defend the nation should deterrence fail." U.S. STRATEGIC COMMAND (USSTRATCOM), FACT SHEET (Dec. 2011), http://www.stratcom.mil/factsheets/snapshot. As cyber operations grew as a threat to U.S. national security, STRATCOM was also given the task to "[b]uild cyberspace capability and capacity." U.S STRATEGIC COMMAND, MISSION (Apr. 2011), http://www.stratcom.mil/mission. In 2009, U.S. Cyber Command, or CYBERCOM, was created and its mission as of December 2011 follows: "USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries." U.S. CYBER COMMAND, FACT SHEET (Dec. 2011), http://www.stratcom.mil/factsheets/Cyber_Command.

that must be considered as cyber deterrence doctrine is solidified, but also provides significant insights into how these theories of cyber deterrence can best be utilized to support national strategic goals.

Part I of this Article will examine some basic principles of deterrence that affect the application of the law, such as the difficulties of attribution and signaling. Part II will then outline six prominent theories of cyber deterrence and briefly describe some legal issues associated with them, including an analysis of how the law is an important consideration in applying these theories in modern U.S. national security strategy. The Article will conclude in Part III.

I. DETERRENCE AND CYBER OPERATIONS

> *The goal of deterrence is to prevent aggressive action . . . by ensuring that, in the mind of a potential adversary, the risks of the action outweigh the benefits, while taking into account the consequences of inaction.*[25]

As mentioned in the Introduction, deterrence theory is not a new phenomenon[26] and has played a significant role in national security theory.[27] With the modern development of cyber operations, the U.S. Government, as well as academics and practitioners, have turned their attention to cyber deterrence.[28] The nature of cyber operations has caused some to diminish the potential role for deterrence. Tang Lan and Zhang Xin have written "the anonymity, the global reach, the scattered nature, and the interconnectedness of information networks greatly reduce the efficacy of cyber deterrence and can even render it completely useless."[29] Despite this competing view, cyber

---

[25] Bunn, *supra* note 20, at 1.

[26] *See generally* RUMBLE, *supra* note 19, at 42–73 (outlining the history of deterrence theory in practice in Western history).

[27] *See* GEORGE & SMOKE, *supra* note 18, at 12–21; AUSTIN LONG, DETERRENCE: FROM COLD WAR TO LONG WAR 2–4 (2008); Christopher Achen & Duncan Snidal, *Rational Deterrence Theory and Comparative Case Studies*, 41 WORLD POLITICS 143, 143 (1989); Robert Powell, *Nuclear Deterrence Theory, Nuclear Proliferation, and National Missile Defense*, 27 INT'L SECURITY 86, 88 (2003). U.S. Strategic Command, the command under which CYBERCOM works, has an annual deterrence symposium that discusses deterrence issues, though it often focuses on nuclear deterrence. *See 2012 U.S Strategic Command Deterrence Symposium*, U.S. STRATEGIC COMMAND, http://www.stratcomds.com (last visited Sept. 22, 2012).

[28] CHARLES L. GLASER, DETERRENCE OF CYBER ATTACKS AND U.S. NATIONAL SECURITY 2 (2011); LIBICKI, *supra* note 22, at 5; Kenneth Geers, *The Challenge of Cyber Attack Deterrence*, 26 COMPUTER L. & SECURITY REV. 298, 298 (2010); Will Goodman, *Cyber Deterrence: Tougher in Theory Than in Practice?*, STRATEGIC STUD. Q., Fall 2010, at 102, 102.

[29] Tang & Zhang, *supra* note 12, at 1.

deterrence continues to increase in importance[30] as nations struggle with the vulnerability of both government and private sector cyber systems.

Before discussing the prominent cyber deterrence theories and the attending legal issues, some comment on the unique aspects of cyber deterrence will be useful.

A. Assumptions

In approaching this topic, some assumptions are necessary. These assumptions undergird the subsequent legal analysis but are relatively uncontroversial, particularly in the cyber domain.

1. Full Spectrum Deterrence Required

The initial assumption is that cyber deterrence is required across a much greater spectrum than most other weapons and actors, and certainly than was present in the post-World War II discussion of nuclear deterrence.[31]

Cyber operations are inherently different than many other weapons that harness state level violence, in that they are accessible to a broad range of actors including but not limited to states.[32] For example, only states, and very few of those, have ever developed a nuclear capability.[33] On the other hand, more than 140 nations are reported to have or be developing cyber weapons,[34] and more than thirty countries are creating cyber units in their militaries.[35] The recent Stuxnet malware[36] has been labeled by some as the first real example of

---

[30] Goodman, *supra* note 28, at 1.

[31] Richard L. Kugler, *Deterrence of Cyber Attacks*, *in* CYBERPOWER AND NATIONAL SECURITY 309, 310 (Franklin D. Kramer et al., eds., 2009).

[32] Taipale, *supra* note 5, at 8. Taipale divides potential attackers into three categories: 1) those who may be deterred directly; 2) those who may be deterred indirectly by others; and 3) those who may not be easily deterred at all. *Id.* at 9–10.

[33] *Cf.* Hollis, *supra* note 6, at 407 (explaining that hacking skills are more universally distributed worldwide due to being inexpensive and easy to obtain unlike nuclear weaponization).

[34] Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties*, 13 SMU SCI. & TECH. L. REV. 249, 249 (2010); *see* Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 96 (2009).

[35] William J. Lynn, III, *The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack*, FOREIGN AFF. (Sept. 28, 2011), www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later.

[36] Mark Clayton, *Stuxnet Attack on Iran Nuclear Program Came about A YEAR AGO*, CHRISTIAN SCI. MONITOR, Jan. 3, 2011, at 3; Richard Adhikari, *Stuxnet: Dissecting the Worm*, TECHNEWS WORLD (Aug. 16, 2010), http://www.technewsworld.com/story/70622.html.

a cyber "armed attack" in violation of the UN Charter, if it proves to have been carried out by a nation or its agents.[37]

The computer security giant Symantec believes that a cyber threat such as Stuxnet could be created by as few as five to ten highly trained computer technicians in as little as six months.[38] Many non-state actors with malicious intentions could muster those resources and use them to create significant damage. Additionally, very effective hacking tools are readily available for purchase on the Internet by anyone desiring to conduct cyber crime.[39] For example, two Chinese authors have written that:

> Citibank . . . suffered tens of millions of dollars in losses at the hands of criminals using "Black Energy" malware, which can be purchased online for only $40. And the "Zeus Trojan" and its variants that attacked 74,000 computers across 196 countries are also available online for a mere $700.[40]

In a recent statement before Congress, General Keith Alexander, head of Cyber Command and the National Security Agency, stated "[i]n 2010 we saw cyber capabilities in use that could damage or disrupt digitally controlled systems and networked devices, and in some cases we are not sure whether these capabilities are under the control of a foreign government."[41] The ability for non-state actors and even individuals to harness the power of cyber weapons and use them at their discretion, with significant effects,[42] has a serious impact on deterrence that was not an issue with the nuclear threat.[43] In fact, "Russian experts believe that it is criminals and terrorists who present the greatest threat to the security of transnational cyberspace."[44]

---

[37] *See* Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, JOINT FORCES Q., 4th Quarter 2011, at 70, 71.

[38] Josh Halliday, *STUXNET Worm is the 'Work of a National Government Agency,'* GUARDIAN (Sept. 24, 2010), http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency.

[39] Tang & Zhang, *supra* note 12, at 1.

[40] *Id.*

[41] *Budget Request for Information Technology and Cyber Operations Programs*, *supra* note 17, at 3 (statement of General Keith B. Alexander, Commander, United States Cyber Command).

[42] Siobhan Gorman, *Alert on Hacker Power Play*, WALL ST. J., Feb. 21, 2012, at A3; Alistair Stevenson, *AntiSec: Anonymous Hackers Strike Again in "Turkish Takedown Thursday,"* INT'L BUS. TIMES NEWS (July 7, 2011), http://www.ibtimes.co.uk/articles/175785/20110707/antisec-anonymous-hackers-turkey-hack-operation-anti-security-internet-lulzsec-redhack.htm.

[43] Tang & Zhang, *supra* note 12, at 1.

[44] Dmitry I. Grigoriev, *Russian Priorities and Steps Towards Cybersecurity*, *in* GLOBAL CYBER DETERRENCE, *supra* note 12, at 5.

Additionally, cyber operations allow an adversary to accomplish a broad spectrum of effects. In nuclear deterrence, the effects were usually considered catastrophic, allowing a limited number of responses.[45] In cyber operations, effects can be as small as the penetration of a system to observe what that system does,[46] or the defacing of a web site.[47] The effects can also be as large as destroying almost 1000 centrifuges, as Stuxnet is supposed to have done,[48] or an electronic version of the attack on Pearl Harbor, as some warn about.[49]

This means that cyber deterrence theory must embrace a much larger spectrum of potential adversaries and account for being able to deter a much more diverse type of actor than most other previous modalities. Cyber deterrence must apply to the full spectrum of actors, from individuals to nations, and consider the full spectrum of actions, from small invasions into computer systems to large scale "attacks" that produce significant kinetic effects.

This spectrum of potential attacks and attackers requires deterrence to be considered on at least two planes: general and specific. General deterrence is designed to apply broadly and in advance of any potential attack.[50] For example, having a nuclear arsenal that can be used in response to various attacks of various kinds is a general deterrent.[51] It deters everyone without reference to a specific incident or threat. In the cyber realm, there are certain actions, such as installing a firewall, that apply as a general deterrent to all actors.[52] Specific deterrence, or what is now being termed "tailored

---

[45] Colin S. Gray, *Nuclear Strategy: The Case for a Theory of Victory*, 4 INT'L SECURITY 54, 57 (1979).

[46] Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project*, WALL ST. J., Apr. 21, 2009, at A1–A2.

[47] Kevin Andersen, *White House Website Attacked*, BBC NEWS (May 5, 2001), http://news.bbc.co.uk/2/hi/americas/1313753.stm.

[48] David Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1.

[49] Michiko Kakutani, *The Attack Coming From Bytes, Not Bombs*, N.Y. TIMES, Apr. 27, 2010, at C1 (statement of cyber defense expert Richard Clarke); Leon E. Panetta, U.S. Sec'y of Def., Remarks at Town Hall Meeting (Mar. 2, 2012) (transcript available at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4989) (warning that "the next Pearl Harbor could very well be a cyberattack that takes down our power grid system, that takes down our government systems, that takes down our financial systems.").

[50] Taipale, *supra* note 5, at 14; *see* Paul Huth & Bruce Russett, *General Deterrence Between Enduring Rivals: Three Competing Models*, 87 AM. POL. SCI. REV. 61, 61 (1993).

[51] *See* Huth & Russett, *supra* note 50, at 61–62.

[52] Joseph H. Schuessler, General Deterrence Theory: Assessing Information Systems Security Effectiveness in Large Versus Small Businesses 10–11 (May 2009) (unpublished Ph.D. dissertation, University of North Texas), *available at* http://digital.library.unt.edu/ark:/67531/metadc9829/m2/1/high_res_d/dissertation.pdf.

deterrence,"[53] is effective in deterring a specific type of cyber operation, a specific actor, or both.[54] In the cyber realm, this might include blocking all cyber traffic that comes from a particular server, or that carries a particular type of file. Because a nation must defend its networks against all potential adversaries with all potential capabilities, deterrence must operate on both planes to be truly effective.

The factors above lead to the conclusion that deterrence must cover the full spectrum of actors, types of "attacks," and levels of action. In other words, cyber operations require full spectrum dominance if they are to be most effective.

2. *Ineffectiveness Guaranteed*

Another assumption concerning cyber deterrence that impacts this paper is that regardless of how much effort is put into deterrence, it can never be completely effective.[55] This is true not only from a technical perspective,[56] but also from a sociological perspective. Some options that will deter some potential adversaries will give incentive to others, and there are some actors who simply cannot be deterred.[57]

Cyber deterrence can never be completely effective because actions that are designed to deter one type of actor will only incentivize other actors. For example, one of the deterrent methodologies that will be discussed below, and that was one of the main bases of nuclear deterrence, is retaliation, including kinetic retaliation.[58] This was effective in the nuclear era because it was not difficult to determine who launched the attack. However, in the cyber area, as will be discussed below,[59] not only is it extremely difficult to determine who is

---

[53] Kugler, *supra* note 31, at 325; Taipale, *supra* note 5, at 14; Bunn, *supra* note 20, at 1.

[54] *See* Taipale, *supra* note 5, at 14 ("Tailored deterrence is a more precisely targeted kind of specific deterrence strategy in which policies are tailored to specific actors, situations, capabilities, and communications.").

[55] Kugler, *supra* note 31, at 326.

[56] William J. Lynn III, U.S. Deputy Sec'y of Def., Remarks on the Department of Defense Cyber Strategy at the National Defense (July 14, 2011) (transcript available at http://www.defense.gov/speeches/speech.aspx?speechid=1593) (stating "no network will ever be perfectly secure.").

[57] PAUL K. DAVIS & BRIAN MICHAEL JENKINS, DETERRENCE AND INFLUENCE IN COUNTERTERRORISM: A COMPONENT IN THE WAR ON AL QAEDA 3–5 (2002).

[58] Kinetic weapons are those that are associated with heat, blast, and fragmentation, such as a bomb or a bullet.

[59] *See infra* Part I.B.1.

initiating the cyber incident, but it is also possible to "spoof" your cyber activity and make it appear that the incident was caused by someone else.[60]

These inherent aspects of cyber operations would allow one entity to conduct a significant cyber operation on a target and then make it appear as if the operation were done by a third entity.[61] The target nation, in an attempt to respond and deter, might unleash a devastating cyber or kinetic attack on the "framed" entity, causing undeserved destruction.[62] In this way, cyber and kinetic retaliation may deter some entities from conducting cyber attacks against certain cyber-capable entities but could ironically incentivize others to conduct such operations, if they could mask or spoof their operation to look like someone else.[63]

A final aspect of the assumption of ineffectiveness of cyber deterrence is that some with cyber capabilities can never be deterred. As a matter of social theory[64] and historical precedent,[65] it seems clear that some individuals are so committed to a certain course of violent action that no methods of deterrence can be truly effective.[66] Rogue states, terrorists,[67] and suicide bombers represent a stark example,[68] though some theorists argue that even these categories of attackers can be deterred in some way.[69] If individuals or entities are willing to commit suicide to accomplish their purposes, it must be assumed that a similarly committed individual, who can accomplish the same death or

---

[60] *China, Not India, Behind Cyber Attacks: US*, HINDUSTAN TIMES (India) (Jan. 21, 2012), http://www.hindustantimes.com/world-news/Europe/China-not-India-behind-cyber-attack-US/Article1-800051.aspx (reporting an attack that was initially claimed to be from India, but actually was likely arranged by China).

[61] *Id.*

[62] *See* Christopher Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 859 (2001).

[63] *See* Charles Arthur, *China 'Targeted 48 Chemical and Military Companies in Hacking Attack,'* GUARDIAN (Nov. 1, 2011), http://www.guardian.co.uk/technology/2011/nov/01/china-hacking-chemical-military-companies (reporting attacks that came from a Chinese national that was hacking from within the United States); *Alert SA07-303A): Federal Trade Commission Reports Spoofed Email* (Oct. 30, 2007), http://www.us-cert.gov/cas/alerts/SA07-303A.html.

[64] DAVIS & JENKINS, *supra* note 57, at 3–5.

[65] Bruce Hoffman, *The Logic of Suicide Terrorism*, ATLANTIC (June 2003), http://www.theatlantic.com/magazine/archive/2003/06/the-logic-of-suicide-terrorism/2739.

[66] DAVIS & JENKINS, *supra* note 57, at 3–7; Hoffman, *supra* note 65.

[67] Lynn, *supra* note 56 (Deputy Secretary of Defense William J. Lynn, III, remarking that terrorists and rogue states are more difficult to deter).

[68] *Twin Suicide Bombers Kill 27 in Syrian Capital*, CBS NEWS (Mar. 17, 2012), http://www.cbsnews.com/8301-202_162-57399452/twin-suicide-bombers-kill-27-in-syrian-capital.

[69] Kugler, *supra* note 31, at 338; Bunn, *supra* note 20, at 3.

destruction by means of cyber operations with no immediate personal risk, is similarly not deterrable.

B. Overarching Issues

In addition to assumptions, there are several overarching issues that, while vital to truly understanding the legal issues surrounding cyber deterrence, cannot be fully explored in this Article. However, a brief mention of them will be helpful here.

1. Attribution

One of the most vexing problems associated with cyber operations is the issue of attribution. This problem has been highlighted in numerous reports and writings.[70] It revolves around the ability of a victim to identify the "attacker." As one commentator has written, "[o]ur continuing inability to attribute attacks is tantamount to an open invitation to those who would like to do us harm, whatever their motives."[71]

Because of the nature of the Internet, combined with the sophistication of many attackers, many of the most significant cyber incidents are still unattributed.[72] Ultimately, even determining the computer that generated the cyber operation does not answer the attribution question unless there is some way of knowing for certain who was using the computer.[73] An attack that can be traced to a Chinese government computer in the basement of a Chinese government building does not ensure that a Chinese government agent was operating on behalf of the Chinese government.[74] Rather, it may be a rogue

---

[70] *See, e.g.*, LIBICKI, *supra* note 22, at 43–51; Hollis, *supra* note 6, at 397–404; Todd C. Huntley, *Controlling the Use of Force in Cyber Space*, 60 NAVAL L. REV. 1, 34–35 (2010). Jonathan Soloman, *Cyberdeterrence Between Nation-States Plausible Strategy or a Pipe Dream?*, 5 STRATEGIC STUD. Q. 1, 5–10 (2011).

[71] Harry D. Raduege, Jr., *The View from the United States: Fighting Weapons of Mass Disruption: Why America Needs a "Cyber Triad," in* GLOBAL CYBER DETERRENCE, *supra* note 12, at 3, 4.

[72] *See* Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian–Georgian Cyber Conflict*, 32 LOY. L.A. INT'L & COMP. L. REV. 303, 319 (2010); *cf.* Hollis, *supra* note 6, at 378 ("In reality . . . anonymity, not attribution, prevails. Current information technology makes it difficult to identify the actual server from which an attack (or exploit) originates, let alone its perpetrators.").

[73] *See* Hollis, *supra* note 6, at 378; Arthur, *supra* note 63; Adam Segal, *A Chinese View on Why Cyber Deterrence Is So Hard*, COUNCIL ON FOREIGN REL. (Jan. 11, 2012), http://blogs.cfr.org/asia/2012/01/11/a-chinese-view-on-why-cyber-deterrence-is-so-hard/.

[74] *See* Grigoriev, *supra* note 44, at 6 (stating that "it is often very difficult to reliably determine precisely what country such [military cyber attacks] were carried out from. And even if the country is identified, it is

Chinese actor or even an agent of a third country trying to make it appear as if the Chinese generated the attack.[75]

The inability to promptly attribute cyber operations provides significant legal hurdles to effective deterrence. Until the victim knows who is assaulting his computer systems, it is difficult to know how to deter them. It is always possible for the victim to unplug the attacked system from the Internet,[76] but if that is a target's only response, deterrence is not playing an effective role.

Given the difficulties just discussed, two other important factors must be considered concerning deterrence. First, despite the fact that many attacks remain unattributed,[77] with sufficient time and resources, many attacks can be attributed with some degree of certainty.[78] In fact, many now argue that the real issue is not attribution, but "prompt" attribution.[79] Computer forensics will often allow eventual attribution,[80] but by the time of discovery, the window to reasonably respond will be gone.

Second, attribution should probably not be characterized as an "either/or" situation, where one either can correctly attribute or not. In actuality, attribution is more like a spectrum where over time a victim becomes more and more sure of who committed the attack.[81] The political decision for the victim nation then becomes how much attribution is required to take a contemplated action.[82] In other words, does the victim nation feel like it has enough

---

very difficult to prove that attack was carried out specifically by its armed forces."); *N. Korea's Cyber Warfare Unit in Spotlight After Attack on S. Korean Bank*, YONHAP NEWS AGENCY (May 3, 2011), http://english.yonhapnews.co.kr/national/2011/05/03/78/0301000000AEN20110503010600315F.HTML (finding that an attack originally attributed to hackers in China was in fact committed by North Korean hackers); *see also* Segal, *supra* note 73.

75 Taipale, *supra* note 5, at 23–24.

76 Zetter, *supra* note 3.

77 *See* Hollis, *supra* note 6, at 378; Swanson, *supra* note 72, at 319.

78 *See, e.g.*, *N. Korea's Cyber Warfare Unit in Spotlight After Attack on S. Korean Bank*, *supra* note 74; *cf.* Hollis, *supra* note 6, at 377 (explaining that proponents of regulating cybercrime and cyber war assume that sufficient attribution of the origins of attacks will occur).

79 *E.g.*, Herbert Lin, Chief Scientist, Computer Science and Telecommunications Board, National Research Council of the National Academies, Remarks at International Conference on Challenges in Cybersecurity: Risks, Strategies, and Confidence Building (Dec. 13, 2011).

80 *See* Soloman, *supra* note 70, at 6.

81 *See id.* at 6–8.

82 *See id.* at 10; Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, HOOVER INSTITUTION, 1, 10 (2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf (explaining that the Information Warfare Monitor chose not to act even though it traced the source of a computer hack to China because it was not fully clear whether a private actor or a government official was responsible for the attack); Lin, *supra* note 79.

attribution to take a specific action? Presumably, less sure attribution would be sufficient for less serious responses. A forceful response would likely require more certain attribution.

It may be that some technological innovation will occur or some structural change will be made to the infrastructure supporting the Internet to make prompt and accurate attribution less difficult, but until then, attribution will continue to be a vexing issue for victims that significantly compromises attempts at deterrence.

2. *Signaling*

In one of the classic quotes from the movie Dr. Strangelove, which deals with an inadvertent onset of nuclear war,[83] the Russian ambassador describes Russia's *secret* "Doomsday Machine" which was meant to act as a deterrent to the U.S. nuclear threat.[84] In response, Dr. Strangelove says "of course, the whole point of a Doomsday Machine is lost, if you keep it a secret!"[85] Though dealing with nuclear war, this quote highlights a significant issue in all forms of deterrence, including cyber deterrence—signaling.

Throughout the history of deterrence, the ability to signal one's adversaries was a fundamental principle, both in times of conflict and in times of peace.[86] Floating an aircraft carrier through the straits of Taiwan[87] or holding a parade where a nation displays all of its weaponry[88] were methods of signaling to an adversary both capability and intention.[89] The ability to clearly signal one's capabilities and intentions added clarity to adversarial interactions and allowed

---

[83] *See* Tim Dirks, *Filmsite Movie Review: Dr. Strangelove, Or: How I Learned to Stop Worrying and Love the Bomb (1964)*, FILMSITE, http://www.filmsite.org/drst.html (last visited Oct. 3, 2012).

[84] DR. STRANGELOVE, *supra* note 1.

[85] *Id.*

[86] *See* Bunn, *supra* note 20, at 6 ("Whether through words or actions, shaping decisions of opponents does not begin with the crisis; their perceptions may already be well entrenched by then, and it may be difficult to communicate new messages to leaders in protective bunkers. Communications in peacetime are probably more important than words said or actions taken in times of tension.").

[87] Patrick E. Tyler, *China Warns U.S. To Keep Away From Taiwan Strait*, N.Y. TIMES, Mar. 18, 1996, at A3.

[88] Tania Branigan & Jonathan Watts, *China Shows Off Military Might at 60th Anniversary Parade*, GUARDIAN (Oct. 1, 2009), http://www.guardian.co.uk/world/2009/oct/01/china-military-60th-anniversary-parade.

[89] *Cf.* Bunn, *supra* note 20, at 5 (discussing the need to demonstrate clearly both the capability and the will to carry out an attack).

greater impact of deterrent options.[90] Signaling in cyber operations is equally important[91] but more difficult for a number of reasons.[92]

First, because attribution is so fundamentally difficult and cloaking an adversary's operations is so beneficial in terms of avoiding a response, openly announcing cyber capabilities is seldom seen as beneficial.[93] Because anonymity on the Internet is so likely even after a cyber operation, the incentives to signal capabilities or intentions are diminished.[94] With most weapons, the use of the weapons divulges what state is using them; however, states can develop and use their cyber capabilities without the use being attributed to the state, thereby diminishing the benefits of signaling.[95]

Second, unlike many kinetic weapons, most cyber weapons are "single use" weapons. In other words, using a cyber tool, or even displaying it, may make it ineffective.[96] For example, Stuxnet took advantage of several "zero-day exploits."[97] These exploits were unknown defects in a software controller program that allowed the Stuxnet to do the things it did.[98] Once the defects were used, they became known and "patches"[99] were issued which prevented those same exploits from being issued again.[100] In this way, signaling a cyber weapon often makes it ineffective, which is seldom the case with standard kinetic weapons.

Third, signaling a target is equally unhelpful. Though the offense can usually outstrip the defense in cyber operations,[101] putting an adversary on notice as to which networks or computer systems are the target of penetration or have already been penetrated undermines the attack. It allows the adversary

---

[90] Kugler, *supra* note 31, at 322.

[91] LIBICKI, *supra* note 22, at 106.

[92] *See* Taipale, *supra* note 5 at 16–18 (discussing cyber signaling and its inherent differences and difficulties).

[93] *Id.* at 27.

[94] *Id.* at 22–23.

[95] *Id.*

[96] *See, e.g.*, Liam Murchu, *Stuxnet Using Three Additional Zero-Day Vulnerabilities*, SYMANTEC OFFICIAL BLOG (Sept. 14, 2010), http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities.

[97] *Id.*

[98] *Id.*

[99] U.S. Computer Emergency Readiness Team, *Security Tip (ST04-006): Understanding Patches*, US-CERT, http://www.us-cert.gov/cas/tips/ST04-006.html (last updated July 14, 2009) (defining the term "patches").

[100] Murchu, *supra* note 96.

[101] Taipale, *supra* note 5, at 26.

to safeguard information, evict the attacker from the system, or prepare some other means of foiling the compromise of the target system or network.[102] Though there is some similarity here in non-cyber operations, the speed with which an adversary can move an intended target to a different platform, such as a different server, is generally much faster in the cyber world.

Together, these three factors make signaling less effective as a means of creating clarity in the relationship and interactions of potential cyber adversaries. While signaling can still play a role,[103] it appears to be diminished in comparison with more traditional means of deterrence.

3. Time and Scale

Time and scale of potential malicious cyber operations are also significant overarching issues that affect cyber deterrence. It is often said that the most dangerous cyber attack is the one that has not yet been discovered.[104] The fact that an adversary has infiltrated a network is alarming enough; finding out that he has been there for several years without anyone knowing is much more problematic. And in cyber operations, an adversary can exfiltrate as much data in minutes as it would take a human spy to sneak out in years. The sheer speed at which cyber operations can occur make them fundamentally different than traditional operations.[105]

One of the unique aspects of the Internet is that it is generally easier to act offensively than to defend. This is especially true in the milliseconds of time in which cyber operations occur. Just as it is much easier to build a cannonball and find the single point of weakness in the fortifications than it is to build impregnable walls that surround the entire city,[106] it is axiomatic that it is easier to find an individual weakness in a network or system than it is to

---

[102] *See generally id.* at 21–28.

[103] Kugler, *supra* note 31, at 332.

[104] Bill Gertz, *China Blocks U.S. from Cyber Warfare*, WASH. TIMES (May 12, 2009), http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/ (quoting Joel Brenner, the head of U.S. counterintelligence, saying "I worry more about attacks we can't even see.").

[105] Gary Brown, Colonel, Staff Judge Advocate U.S. Cyber Command, Keynote Address at The Internet *in Bello*: Cyber War, Ethics, & Policy (Nov. 18, 2011) (summary available at http://www.law.berkeley.edu/12032.htm).

[106] Helen Starkweather, *Endangered Site: Famagusta Walled City, Cyprus*, SMITHSONIAN MAG. (March 2009), http://www.smithsonianmag.com/travel/Endangered-Cultural-Treasures-Famagusta-Walled-City-Cyprus.html (discussing the use of cannonballs to penetrate city walls).

defend the entire network or system.[107] This fact creates a sense of near hopelessness in some, particularly in the business world, who decide it would cost more to secure their networks than they would gain from the security.[108] In a purely economic model, it is unsurprising that some would choose the path of least expense.[109]

Like time, the scale of a malicious cyber operation must be conceived of differently than typical kinetic operations. In the milliseconds it takes to conduct an attack, the scale of the damage can be immense. There is a spectrum across which cyber operations may be categorized, with the "pinprick attack"[110] on one end and Richard Clarke's "electronic Pearl Harbor"[111] on the other. Great debate rages about the likelihood and effectiveness of either scenario.[112] However, from a deterrence perspective, the resolution matters little in the short term, as a nation committed to deterrence must prepare for and defend against both extremes, as well as all scenarios between the two ends of the spectrum. Similarly, while each different methodology requires a different deterrent to be truly effective,[113] each will also raise separate legal issues.[114]

4. Necessity

Finally, it is important to mention briefly the doctrine of necessity. Under the law that regulates initiation of hostilities, or jus ad bellum, the doctrine of necessity is a requirement for any self-defense response to an armed attack.[115] While the practical application of these principles to cyber operations is of

---

[107] *See* Lingyu Wang et al., *Minimum-cost Network Hardening Using Attack Graphs*, 29 COMPUTER COMM. 3812, 3812 (2006).

[108] *See* Peter Lichtenbaum & Melanie Schneck, *The Response to Cyberattacks: Balancing Security and Cost*, 36 INT'L Law. 39, 48 (2002).

[109] *Cf.* Tyler Moore, *Introducing the Economics of Cybersecurity: Principles and Policy Options*, *in* COMMITTEE ON DETERRING CYBERATTACKS, NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 9–22 (2010) (proposing several ideas to incentivize better deterrent methodologies, including cyber insurance).

[110] Antoine Lemay, Jose M. Fernandeza & Scott Knight, *Pinprick Attacks, A Lesser Included Case?*, *in* CONFERENCE ON CYBER CONFLICT PROCEEDINGS 183, 190 (Christian Czosseck & Karlis Podins eds., 2010).

[111] Kakutani, *supra* note 49, at C1.

[112] Paul Roberts, *Despite Intrusions, Chances of US–China Cyberwar Are Small*, KASPERSKY LAB SECURITY NEWS SERV. (March 1, 2012), https://threatpost.com/en_us/blogs/despite-intrusions-chances-us-china-cyber-war-are-small-030112.

[113] *See supra* notes 110–11.

[114] *See supra* notes 110–11.

[115] Craig J.S. Forrest, *The Doctrine of Military Necessity and the Protection of Cultural Property During Armed Conflicts,* 37 CAL. W. INT'L L.J. 177, 179 (2007).

great debate and beyond the scope of this Article, the doctrine of necessity is directly affected by deterrence.

Although there are several theories of how to determine whether a cyber attack has occurred, the most prominent theory involves looking at the results of the attack.[116] Generally, if the threshold of attack is crossed, the doctrine of necessity acts to limit the scope of the response in self-defense by the victim state to that amount of force necessary to counter the threat.[117] In other words, when a victim state is justifying its response to the armed attack, the victim state must demonstrate why the response is necessary and that stopping the attack cannot be accomplished by lesser means.[118]

The theories of deterrence discussed below could actually remove the ability of a victim state to justify a response because they would remove the necessity to respond. For example, one theory of deterrence is for a nation to have such redundancy in its systems that an attack, which might otherwise have significant effects on the targeted system, would not have the intended effects.[119] Because there would be no actual impact, there would also be no necessity for the victim to respond in order to restore operations.

As a matter of law, the victim nation could not justify a response as necessary if nothing resulted from the attack.[120] Even if deterrence were only able to mitigate the attack, the doctrines of necessity and proportionality[121] would restrict the legal responses available to the victim. This is certainly not a justification to forego deterrence, but it is a significant issue that must be accounted for by a nation in its various approaches to deterring adversaries.

* * *

---

116 *See* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, 84 INT'L REV. RED CROSS 365, 373–75, 378 (2002); Paul A. Walker, *Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine*, 1 NAT'L SECURITY L. BR., no. 1, 2011, at 33, 45–47.

117 Jasmine Moussa, *Can Jus Ad Bellum Override Jus In Bello? Reaffirming the Separation of the Two Bodies of Law*, 90 INT'L REV. RED CROSS 963, 973–74 (2008).

118 *See id.*

119 *See* Taipale, *supra* note 5, at 36.

120 *See id.* at 35.

121 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 51, *adopted* June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I]; *see also* DEP'T OF THE ARMY, FIELD MANUAL No. 27-10: THE LAW OF LAND WARFARE para. 41, app. A at v (Supp. 1976); Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, 50 VA. J. INT'L L. 795, 804–05, 2010. *But see* James Adams, *Virtual Defense*, 80 FOREIGN AFF., May–June 2001, at 98, 110 (arguing that it is unclear how the law of proportionality applies to information warfare).

Despite these important issues, applying deterrence through and against cyber operations is vital to national security. Accounting for the assumptions and working through the issues will be a necessary hazard for nations, but the benefits of applying a full-spectrum cyber deterrent will be worth the trouble.

II. CYBER DETERRENCE

The Internet was not designed with the goal of deterrence in mind.[122]

Cyber deterrence can and should be an active part of national security strategy. Because of their unique nature, cyber operations provide an expanded view of cyber deterrence, one that includes many of the historical notions of deterrence but which may only slightly resemble the deterrence efforts of the Cold War. This Part will be divided into two broad categories of cyber deterrence: A) Retaliation and B) Denying the benefit of the attack. Within these two categories, the Article will define and analyze six approaches to cyber deterrence and their attending legal issues.[123]

A. Retaliation

The threat of retaliation, when coupled with the present capability and apparent will to do so, can be a great deterrent to many potential actors.[124] Such a strategy was the foundation of U.S. deterrence policy during the Cold War[125] and continues to be a significant aspect of current U.S. deterrence policy.[126] Not all potential foes will be completely deterred by the threat of a response, but because many may, it is a vital aspect of deterrence. This is also true of cyber deterrence. Two specific aspects of retaliation deserve study here. First, retaliation to a cyber incident may come in the form of striking back at

---

[122] David D. Clark & Susan Landau, *Untangling Attribution*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 25, 25 (Comm. on Deterring Cyberattacks, Nat'l Research Council of the Nat'l Acads. eds., 2010).

[123] *See* Geers, *supra* note 28, at 299 (dividing cyber attack deterrence strategies into two categories: denial and punishment. Each category has three basic requirements: 1) capability; 2) communication; and 3) credibility). *But see* Taipale, *supra* note 5, at 4 (dividing his discussion of cyber deterrence into the following categories: 1) penalty; 2) futility; 3) dependency; and 4) counter-productivity).

[124] Taipale, *supra* note 5, at 44.

[125] Kugler, *supra* note 31 at 321–24; Willie Curtis, *National Missile Defense: A Retreat from Dr. Strangelove or How I Learn to Stop Worrying and Love MAD*, 36 NEW ENG. L. REV. 795, 797 (2002).

[126] *See* NEW DETERRENT WORKING GROUP, US NUCLEAR DETERRENCE IN THE 21ST CENTURY: GETTING IT RIGHT 38–39 (2009).

the perpetrator, to include the use of force.[127] Such a response is lawful in many cases, though there are attending legal issues.[128] Second, retaliation can also be based on a law enforcement paradigm and be characterized by potential legal actions, such as criminal or civil liabilities and penalties. These two means of deterrence will be discussed next.

1. Strike Back

The ability to strike an adversary in response to an attack that is imminent or has already commenced was the backbone of nuclear deterrence. Often referred to as Mutually Assured Destruction,[129] this doctrine in its most basic form relied on the threat of such a devastating attack against an opponent's complete civilization that there was no need to exercise defense.[130] In other words, the threat of such a devastating response can alter the cost-benefit analysis and convince others not to attack.

a. Response to a Cyber Attack

In response to a cyber attack, a state can consider, plan on, and signal the full spectrum of responses.[131] Promised kinetic response, even nuclear response, remains an option as a deterrent to cyber warfare. The potential for responses based on misunderstandings has prompted the United States to engage with both Russia and China concerning the establishment of a cyber version of the nuclear "hotline," where one country could forewarn the other of either unintended acts or intended acts that were not meant as aggressive.[132]

Similarly, the recent National Security Strategy for Cyberspace stated that:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country . . . . We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent

---

[127] Jeremy A. Rabkin & Ariel Rabkin, *To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict*, HOOVER INSTITUTION, 1, 3 (2012), http://media.hoover.org/sites/default/files/documents/Emerging Threats_Rabkin.pdf.

[128] *Id.*

[129] RUMBLE, *supra* note 19, at 42, 71 (explaining mutually assured destruction in nuclear deterrence).

[130] Henry S. Rowen, *Introduction* to GETTING MAD: NUCLEAR MUTUAL ASSURED DESTRUCTION, ITS ORIGINS AND PRACTICE 1, 3 (Henry D. Sokolski ed., 2004).

[131] *But see* Tang & Zhang, *supra* note 12, at 1 (arguing that retaliation is ineffective in the cyber realm).

[132] *See* Ellen Nakashima, *U.S., Russia May Use Alert System for Cybersecurity*, WASH. POST, April 27, 2012, at A1; *see also* Adam Segal, *U.S., China Butt Cyber Heads*, DIPLOMAT (June 19, 2012), http://thediplomat.com/china-power/u-s-china-butt-cyber-heads.

> with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.[133]

While this statement was controversial when made,[134] there is no doubt of its legality.[135] Neither international law nor the law of armed conflict requires a response in kind, as long as the response is proportional, as will be discussed below.

The idea of using a kinetic response to a cyber attack is not new and has been discussed in the literature.[136] It seems clear that while most commentators agree in principle, they acknowledge that responding kinetically to a cyber attack raises a number of valid concerns. With the difficulties of attribution discussed above and the ability to spoof the identity of the attacker, a kinetic response carries with it some risks.[137] Besides the attribution issue, a kinetic

---

[133] EXEC. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE 2 (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf; *see also* Kevin Chilton & Greg Weaver, *Waging Deterrence in the Twenty-First Century*, STRATEGIC STUD. Q., Spring 2009, at 31, 39.

[134] Tom Gjelten, *Pentagon Strategy Prepares For War in Cyberspace*, NPR (July 15, 2011), http://www.npr.org/2011/07/15/137928048/u-s-military-unveils-cyberspace-strategy. Additionally, the author attended an international cyber conference in Singapore shortly after the announcement was made and was literally accosted by representatives of other governments for greater explanation of this policy statement.

[135] *See infra* Part II.A.1.b; *cf.* Hathaway et al., *supra* note 5, at 841 (arguing that states may respond with armed force to a cyber attack pursuant to Article 51 of the United Nations Charter if the effects of the attack are equivalent to those of a conventional armed attack); Adam Segal, *Policy Innovation Memorandum No. 2*, COUNCIL ON FOREIGN REL. (Nov. 14, 2011), http://i.cfr.org/content/publications/attachments/Policy_Innovation_Memo2_Segal.pdf (arguing that most countries would accept that cyber attacks with "kinetic effects" could be met with kinetic responses). *But see* Jack Goldsmith, *General Cartwright on Offensive Cyber Weapons and Deterrence*, LAWFARE (Nov. 28, 2011, 10:27 AM), http://www.lawfareblog.com/2011/11/general-cartwright-on-offensive-cyber-weapons-and-deterrence (arguing that although armed responses to cyber attacks may be legal, they are unlikely to occur).

[136] *See, e.g.*, Huntley, *supra* note 70, at 39 (explaining that cyber attacks that cause physical damage, injury, or death may be met with a kinetic response); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 594 (1999) (laying out principles dictating when a kinetic response to a cyber attack may be appropriate); Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 575–77, 594 (2011) (arguing that if no other recourse exists to thwart a cyber attack amounting to an armed attack, kinetic options are permissible under the law of self-defense); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 426–40 (2011) (summarizing the debate over how cyber attacks fit into the armed attack paradigm, if at all).

[137] *See* Joyner & Lotrionte, *supra* note 62, at 856; *see also* DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 21 (1999), *available at* http://www.au.af.mil/au/

response may simply not be fast enough to act as a deterrent before the damage is done.[138] Further, a kinetic response may provoke the victim or lead to an escalation.[139] These limitations on the value of strike back as a deterrent do not prevent its usefulness but act to encourage states to not rely on one single theory of deterrence.

Additionally, nothing would preclude using cyber means to strike back at an attacker, and this is certainly an assumed possibility. Cyber responses to a cyber attack might be the most effective in some situations.[140] General Alexander recently testified before Congress, "I can assure you that, in appropriate circumstances and on order from the National Command Authority, we can back up [DoD's] assertion that any actor contemplating a crippling cyber attack against the United States would be taking a grave risk."[141] The key point is that, as a matter of signaling deterrence, strike back is not limited to cyber operations and could include the full spectrum of kinetic responses as well.

b. Legal Issues

The legal issues with preparing and signaling a kinetic strike in response to cyber warfare include all the legal issues of a kinetic strike in response to a similar kinetic strike.[142] Because these issues are not unique to cyber conflict, they deserve little attention here except to make three important points concerning "armed attack," necessity and proportional response.

i. Armed Attack

The Charter of the United Nations is the paradigm that governs the use of force by states as well as the legality of a forceful response in self-defense.[143]

---

awc/awcgate/dod-io-legal/dod-io-legal.pdf; Marco Roscini, *World Wide Warfare—Jus Ad Bellum and the Use of Cyber Force*, 14 MAX PLANCK Y.B. UNITED NATIONS L. 85, 96 (2010) (Ger.); Goldsmith, *supra* note 134.

138 Joyner & Lotrionte, *supra* note 62, at 856.

139 *See id.*

140 For example, a country may wish to send a "shot across the bow" of a cyber attacker by disabling some, but not all, of the attacker's computer systems. OFFICE OF THE GEN. COUNSEL, DEP'T OF DEFENSE, AN ASSESSMENT OF LEGAL ISSUES IN INFORMATION OPERATIONS 20 (1999).

141 *Budget Request for Information Technology and Cyber Operations Programs*, *supra* note 17, at 3 (statement of General Keith B. Alexander, Commander, United States Cyber Command).

142 *See* Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, *supra* note 136, at 913. *See generally id.* at 910–23 (discussing appropriate state responses to varying levels of cyber attack).

143 Waxman, *supra* note 136, at 426–27.

Again, it is not necessary to fully explain the paradigm here, but it is necessary to address the issue of "use of force" and "armed attack," two of the key terms in the Charter paradigm. The Charter categorically prohibits "the threat or use of force against the territorial integrity or political independence" of a state.[144] Accordingly, any cyber action that amounts to a use of force is illegal.[145] However, the Charter does not allow a victim of a cyber attack that amounts to a "use of force" to respond in self-defense.[146] Such responses are limited to activities that equate to an armed attack,[147] a standard clearly indicating a greater quantum of force than a "use of force."[148]

A state's ability to lawfully signal a "strike back" deterrent to cyber attacks would be subject to a determination that a cyber attack not only rose to the level of a use of force, but also an armed attack.[149] While conceivable as a theoretical matter, there has yet to be a reported cyber attack between states that has been acknowledged as even a use of force, let alone an armed attack.[150] The recent Stuxnet attack against Iranian nuclear capabilities,[151] if found to have been sponsored by a state, is likely the closest the international community has come to such an event.[152]

Some have argued that particular targets that are especially susceptible to cyber attack, such as certain critical infrastructure, might not require a traditional armed attack to allow a proportional self-defense response.[153]

---

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

145 Roscini, *supra* note 137, at 113.

146 *See* Waxman, *supra* note 136, at 434–35.

147 U.N. Charter art. 51.

148 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, paras. 191, 210 (June 27) ("[M]easures which do not constitute an armed attack . . . may nevertheless involve a use of force."); Albrecht Randelzhofer, *Article 51*, *in* 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 788, 790 (Bruno Simma ed., 2d ed. 2002); Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, *supra* note 136, at 587 ("Simply put, all armed attacks are uses of force, but not all uses of force qualify as armed attacks."); Waxman, *supra* note 136, at 427.

149 Roscini, *supra* note 137, at 113.

150 Hathaway et al., *supra* note 5, at 840.

151 Peter Beaumont, *Cyberwar on Iran More Widespread Than First Thought, Researchers Say*, GUARDIAN (Sept. 21, 2012), http://www.guardian.co.uk/technology/2012/sep/21/cyberwar-iran-more-sophisticated.

152 Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, JOINT FORCES Q., 4th Quarter 2011, at 70, 71.

153 Sean Condron, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 415–16 (2007); *see* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 221–29 (2002).

President Obama's May 2009 statement[154] seems to provide some support for this idea. However, the current state of international law makes no such allowance.[155] Therefore, the requirement that a cyber attack amount to an armed attack remains applicable as the necessary legal trigger before a state can respond in self-defense.[156]

In 1999, the DoD's Office of General Counsel issued its Assessment of Legal Issues in Information Operations,[157] which gave an example of a potential cyber armed attack. The Assessment states:

> [I]f a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack.[158]

The fact that the Assessment lists all of these potential harms in the conjunctive limits its usefulness as a good barometer for what cyber operations would actually rise to the level of an armed attack. However, it at least provides a starting point from which to work.

The limitation in the UN Charter on using self-defense to an armed attack does not mean that a state must sit idly while being harmed from cyber operations. As early as 1986, in a case concerning U.S. military activities in Honduras in response to an insurgency aided by Nicaragua,[159] the International Court of Justice stated that proportionate countermeasures would be permissible in response to a use of force that did not amount to an armed

---

154 *Compare* Obama, *supra* note 17 (digital infrastructure should be treated as a "strategic national asset" and attacks against it "deter[red], prevent[ed], detect[ed], and defend[ed] against . . . ."), *with* INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 133, at 14 (the United States reserves the right to use "all necessary means—diplomatic, informational, military, and economic," to defend itself against "hostile acts in cyberspace.").

155 *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 195 (June 27) (limiting the lawful use self-defensive force to when the state concerned has been the victim of an armed attack).

156 A state would still be able to respond with appropriate countermeasures. *See* Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. ONLINE 11, 12, 16, 19 (2011), http://www.yjil.org/docs/pub/o-37-hinkle-countermeasures-in-the-cyber-context.pdf.

157 OFFICE OF THE GEN. COUNSEL, *supra* note 140, at 18.

158 *Id.*

159 *Military and Paramilitary Activities in and Against Nicaragua*, 1986 I.C.J. 14, paras. 1, 15, 20.

attack.[160] The Court laid out a three-part test for the use of countermeasures in a subsequent case:[161]

> First, the action must be taken in response to a previous international wrongful act of another state, and it must be directed against that state. Second, the injured state must have called upon the offending state to discontinue its wrongful conduct or to make reparation for it. Third, the countermeasure must be commensurate with the injury suffered, taking into account the rights in question.[162]

While this is an unsatisfactory situation, particularly in response to cyber operations against critical national infrastructure,[163] it appears to be the status of the law, as illustrated by the recent International Law Commission's "Draft Articles on Responsibility of States for Internationally Wrongful Acts . . . ."[164] Article 49 allows a state to use countermeasures "against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations."[165] This wrongful act would be something short of an armed attack, thereby not allowing the victim state to respond in self-defense, but only with proportional countermeasures.

A detailed discussion of countermeasures deserves greater attention than can be given here, but it is important to note that countermeasures may be forceful[166] and can be forceful enough to induce compliance with international law.[167] In terms of cyber operations, that would mean that the appropriate countermeasure could include a kinetic or cyber option that would not be an illegal use of force,[168] but would be strong enough to convince the attacker to cease the cyber operations.

---

160 *Id.* para. 249.

161 Gabcikovo-Nagymaros Project (Hung./Slovk.), Judgment, 1997 I.C.J. 7, paras. 83–85 (Sept. 25).

162 Jensen, *supra* note 153, at 220.

163 *See id.* at 221, 229.

164 *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, U.N. GAOR, 53rd Sess., at 128–29, Supp. No. 10, art. 22, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 Y.B. Int'l L. Comm. 26, U.N. Doc. A/CN.4/SER. A/2001/Add.1.

165 *See id.* at 129.

166 *See id.* at 128.

167 *See id.*

168 *See id.*

ii. Necessity

The doctrine of necessity is adequately discussed above.[169] It is mentioned here again merely to demonstrate that this is a good example of how deterrence may remove the doctrine of necessity. It would be unlawful for a state to signal a potential kinetic or cyber anticipatory defensive action to even an armed attack, if that state's defenses were sufficient to completely nullify any damage from an impending attack.[170] If the victim state knew that an impending attack was going to be futile or completely ineffective, it would not have the necessity to act in anticipation of that attack.[171]

iii. Proportionality

Though international law does not require a response in kind to an attack, any response in self-defense is limited not only by the principle of necessity, but also by the principle of proportionality. Any planned or signaled response intended as a deterrent would have to be proportional to the threat or use of force anticipated.[172] Deputy Secretary of Defense Lynn has stated, "[w]e have to have a system that recognizes an attack, registers it and then allows us to react in a way that's appropriate and proportional."[173] As discussed above, this would not require a response in kind, but any response would have to meet this legal criterion.[174] Uniquely, cyber attacks may expand the spectrum of proportional responses available to a state.[175] Such responses could be done alone or in conjunction with kinetic responses, so long as the complete response still met the proportional response requirement.

The use of the term "proportional" does not mean that the response must be the same as the attack or equal in method.[176] Rather it means that the response must be comparable to the initial wrong and not equate to an escalation.[177] Some have argued that determining a proportionate response to a cyber

---

169 *See supra* Part I.B.4.

170 *See supra* Part I.B.4.

171 *See supra* Part I.B.4.

172 *See* Hathaway et al., *supra* note 5, at 840 n.84, 849.

173 Jared Serbu, *DoD Cyber Strategy Aims at Deterrence*, FED. NEWS RADIO (July 15, 2011), http://www.federalnewsradio.com/697/2457989/DoD-cyber-strategy-aims-at-deterrence.

174 *See supra* Part II.A.1.a.

175 *See* Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEX. L. REV. 1571, 1595 (2010); Brian T. O'Donnell & James C. Kraska, *Humanitarian Law: Developing International Rules for the Digital Battlefield*, 8 J. CONFLICT & SECURITY L. 133, 160 (2003).

176 *See supra* Part II.A.1.a.

177 Hathaway et al., *supra* note 5, at 849.

operation may prove difficult.[178] The legal standard by which a response is judged is whether it is no more than what is required to end the situation and successfully defend the victim.[179] Because cyber operations offer such a broad spectrum of potential activities, it may be that cyber responses actually will prove to be very useful in crafting a proportionate response to any attack, including a cyber attack.

While much more could be said on this specific aspect of cyber deterrence,[180] it is sufficient here to note that the cyber deterrence issues are not significantly different than kinetic deterrence issues, other than the specific aspects mentioned. The possibility of cyber deterrence through a strike back by either kinetic or cyber means should be an effective means of deterrence, at least to certain actors.

2. *Legal Strike Back*

As opposed to the Subpart above where the strike back contemplated is likely to have some destructive effect, this Subpart contemplates deterrence through the traditional law enforcement paradigm. In other words, this type of deterrence might be characterized as "I will find you after your attack and make you pay, either criminally, or civilly, or both." In discussing the need for other deterrence methodologies, Kim Taipale has written:

> [B]ecause of the particular characteristics of cyberspace—in particular because of its dual use and borderless nature; the difficulty of differentiating probe from attack and definitively identifying attackers; the zero time interval between detection and attack and the scale-free, unpredictable and unbounded nature of potential consequences; the multiplicity of potential attack vectors, attackers, and motivations; and the contestability of potential responses—a general retaliatory-based policy that explicitly threatens severe punishment in response to a particular kind of attack may not be

---

178 *Cf.* LIBICKI, *supra* note 22, at 41–52 (giving an in depth discussion of the difficulties surrounding cyber attribution).

179 *See* Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, *supra* note 136, at 582.

180 *See generally* Huntley, *supra* note 70 (discussing the connection between jus ad bellum principles and cyber attacks); Schmitt, *Computer Network Attack and the Use of Force in International Law*, *supra* note 135 (suggesting a normative framework in which to conceptualize cyber attacks); Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, *supra* note 135 (explaining fault lines in international law on the use of force and the effect of this disagreements on the status of cyber attacks); Waxman, *supra* note 136 (investigating the relationship between strategy and legal definitions of force).

> sufficient to deter cyber attacks, and, in some circumstances, may be counterproductive.[181]

As Duncan Hollis has recently written, "[c]ybercrime rules rest on the theory that if states identify and prosecute enough hackers, hactivists, and criminal organizations for cyber threats, other individuals will refrain from engaging in that conduct."[182] This same view is reflected by General Alexander who stated "[t]he bottom line is, the only way to deter cyber attack is to work to catch perpetrators and take strong and public action when we do."[183]

a. Prosecution

State practice in response to a cyber incident has almost universally relied on the criminal law paradigm.[184] This has even been true when the cyber operations were conducted against government computers. For example, the 2006 cyber attacks against government and civilian computer systems in Estonia that many initially thought were sponsored by the Russian government were eventually pursued using the criminal law paradigm.[185] The existence of an ongoing armed conflict does not seem to change this approach.[186] Therefore, if for no other reason than current state practice, legal strike back has become a significant response to cyber attack and must be considered as part of a nation's cyber deterrence strategy.[187]

Legal strike back in the form of prosecutions can undoubtedly play an important role in both general and specific deterrence. Past prosecutions signal the willingness to use the punishment and add credibility to the deterrence

---

[181] Taipale, *supra* note 5, at 3–4.

[182] Hollis, *supra* note 6, at 395.

[183] *Id.* at 396.

[184] *See, e.g.*, Adams, *supra* note 120, at 107; Hathaway et al., *supra* note 5, at 863; Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1004–05 (2001); Gilbert C. Sosa, *Country Report on Cybercrime: The Philippines*, 79 U.N. ASIA & FAR E. INST. 81–82 (2001).

[185] ENEKEN TIKK & KADRI KASKA, *Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons*, *in* PROCEEDINGS OF THE 9TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY, 288, 288–89 (Josef Demergis ed., 2010); Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 208 (2009).

[186] *See* Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 68 (2001); Kevin Poulsen, *Solar Sunrise Hacker 'Analyzer' Escapes Jail*, REGISTER (June 15, 2001), http://www.theregister.co.uk/2001/06/15/solar_sunrise_hacker_analyzer_escapes.

[187] Raduege, *supra* note 71, at 5 ("Working together, we need concerted efforts to appropriately punish criminal [cyber] activity, which will aid in deterrence in countering syndicated global criminal activity.").

methodology.[188] Public arrests and prosecutions allow states to argue that if someone hacks into their systems, the day of reckoning will eventually arrive and the hacker will pay a costly price in either jail time, money damages, or both.[189] Many nations are increasing their cyber forensics capabilities[190] and enacting domestic laws that increase both coverage and penalties for cyber crimes.[191]

International cooperation is equally important.[192] The ability to demonstrate that those who have engaged in these activities across transnational borders have been brought to justice through cooperation of nations should serve to deter would-be attackers. The Cybercrime Convention[193] and its mostly procedural provisions[194] increase the likelihood of someone from one of the signatory countries being prosecuted for cyber crime in one of the other signatory countries.[195] As these types of prosecutions occur more often, they will have a greater deterrent effect.

In addition to the Cybercrime Convention, a continuing web of bilateral Mutual Legal Assistance Treaties ("MLATs")[196] allow for a much streamlined process for seeking help when one nation is the victim of a cyber incident that originates or travels through another nation.[197] The U.S. Department of Justice

---

[188] U.S. Attorney's Office, S. Dist. of N.Y., *Six Hackers in the United States and Abroad Charged for Crimes Affecting Over One Million Victims*, FBI (Mar. 6, 2012), http://www.fbi.gov/newyork/press-releases/2012/six-hackers-in-the-united-states-and-abroad-charged-for-crimes-affecting-over-one-million-victims; Mary Slosson, *Accused LulzSec Hacker Pleads Guilty in Sony Breach*, REUTERS (April 5, 2012), http://www.reuters.com/article/2012/04/05/us-hacking-lulzsec-sony-idUSBRE8340YR20120405.

[189] U.S. Attorney's Office, S. Dist. of N.Y., *supra* note 188; Slosson, *supra* note 187.

[190] Aaron Edwards, *Manhattan Prosecutor to Centralize Efforts Against Cybercrime*, N.Y. TIMES: CITY ROOM BLOG (Aug. 14, 2012, 4:14 PM), http://cityroom.blogs.nytimes.com/2012/08/14/manhattan-prosecutor-to-centralize-efforts-against-cybercrime.

[191] For example, India has recently passed a number of new laws strengthening its position on cyber criminality. Pavan Duggal, *The View from India: Cyber Deterrence: Legal Perspectives*, *in* GLOBAL CYBER DETERRENCE, *supra* note 12, at 8, 9.

[192] *See* Tang & Zhang, *supra* note 12, at 2 (arguing that "only international cooperation will enable us to better crack down on cyber crime and ensure the healthy development of the Internet.").

[193] *See* Convention on Cybercrime art. 23, *opened for signature* Nov. 23, 2001, E.T.S. No. 185 (entered into force July 1, 2004).

[194] *Id.*

[195] *Id.*

[196] *See generally* Robert Neale Lyman, *Compulsory Process in a Globalized Era: Defendant Access to Mutual Legal Assistance Treaties*, 47 VA. J. INT'L. L. 261 (2006) (explaining how Mutual Legal Assistance Treaties streamline the evidence-gathering process).

[197] *Id.* at 276.

is actively engaged in both seeking and using MLATs as it fights cyber crime across international borders.[198]

This means of deterrence (and punishment, for that matter) is the means on which most nations currently rely. It has arguably proven very effective in many cases. However, the legal strike back option, including when facilitated by the Cybercrime Convention or MLATs, still suffers from a number of significant legal issues.

b. Legal Issues

Legal issues in legal strike back deterrence include transnational and international procedural problems, such as extradition and jurisdiction, as well as the inability for the law to reach certain actors who operate from ungoverned territory. Additionally, the paucity of effective international agreements to solve these problems limits the ability for a nation to signal legal strike back as a realistic deterrent.

The limited success of the Cybercrime Convention highlights the need for greater cooperation in this area. Currently, there are only thirty-three parties to the Convention, and many of the most notorious hacking nations are not among them.[199] The otherwise effective measures based on the Convention are much less meaningful as a deterrent when so few countries are parties.

Additionally, there are legal issues with the use of MLATs. In most cases, MLATs are subject to domestic implementation and are traditionally not a timely way to gather information or seek timely judicial assistance.[200] Countries often take many months to respond to an MLAT request.[201] The deterrent effect of prosecution likely is minimized when the trial occurs many years after the event.

There may also be limitations on the exchange of information in support of the Cybercrime Convention, an MLAT, or some other request to support prosecution. Some statutory preclusions to sharing of information exist, such

---

[198] *EU: JHA Council Authorises Signing of EU–USA Agreements on Extradition and Mutual Legal Assistance*, STATEWATCH (June 1, 2003), http://www.statewatch.org/news/2003/jun/01useu.htm.

[199] *Convention on Cybercrime*, COUNCIL OF EUR. (Sept. 13, 2012), http://www.conventions.coe.int/Treaty/Commun/print/Cherchesig.asp?NT=185&CM=*&DF=&CL=ENG.

[200] Parth Shastri, *Cyber Police Dreads Crimes that Crosses National Boundaries*, TIMES OF INDIA (July 23, 2012), http://articles.timesofindia.indiatimes.com/2012-07-23/ahmedabad/32803348_1_cyber-crimes-data-theft-data-security-council.

[201] *Id.*

as the American Servicemembers' Protection Act,[202] which prevents the "transfer of classified national security information and law enforcement information to the International Criminal Court for the purpose of facilitating an investigation, apprehension, or prosecution."[203]

One of the results of an MLAT or of the cooperative work through the Cybercrime Convention might be a request for extradition of the hacker to stand trial in the country where the damage occurred. Extradition is normally based on the principle of dual criminality, which requires that any conduct for which a victim nation is seeking extradition is criminalized in both countries.[204] Where domestic cyber legislation is still in its infancy in many nations across the world, a perpetrator might not be subject to extradition, despite the clarity of the evidence.[205]

The shortcomings of extradition demonstrate a clear need for greater harmonization of domestic laws among nations. Many groups are advocating such actions,[206] and some progress is being made,[207] but there is a long way to go. Until domestic cyber laws and procedure are harmonized to provide greater similarity in cyber crimes across national systems, effective deterrence through a legal strike back theory will be diminished.

In addition to the harmonization of domestic laws, effective deterrence for cyber malfeasance also depends on general recognition of transnational theories of jurisdiction to include the protective principle and passive personality theory.[208] Both have recently been used in terrorism cases[209] and would presumably be equally acceptable in cases of cyber operations, though there is little state practice currently in the area. For legal strike back to really deter potential actors, it is likely that these actors would have to expect that the

---

202 22 U.S.C. §§ 7421–7433 (2006) (enacted as part of the 2002 Supplemental Appropriations Act for Further Recovery from and Response to Terrorist Attacks on the United States).

203 *Id.* § 7425(a).

204 *See* Jonathan O. Hafen, *International Extradition: Issues Arising Under the Dual Criminality Requirement*, 1992 BYU L. REV. 191, 191.

205 Scot M. Graydon, *Jurisdiction Issues in Cybercrime*, 59 CONSUMER FIN. L.Q. REP. 99, 101 (2005).

206 Duggal, *supra* note 191, at 10; *see, e.g.*, Sharon R. Stevens, *Internet War Crimes Tribunals and Security in an Interconnected World*, 18 TRANSNAT'L L. & CONTEMP. PROBS. 657, 685–86 (2009).

207 *See, e.g.*, *Fair Trials International Submits Plan for Extradition Reform*, BELTRAMI & CO. CRIM. L. & GLASGOW SOLIC. BLOG (Feb. 22, 2012), http://www.beltramiandcompany.co.uk/Latest-News/Entry/human-rights/fair-trials-international-submits-plan-for-extradition-reform.html.

208 RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (1987).

209 *See, e.g.*, United States v. Yousef, 327 F.3d 56, 96–97 (2d Cir. 2003).

victim country would be able to effectively assert jurisdiction in its domestic courts.

Even if domestic laws were harmonized, formal dual criminality in extradition resolved, and principles of jurisdiction fully accepted, there are still areas in the world where legal strike back would provide little deterrence because of the limited reach of the law. These areas include failed (or failing) states and states where the computer operators were acting with the complicity of the government.

The problem with failed or failing states is that the ability to deter by threat of recourse to the law is only effective in areas where the law can reach. Just as terrorism[210] and piracy[211] tend to flourish in ungoverned or poorly governed areas, cyber actors often seek refuge in areas that are beyond the legal reach of their victims.[212] When an area lacks domestic enforcement capabilities that can respond to international or transnational procedure, the deterrent effect of legal strike back is severely diminished.

A similar legal issue occurs when a government lacks the will to respond to international and transnational procedure following a malicious cyber operation.[213] This scenario may demonstrate itself most often when the state is complicit in the attacks. An example cited for this situation is the attacks on Estonia by Russian hacktivists. Despite no direct link to the Russian government, many experts still believe that the Russians facilitated the cyber attacks. [214] Once it was determined that the attacks originated from Russian hacktivists, Estonia submitted requests to Russia for assistance in tracking the perpetrators.[215] Russia responded by refusing to provide information to Estonia under their MLAT.[216] Of course, if Russia was complicit in orchestrating the

---

210 ANGEL RABASA ET AL., UNGOVERNED TERRITORIES: UNDERSTANDING AND REDUCING TERRORISM RISKS 111 (2007).

211 *See id.*

212 *Id.* at 15–21.

213 *See generally* Shackelford, *supra* note 185, at 208 (noting how Russia refused to cooperate with an Estonian investigation into an alleged cyber attack committed by the Russian Government despite MLATs between the two countries).

214 Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (May, 16, 2007), http://www.guardian.co.uk/world/2007/may/17/topstories3.russia; *see also* Collin Allan, *Control Issues in Cyberspace* 8–9 (Apr. 5, 2012) (unpublished manuscript on file with author) (demonstrating Russian government complicity in later attacks by Russian hacktivists on Georgia).

215 *See* Shackelford, *supra* note 185, at 208.

216 *Id.*; *see also* TIKK & KASKA, supra note 185, at 289 ("In its answer to the European Commission's inquiry on that subject, the Ministry of Justice pointed out the following issues with Russia regarding cooperation in criminal matters: 1) Revision of a letter rogatory generally takes much time and reminders are

attacks, they will be hesitant to either prosecute the hacktivists or even provide information concerning the operation.

This example shows the legal difficulties generated by complicit states and, on the broader front, the problems with legal strike back as a means of deterrence. In international and transnational systems where so much is based on inter-state cooperation, legal strike back can only be an effective means of deterrence when states work together with the common goal of suppressing malicious cyber activity. Many commentators and states have urged new international agreements to promote cooperation,[217] but as community agreement of how to effectuate that goal is unlikely to coalesce any time soon, legal strike back can be effective only in limited circumstances as a deterrent and must be supplemented by additional methodologies to ensure national security.

B. Denying the Benefit of the Attack

The success of the previous two methodologies for deterrence relies on fear of some form of retaliation, either because a potential victim appears capable and willing to retaliate or because a potential victim has previously retaliated after prior attacks. The threats or historical examples of retaliation are designed to discourage future attackers.[218] However, this is not the only way to view deterrence. Deterrence can also be accomplished by denying an adversary the benefit of an attack.[219] As was recently stated by then-Deputy Secretary of Defense William Lynn:

> Our strategy's overriding emphasis is on denying the benefit of an attack. Rather than rely on the threat of retaliation alone to deter attacks in cyberspace, we aim to change an adversaries' [sic] incentives in a more fundamental way. If an attack will not have its

---

ignored; 2) Assistance is refused for procedural activities regarding suspects; this is justified by referring to the fact that the notion of 'suspect' does not exist in Russian legislation; also, Russia will not interrogate a person of Russian citizenship; 3) A prior court ruling is required as a precondition for transferring of documents; 4) Covert investigation is refused without a court order (in Estonia, the relevant authorisation is issued by the Public Prosecutor's Office); 5) On occasions, Russia has insisted that a particular request be submitted through Interpol—this was also the case in relation to the letter rogatory concerning the April/May 2007 cyber attacks.").

[217] Grigoriev, *supra* note 44, at 7; Hathaway et al., *supra* note 5, at 11; Stein Schjolberg, *The View from Norway: Wanted: A United Nations Cyberspace Treaty*, *in* GLOBAL CYBER DETERRENCE, *supra* note 12, at 11.

[218] *See, e.g.*, Kugler, *supra* note 31, at 324.

[219] *Id.* at 327.

> intended effect, those who wish us harm will have less reason to target us through cyberspace in the first place.[220]

Lynn's comment is especially important to an understanding of why cyber deterrence is different from other kinetic deterrence strategies, which rely so heavily on retaliation. Though all deterrence paradigms rely in some way on the idea of denying an adversary the benefit of the attack,[221] cyber operations allow this aspect of deterrence to become the primary approach. Through making cyber systems invulnerable to cyber attack, building resiliency into cyber systems, making certain systems invisible to attackers, and making networks so interdependent that some potential attackers would also hurt themselves in an attack, a state can deny the anticipated benefits to would-be attackers. Each of these ideas will be analyzed separately below.

One caveat to this theory of cyber deterrence: it creates a balancing between the costs of the attack and the perceived likelihood of success.[222] In other words, for some attackers where the perceived costs of the attack are near zero, even a very small chance of success compared to their cost of actual attack will almost always lead to attack. Therefore, complete deterrence would require an attacker to perceive no chance of success. Getting to a zero chance of success may simply not be possible, but the closer nations come to developing systems with a perfect or near-perfect level of security, the more likely potential attackers may be deterred.

1. Invulnerability

In the broadest terms, this deterrent methodology may be simplified as "even if you try, you can't get me."[223] This is much like the Strategic Defense Initiative ("SDI")[224] in nuclear policy, which purported to create a "shield between the U.S. and its enemies . . . that could intercept and destroy attacking ballistic missiles in mid-flight."[225] This proposed form of deterrence would

---

[220] Lynn, *supra* note 56 (stating, in addition, that "[a]n important element of our strategy is therefore focused on denying or at least minimizing the benefit of an attack."); Serbu, *supra* note 173.

[221] *See* Kugler, *supra* note 31, at 324, 327.

[222] *Id.* at 327.

[223] *See supra* Part I.B.4 (discussing the potential effects of this capability on the doctrine of necessity in relation to taking anticipatory actions prior to a computer attack).

[224] *President's Speech on Military Spending and a New Defense*, N.Y. TIMES, Mar. 24, 1983, at A20; *see also* DEP'T OF DEF., INFORMATION AND GUIDANCE ON THE PRESIDENT'S STRATEGIC DEFENSE INITIATIVE 1 (1984), *available at* http://www.dtic.mil/dtic/tr/fulltext/u2/a344624.pdf.

[225] John E. Parkinson, Jr., *International Legal Implications of the Strategic Defense Initiative*, 116 MIL. L. REV. 67, 70 (1987). A modern version of this might be the "Iron Dome" system that Israel uses against rockets

have allowed the holder to say to its enemies "fire all the nuclear weapons you want, but I can shoot them all down before they hurt me."[226] In retrospect, SDI may not have been scientifically possible at the time,[227] but it was instrumental in the downfall of the Soviet Union, as they expended time, energy, and resources to try and overcome such a great defense.[228] A similar ability to secure U.S. cyber networks and assets would significantly deter would-be attackers because of the futility of the attack.

a. Protecting the Systems

The ubiquity of cyber systems makes the task of protecting them extremely difficult. In an era of nuclear attack, SDI was designed to prevent missiles fired from the ground or launched from the sea from crossing into U.S. airspace.[229] While the targets could be very diverse, they were contained in a geographical limit and were discernible shortly after the attacks were launched.[230] Further, once an attack would have been initiated, it would have been clear that the victim state was under attack and the effects would have been generally

---

fired from the West Bank. *See Iron Dome Defense System Against Short Range Artillery Rockets*, RAFAEL ADVANCED DEF. SYS. LTD., http://www.rafael.co.il/marketing/SIP_STORAGE/FILES/6/946.pdf.

[226] While it would have been a very effective defense, the deterrent nature of the threat of producing Strategic Defense Initiative ("SDI") was very destabilizing. Stephen J. Cimbala, *The Strategic Defense Initiative: Political Risks*, AIR U. REV. (Nov.–Dec. 1985), http://www.airpower.au.af.mil/airchronicles/aureview/1985/nov-dec/cimbala.html; Parkinson, *supra* note 224, at 150–51; Eric A. Posner, *Distinguished Scholar Series: International Law and the Disaggregated State*, 32 FLA. ST. U. L. REV. 797, 821 (2005). In the context of potential state-on-state cyber warfare, the ability to produce SDI-like security on computer systems would likely be less destabilizing but should be considered.

[227] Michael A. McCann, *National Missile Defense: Legal & Policy Justifications for Expanding Deterrence & Preventing War in the 21st Century*, 3 SAN DIEGO INT'L L.J. 207, 227–28 (2002); Robert A. Ramey, *Armed Conflict on the Final Frontier: The Law of War in Space*, 48 A.F. L. Rev. 1, 23–24 n.97 (2000); David Sulek & Ned Moran, *What Analogies Can Tell Us About the Future of Cybersecurity*, 6–7 (June 18, 2009) (working paper, CCDCOE Conference on Cyber Warfare), http://www.ccdcoe.org/publications/virtualbattlefield/08_SULEK_What%20Cyber%20Analogies%20Can%20Tell%20Us.pdf.

[228] Joseph Patterson Hyder, *Cold War (1972–1989): the Collapse of the Soviet Union*, *in* 1 ENCYCLOPEDIA OF ESPIONAGE, INTELLIGENCE, AND SECURITY 238, 240 (K. Lee Lerner & Brenda Wilmoth Lerner eds., 2004); Warren E. Norquist, *How the United States Won the Cold War*, INTELLIGENCER: J. OF U.S. INTELLIGENCE STUD., Winter/Spring 2003, at 47, 51, 53, 55; Kathryn Stoner-Weiss & Michael McFaul, *Domestic and International Influences on the Collapse of the Soviet Union (1991) and Russia's Initial Transition to Democracy (1993)* 17–19 (Stanford Univ. Ctr. on Democracy, Dev., & the Rule of Law, Working Paper No. 108, 2009); Eric S. O'Malley, *Destabilization Policy: Lessons from Reagan on International Law, Revolutions and Dealing with Pariah Nations*, 43 VA. J. INT'L L. 319, 355 (2003).

[229] *See* Stoner-Weiss & McFaul, *supra* note 228, at 17.

[230] *Cf.* McCann, *supra* note 227, at 232–33 (discussing the ability of the U.S. military to analyze an enemy attack and intercept the enemy missile to prevent it from reaching its target).

predictable.[231] Attacking an adversary with an intercontinental ballistic missile would have been nearly impossible to do without the victim knowing it was under attack.

These aspects of nuclear attack are simply not the case with cyber attack. Adversaries' attack systems almost constantly change and it is almost never immediately discernible where the attack originated or what it ultimately targets.[232] Attacks on cyber systems are often undetectable,[233] and the most dangerous attack is often the one you don't know is occurring.[234] For these reasons, protecting cyber systems has to be viewed in a different way than through an SDI-type analogy.

The ability to secure networks is heavily debated[235] and beyond the scope of this paper. However, it is clearly a key foundation of cyber deterrence and one closely connected with denying the benefit of the attack.[236] As Deputy Secretary Lynn recently commented, "our strategy of securing networks to deny the benefit of an attack will help dissuade military actors from using cyberspace for hostile purposes."[237] To the degree that networks can be secure, the futility of conducting a cyber attack would act as a great deterrent. Even if only some networks could be secured or if the networks could only be secured from certain attacks, such actions would deter some attacks and/or some attackers. Therefore, security will continue to be a foundational element of cyber deterrence.

---

231 *See* Eric Sterner, *Retaliatory Deterrence in Cyberspace*, STRATEGIC STUD. Q., Spring 2011, at 62, 65–66.

232 Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 589 (2011); Geers, *supra* note 28, at 301–02; Natasha Solce, Comment, *The Battlefield Of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 307–08 (2008).

233 Arnie Heller, *Defending Computer Networks Against Attack*, SCI. & TECH. REV., Jan./Feb. 2010, at 14, 14–15.

234 Gertz, *supra* note 104.

235 *Compare* Lynn, *supra* note 56 (stating "[a]lthough no network will ever be perfectly secure, our military networks today are better defended, and our cyber hygiene more effective, than before."), *with* Mark Kaelin, *An Absolutely Secure Network Is Not Possible, but the Risk Can Be Managed*, TECHREPUBLIC (Aug. 5, 2005), http://www.techrepublic.com/article/an-absolutely-secure-network-is-not-possible-but-the-risk-can-be-managed/5820491 (noting "it is an unfortunate fact of life that no network can achieve an end-state that is totally secure. No matter how much you may wish it to be otherwise, network security, regardless of platform, is a continuous battle where engagement with intruding forces ebbs and flows with the security vulnerability of the moment. The best you can ultimately achieve is a stalemate where the risk of invasion is at a manageable level.").

236 Kugler, *supra* note 31, at 324, 327, 334.

237 Lynn, *supra* note 56, at 2.

b. Legal Issues

In addition to the technological concerns, the ability to secure computers and computer networks also raises significant legal concerns. These concerns center around the interaction any security measures would have with private-civilian institutions that facilitate the Internet and with friends, allies, and partners who might have to interact through these security measures and the potential technology transfer issues necessary to facilitate that.[238] Additionally, there would inevitably be some legal issues with enforcing the requirements necessary to maintain that level of security from the threat of employees and insiders.[239] As mentioned above,[240] the ability for one state to make itself impervious to attack may, under international law, significantly affect that victim nation's ability to respond in self-defense to an adversary's actions.

The vast majority of government Internet traffic in the United States flows over civilian Internet infrastructure. Some accounts have that number as high as ninety-eight percent.[241] The implementation of any security measure to protect against malicious cyber operations would necessarily affect private Internet providers.[242] However, President Obama has made it clear that he will not dictate security measures to the private sector. In a recent speech, President Obama stated:

> 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.[243]

Even if President Obama took a different view, the legality of imposing specific security measures on private entities is dubious at best,[244] though this is potentially easier with private entities that contract with the government.[245]

---

238 *See infra* notes 241–48 and accompanying text.

239 *See infra* notes 249–61 and accompanying text.

240 *See supra* Section II.A.1.b.iii.

241 Eric Talbot Jensen, *Cyberwarfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1534 (2010) (citing a statement by Michael McConnell, former Director of National Intelligence).

242 *Id.* at 1555–56.

243 Obama, *supra* note 17.

244 *See* Ellen Nakashima, *NSA Thwarted in Cybersecurity Initiative*, WASH. POST, Feb. 28, 2012, at A1, A2; Michelle Richardson, *Keep Domestic Cybersecurity Efforts in Civilian Hands*, ACLU (Apr. 27, 2012), http://www.aclu.org/blog/national-security-technology-and-liberty/keep-domestic-cybersecurity-efforts-civilian-hands.

Further, if the government imposed security measures, some form of monitoring of the civilian networks would be required. Governmental monitoring of the Internet has already been a controversial topic in the past.[246] This may explain some of President Obama's hesitation to regulate civilian networks. The legality of such government monitoring would be contested and would certainly have to be made clear before any system was put in place.

Additionally, some in Congress have proposed a "kill switch" option for the President in cases of large-scale attacks or significant danger to the infrastructure.[247] Such action by the President would not only have a significant impact on the private sector and implicate the President's constitutional authority, but it would also have significant implications on individual rights.[248]

Similarly, particularly for government agencies, much of the government's communications with allies and partners occurs over the Internet.[249] Whatever security measures the government installs may affect its ability to communicate with others. For example, if the government develops some enhanced encryption system, it might require the government to share technology with allies/partners to ensure that they can receive the encrypted communications. Any technology transfer of this kind is likely regulated by

---

[245] *See* Dep't of Def., *News Release: DOD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities* (May 11, 2012), http://www.defense.gov/releases/release.aspx?releaseid=15266; Elizabeth Ferrell & Erin Sheppard, *Interim DoD Regulation Expands Defense Industrial Base Pilot to Facilitate Government–Industry Cooperation on Cybersecurity*, MCKENNA LONG & ALDRIDGE (May 14, 2012), http://www.mckennalong.com/publications-advisories-2975.html.

[246] *See* David J. Barron, *Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch*, DEP'T OF JUST. (Aug. 14, 2009), http://www.justice.gov/olc/2009/legality-of-e2.pdf; *see also* Ellen Nakashima, *Cybersecurity Plan Doesn't Breach Employee Privacy, Administration Says*, WASH. POST, Sept. 19, 2009, at A16; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

[247] Jon Swartz, *Should the Internet Have an 'Off' Switch? Bill Gives President Power to Shut It Down During Cyberattack*, USA TODAY, Feb. 16, 2011, at 1B; *see also* Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. § 249 (2010). This bill was later revised to become the Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. § 1 (2011).

[248] Swartz, *supra* note 247, at 1B; *see also* Karson K. Thompson, Note, *Cybersecurity and the Internet Kill Switch Debate*, 90 TEX. L. REV. 465, 487–88, 491 (2011).

[249] *Cf. Budget Request for Information Technology and Cyber Operations Programs*, *supra* note 17, at 3 (statement of General Keith B. Alexander, Commander, United States Cyber Command) (discussing the U.S. Government's reliance on the accessibility of the Internet).

various export regimes[250] and may require additional legislation to allow such transfer.

Another potential legal issue with a deterrence strategy based on security of computers and computer networks is the ability to control and monitor the personnel who operate the systems. One of the most effective ways to infiltrate a system with malicious code is to have someone with approved access to the system accomplish the infiltration.[251] This is known generally as the "insider" problem.[252] The idea is that one can avoid many of the security measures that protect a computer if someone installs malware who already has access to the system.[253] Some have speculated that just such an approach was necessary to effectuate the Stuxnet malware.[254]

The U.S. government recognizes the potential use of an insider for espionage.[255] A recent DoD Directive defined the counterintelligence insider threat as "[a] person, known or suspected, who uses their authorized access to DoD facilities, personnel, systems, equipment, information, or infrastructure to damage and disrupt operations, compromise DoD information, or commit espionage on behalf of a [foreign intelligence entity]."[256] The directive places shared responsibility for protection against the insider threat on counterintelligence, law enforcement, and antiterrorism forces.[257]

Trying to protect against the insider threat suggests numerous legal issues, including searches of employees' offices, computers, and persons;[258]

---

250 Arms Export Control Act, 22 U.S.C. § 2778 (2010) (providing strict controls on the export of defense-related materials, including the technical data, to a foreign national or a foreign nation); *see also* Exec. Order No. 12591, 52 Fed. Reg. 13,414 (Apr. 10, 1987).

251 *See* Steven M. Bellovin, *The Insider Attack Problem Nature and Scope*, *in* INSIDER ATTACK AND CYBER SECURITY 1, 1–4 (Salvatore J. Stolfo et al. eds., 2008).

252 *Id.*; *see also* DEP'T OF DEF., INSTRUCTION NO. 5240.26, at 13 (2012) (defining an insider as "[a]nyone who has authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD.").

253 *See* Bellovin, *supra* note 251, at 3.

254 Dan Raywood, *'Iranian Acting for Israel' Planted Stuxnet Virus*, SC MAGAZINE (Apr. 16, 2012), http://www.scmagazineuk.com/iranian-acting-for-israel-planted-stuxnet-virus/article/236635.

255 *See* DEP'T. OF DEF., *supra* note 4, at 3 (discussing at length the danger of the insider and describing the potential effect as "devastating.").

256 DEP'T OF DEF., *supra* note 252, at 13.

257 *Id.* at 6–9.

258 Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 345 (2011); Bryan R. Lemons, *Warrantless Workplace Searches of Government Employees*, FED. L. ENFORCEMENT TRAINING CENTER, http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/4th-amendment/workplacesearches.pdf (last visited Oct. 10, 2012).

consensual and non-consensual monitoring in the workplace and non-workplace;[259] and the ability to conduct initial background and continuing qualifying security checks.[260] Consent and waiver will likely play a significant part in working through these legal issues, but they also have limits based on reasonableness.[261]

To be truly effective against an insider, he or she would have to be monitored not only at work but outside of work and in ways that are likely too invasive to survive U.S. constitutional review. Therefore, the mitigation of potential threats may be all the law will allow.

Finally, as mentioned above, if a nation is attacked, but there is no result due to the security of its systems, the victim nation may have limited its own lawful ability to respond with countermeasures[262] or in self-defense.[263] There is insufficient state practice in this area to determine what would actually be acceptable,[264] but it seems unlikely that a nation would just permit the attacks and take no responsive action.

2. *Resiliency*

The idea of resiliency is that a nation's cyber systems are so durable that an attack will not actually hurt the victim.[265] This type of deterrence will not necessarily deter adversaries who are after specific information that is resident on a single target computer or system or who just want to degrade a particular computer; however, the victim's resiliency may remove the incentive to attack if the attacker's goal is to achieve system-wide degradation or destruction.

---

259 Michele Morris, *Employees' Fourth Amendment Rights Beyond Their Work Space: The Employment Relationship as a Source of Privacy Expectations*, 23 W. NEW ENG. L. REV. 191, 234–35 (2001).

260 THOMAS R. GIMBLE, OFFICE OF THE INSPECTOR GEN. FOR THE DEP'T OF DEF., DoD SECURITY CLEARANCE ADJUDICATION AND APPEAL PROCESS, passim (2003).

261 Michelle Hess, *What's Left of the Fourth Amendment in the Workplace: Is the Standard of Reasonable Suspicion Sufficiently Protecting Your Rights?*, 15 FED. CIR. B.J. 255, 261–71 (2006).

262 Hinkle, *supra* note 156, at 14–16; *see* Jensen, *supra* note 153, at 220 ("[T]he countermeasure must be commensurate with the injury suffered . . . .").

263 Moussa, *supra* note 117, at 973–74 (discussing the limitations necessity and proportionality place on states acting in self defense).

264 Raduege, *supra* note 71, at 4.

265 *See* DEP'T OF DEF., *supra* note 4, at 6 ("Operating with a presumption of breach will require DoD to be agile and resilient, focusing its efforts on mission assurance and the preservation of critical operating capability."); *see also* Taipale, *supra* note 5 (using futility and subcategories of redundancy and recovery to describe resiliency).

Resilience comes in two major categories: redundancy and reconstitution.[266] The ability to continue to function even after a successful attack (redundancy)[267] or to rebuild the system so quickly that the effects of the successful attack are minimal (reconstitution)[268] will deter a certain segment of those conducting attacks.

a. Redundancy

Redundancy in a system acts as a deterrent to potential attackers because it limits the ability of an attacker to inhibit functionality of the system.[269] When a cyber system is sufficiently redundant, the attacker may be able to shut down specific computers or portions of the system, but enough alternative systems continue to run the required capabilities so that the system is still able to function.[270]

In a larger sense, the Internet functions in much the same way. Due to the architecture of the system, even if a large section were disconnected or stopped responding in accordance with normal protocols, the Internet is large enough and constructed in a redundant manner such that it would continue to function.[271] Digital packets would continue to find a path to their required active destination. Individuals may lose access for a time, but the system would continue to work.[272]

Truly redundant cyber systems would make allowance for redundancy even at the individual–user level. In other words, any function that was necessary for the system would be performable at multiple points so that one system did

---

[266] Retired United States Air Force Lieutenant General Harry D. Raduege, Jr., calls resilience the first leg of a new "cyber triad" and defines resilience as "redundancy of critical connectivity; the ability to handle increased traffic loads, even under the most stressed conditions; and the ability to protect and secure sensitive and private information." Raduege, *supra* note 71, at 4.

[267] Taipale, *supra* note 5.

[268] GLASER, *supra* note 28, at 1. The term "recovery" is used as a synonym for reconstitution. *See* Taipale, *supra* note 5.

[269] Taipale, *supra* note 5; *e.g.*, *Budget Request for Information Technology and Cyber Operations Programs*, *supra* note 17, at 3 (statement of General Keith B. Alexander, Commander, United States Cyber Command) ("Our strategic objective is to reduce the attack surface of our critical networks that is available to adversaries, enabling us to 'Defend and Jump' as needed."). The "Defend and Jump" theory represents a method of redundancy.

[270] Taipale, *supra* note 5.

[271] Chuck Yoke, *The Internet—Redundant, Reliable, and Risky*, NETWORK WORLD (Sept. 5, 2005), http://www.networkworld.com/columnists/2005/090505yoke.html.

[272] *Id.*

not represent a single point of failure.[273] On a broader scale, system functionality would be spread over sufficient platforms so that when a segment of those platforms was degraded, the overall system would continue to function.[274]

If a system is sufficiently redundant that attacks do not degrade the system's ability to operate, attackers whose intent is to threaten the functioning of the system will be deterred from attacking. Again, this will not deter all adversaries, but it will deter a certain section of cyber operators with specific goals and intentions.

b. Reconstitution

In addition to redundancy, a nation can deter would-be attackers by increasing its ability to reconstitute after an attack. This is a slightly different view of resiliency, in that it does not actually mean that the attack will not have its desired effect in the short term, but rather it means that the nation can reconstitute so quickly that the effects of the attack are minimal, if felt at all.[275] Reconstitution might be accomplished by having a stockpile of computers or servers that a victim could utilize in the event that his or her normal computer or server is disabled by an attack.[276] Some have suggested that the United States maintain a "strategic reserve" of bandwidth in the event of a debilitating attack on government and industry.[277] However reconstitution is effectuated, the key is that the system can suffer an attack and recover in such a way and in such time that the functionality of the system is not compromised.[278]

c. Legal Issues

As with other deterrent methods, achieving resilience has many potential legal issues and implications. The United States' ability to achieve redundancy and/or reconstitute after an attack is significantly impacted by domestic law and regulation. For example, if the government determined that it would achieve bandwidth redundancy by passing a law allowing the government to take bandwidth from the private sector in time of need, that action might

---

273 Taipale, *supra* note 5.
274 *Id.*
275 *See id.* (using the term "recovery" as a synonym for "reconstitution").
276 *See id.*
277 Jensen, *supra* note 241, at 1567 & nn.209 & 210.
278 GLASER, *supra* note 28, at 1.

infringe on individual rights. A recent bill proposing a kill switch for the President in time of emergency[279] received concerted opposition because of its infringement on the private sector and individual rights.[280]

Additionally, when contemplating the availability of back-up or replacement systems that could be employed to reconstitute after an attack, the rules of government purchasing require a bona fide need for every purchase.[281] It is unlikely that, without some kind of Congressional fiscal regulation, the government could purchase large numbers of computers and other spare systems in case of an attack where spares would be needed.

There are also international legal implications of a resilient system. Under the current legal paradigm, a state may respond to an attack with a proportional response.[282] Whether that response is a countermeasure to an unlawful use of force, or an action in self-defense in response to an armed attack, it must be proportional.[283]

Much like the similar issue discussed above in reference to security, assuming that an attack occurs but the system is so resilient that there are no effects, the targeted state would be very limited in its ability to respond.[284] What is a proportionate response to a completely ineffective attack? One might argue that a proportionate response might still include doing what is necessary to prevent any future attacks;[285] however, this position is not universally

---

279 *See* Protecting Cyberspace as a National Asset Act of 2010, S. 3840, 111th Cong. § 249 (2010); H.R. 5548, 111th Cong. (2010); Hathaway et al., *supra* note 5, at 875–76.

280 *See* Daniel Tencer, *Obama May Get Power To Shut Down the Internet Without Court Oversight*, RAW STORY (Jan. 24, 2012), http://www.rawstory.com/rs/2011/01/24/power-shut-internet-court-oversight.

281 31 U.S.C. § 1502(a) ("The balance of an appropriation or fund limited for obligation to a definite period is available only for payment of expenses properly incurred during the period of availability or to complete contracts properly made within that period of availability and obligated consistent with section 1501 of this title. However, the appropriation or fund is not available for expenditure for a period beyond the period otherwise authorized by law.").

282 *See supra* note 133 and accompanying text.

283 *See supra* note 172 and accompanying text.

284 *See supra* notes 176–77 and accompanying text.

285 In response to the April 5, 1986, bombing of a Berlin discothèque by Libyans, U.S. Air and Naval assets executed Operation El Dorado Canyon and struck targets in and around Tripoli, including an intelligence headquarters, military bases, airfields, and suspected terrorist training camps. President Ronald Reagan announced, "[t]hese strikes were conducted in the exercise of our right of self-defense under Article 51 of the United Nations Charter. This necessary and appropriate action was a preemptive strike . . . designed to deter acts of terrorism by Libya . . . ." Letter from Ronald Reagan, President Of the United States, to the Speaker of the House of Representatives & the President Pro Tempore of the Senate on the United States Air Strike Against Libya (Apr. 16, 1986), *in* 1 PUBLIC PAPERS OF THE PRESIDENTS OF THE UNITED STATES: RONALD REAGAN, 1986, at 478 (1988).

accepted as compliant with international law.[286] To the degree that a resilient system would have a self-limiting effect on a proportionate response by the victim state, it acts as a disincentive on states to use this form of deterrence.

3. *Invisibility*

One way to protect oneself from attack is to be invisible to your enemies. If an adversary cannot find the systems or computers it intends to attack, it will be deterred from conducting attacks.[287] In such a case, it would not matter how potent an adversary's weapons might be; if the attacker cannot find the target, its weapons are ineffective.

a. Hiding the System

Invisibility works as a deterrent because, if the adversary cannot find his target, he will take his efforts elsewhere. Even if the attacker knows the system exists, he will have to determine how to allocate his time and resources to try to locate it. In an environment where there are lots of available targets, systems that are harder to find will be less likely to be attacked. If the system is completely invisible, to the extent that is technologically possible, attackers can search continuously with no chance of success.

Invisibility includes more than just making the existence of the system invisible; it also includes masking the true nature or attributes of the system.[288] This type of invisibility may be more practical. As Martin Libicki wrote in his work on deterrence prepared for the U.S. Air Force,

> By falsely portraying its networks and their contents, DoD can variously hope to persuade the attacker to direct its energies elsewhere; hope to misdirect the attacker's focus; and hope to give the attacker an exaggerated or understated view of what it has been able to accomplish—not to mention foster a false impression of its physical capabilities.[289]

Invisibility includes presenting the system as something it is not, either by making the system look like something else, or by making something else look

---

286 *See infra* Part II.B.3.a.
287 *See infra* Part II.B.3.a.
288 *See* LIBICKI, *supra* note 22, at 171–72.
289 *Id.*

like the system.[290] The latter approach includes the use of "honeypots," spoofed systems meant to lure attackers into a harmless yet apparently valid system.[291] In these cases, the initial attacker may not be deterred, but as the system becomes known to have these attributes, and as the lack of success of would-be attackers becomes known, the invisibility mechanisms of the system will deter future attackers.

b. Legal Issues

Most of the legal issues with this form of deterrence seem to revolve around hiding the true nature of attributes of the computer system. To the extent that making a system truly invisible is technologically possible, the methodology for doing so may raise legal issues, but there do not appear to be any legal issues inherent in having a system that no one can see or detect.

In contrast, many legal issues arise as someone tries to mask the true nature of his or her computer systems by representing them as something they are not or by having other computer systems appear to be his or hers. Taking the former first, the law requires that belligerents separate, to the maximum extent feasible, their military objectives from the civilian population.[292] The practical application of this provision of law in the cyber age is a matter of great discussion,[293] but it would seem to clearly preclude purposefully cloaking military systems as protected civilian systems to hide them from potential attackers.[294]

Even more egregious would be any attempt to represent military systems as systems that receive special protections under the LOAC, such as those belonging to the International Committee of the Red Cross ("ICRC") or medical or religious computer systems. During an armed conflict, these actions would most likely be grave breaches of the Geneva Conventions and trigger a nation's requirements to search out and prosecute those responsible for such actions.[295]

---

290 *See, e.g.*, Lauren Oudet, *Fighting Internet Worms with Honeypots*, SYMANTEC, http://www.symantec.com/connect/articles/fighting-internet-worms-honeypots.

291 LIBICKI, *supra* note 22, at 172–73; Oudet, *supra* note 290.

292 Protocol I, *supra* note 120, art. 58.

293 *E.g.*, Jensen, *supra* note 241, at 1549–52.

294 *See, e.g.*, *id.*

295 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 50, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva Convention I]; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed

By masking the true nature of computer systems, government—particularly military—actions undercut the basic LOAC principle of distinction in armed conflict: combatants have an obligation to have a "fixed distinctive sign recognizable at a distance" and to "[carry] arms openly."[296] It is unclear how this principle will be applied by states in the cyber age,[297] but it seems to preclude portraying military computers as civilian computers and conducting attacks from computers not clearly identifiable as belonging to the military.[298]

Cyber actions during armed conflict might invoke the principles of ruse and perfidy,[299] particularly if a nation was using or spoofing a protected system, such as the ICRC, in order to gain advantage based on the adversary's reliance on the LOAC. Any such actions would be violations of the LOAC and would seriously undercut the principle of distinction.[300] These principles would apply equally to defensive measures during armed conflict.

There are also legal issues with having other computers appear to be the target computers. This might occur if a government knows adversaries are targeting a system of computers that monitor the logistics movements of military goods. To protect that system, the government creates another, false system that appears to be the logistics systems but is populated with false and misleading data.[301] These types of systems are often referred to as honeypots.[302]

While there is nothing inherently illegal in using honeypots,[303] the method for attracting adversaries might raise legal issues, as well as any deceptive

---

Forces at Sea art. 51, Aug. 12, 1949, 6, U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War art. 130, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 147, Aug. 12, 1949, 6, U.S.T. 3516, 75 U.N.T.S. 287.

296 Geneva Convention III, *supra* note 295, art. 4.

297 *See* Michael N. Schmitt et al., Computers and War: The Legal Battlespace, 11–12 (June 2004) (working paper) (on file with Harvard Univ. Program on Humanitarian Policy & Conflict Research).

298 The use of attacking with computers on a ".com" domain versus a ".mil" domain needs much more discussion and analysis amongst both practitioners and academics. Disclosed state practice has been very limited in this area, making it difficult to address this topic.

299 *See* Protocol I, *supra* note 121, art. 37; Int'l Comm. of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, at 430–40 (1987).

300 Geneva Convention III, *supra* note 295, at art. 4; Protocol I, *supra* note 121, art. 37.

301 *See* Oudet, *supra* note 290.

302 *Id.*

303 Ian Walden & Anne Flanagan, *Honeypots: A Sticky Legal Landscape?*, 29 RUTGERS COMPUTER & TECH. L.J. 317, 323–24 (2003) (explaining that the passive presence of a honeypot is insufficient to amount to entrapment under U.S. law).

information available in the honey pot. For example, if the honeypot provided information that misdirected the adversary's focus and then led the adversary to attack a protected target such as the ICRC,[304] this type of misdirection might be a violation of the LOAC.[305]

4. Interdependence

The final method of cyber deterrence discussed in this Article is interdependence.[306] As with others, this method has unique characteristics in the cyber paradigm. The ability to become digitally interconnected and interdependent with other nations, including adversaries, has increased exponentially with the advent of the Internet.[307] The DoD recognizes that "[t]he development of international shared situational awareness and warning capabilities will enable collective self-defense and collective deterrence."[308]

Interdependence is a broad proposition and can occur over a multitude of genres. The Internet has facilitated interconnectedness in finances,[309] science,[310] the arts,[311] and a host of other fields that facilitate state governance and provide a richer life experience to citizens.[312] This interdependence has led to some inherent disincentives for states and non-state actors to conduct cyber attacks.

During the 2003 invasion of Iraq, the United States contemplated conducting a cyber attack on Saddam Hussein's financial networks.[313] It

---

304 Geneva Convention I, *supra* note 295, arts. 24, 26.

305 *See id.* (explaining that members of the ICRC are entitled to the same protections as medical personnel engaged in providing aid).

306 *See* Taipale, *supra* note 5, at 39–40.

307 *See id.*

308 *See* DEP'T OF DEF., *supra* note 4, at 9. The DoD also claims, "[e]very year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and governmental departments and agencies." *Id.* at 4.

309 *Global Internet Users Manage Finances (59%), Shop (48%), and Look for Jobs (41%) Online*, IPSOS (Apr. 3, 2012), http://www.ipsos-na.com/news-polls/pressrelease.aspx?id=5573.

310 *See* Ian Peter, *So, Who Really Did Invent the Internet?*, NETHISTORY, http://www.nethistory.info/History%20of%20the%20Internet/origins.html (last visited Sept. 11, 2012).

311 Mary Madden, Pew Internet & Am. Life Project, Presentation to the Chicago Wallace Audience Engagement Network: The Internet and the Arts: How New Technology Affects Old Aesthetics (Apr. 22, 2008), *available at* http://www.slideshare.net/tchoubar/the-internet-andthearts42208.

312 Duncan Cornell Card, *The Internet and Democratic Stability: The Legal Challenge To Face the Threat*, 56 U.N.B. L.J. 22, 22–23 (2007) (Can).

313 John Markoff & Thom Shanker, *U.S. Weighs Risks of Civilian Harm in Cyberwarfare*, N.Y. TIMES, Aug. 2, 2009, at A1.

appears the attack was not carried out because "Bush administration officials worried that the effects would not be limited to Iraq but would instead create worldwide financial havoc, spreading across the Middle East to Europe and perhaps the United States."[314] This type of interdependence might not only act as a deterrent on attackers but also on those who retaliate in response to a prior attack.[315]

Importantly, not all forms of interdependence are desirable. The DoD Cyberspace strategy acknowledges the danger to supply chains from too much interdependence.[316] For example, some of the United States' key materiel components are only manufactured in adversary nations such as China.[317] Supply chain liabilities are a serious concern that should be balanced with the potential benefits to deterrence.

a. Sharing the Pain

The increasing level of interdependence allows a target nation to argue to the attacker that hurting the target state equally hurts the attacker.[318] Arguments such as this admittedly have much more impact on nations than on non-state actors, but even some non-state actors might be persuaded that attacking certain aspects of an area of interconnectedness, such as the target state's economic power, may have significant impacts on the non-state actor's ability to accomplish its overall objectives.

The most obvious candidates for this method of deterrence are nations that share the same currency (such as the Euro)[319] or are actively engaged in a trade agreement, such as members of the European Union[320] or the North American Free Trade Agreement.[321] However, this could also be effective between potential cyber adversaries such as the United States and China or the United States and Russia. China is now the top-trading partner for imports and second

---

314 *Id.*

315 Tang & Zhang, *supra* note 12, at 1–2.

316 DEP'T OF DEF., *supra* note 4, at 8.

317 Scott Hamilton, *Outsourcing U.S. Defense: National Security Implications–UPDATED*, NAT'L DEF. (Jan. 2011), http://www.nationaldefensemagazine.org/archive/2011/January/Pages/OutsourcingUSDefenseNationalSecurityImplications.aspx.

318 Taipale, *supra* note 5, at 39–40.

319 *Preface* to THE EURO AND THE DOLLAR IN A GLOBALIZED ECONOMY xvii (Joaquin Roy & Pedro Gomis-Porqueras eds., 2007).

320 *Basic Information on the European Union*, EUROPEAN UNION, http://europa.eu/about-eu/basic-information/index_en.htm (last visited Sept. 19, 2011).

321 North American Free Trade Agreement, U.S.-Can.-Mex., Dec. 17, 1992, 32 I.L.M. 289, 605 (1993).

for total trade with the United States,[322] and Russia is the twentieth.[323] Much of this trade is carried out via cyber systems.[324] While this global economic interdependence has proven insufficient to prevent these countries from using cyber means to steal large amounts of commercial and economic data from U.S. businesses,[325] it undoubtedly disincentivizes both Russia and China to take actions that would significantly harm the U.S. economy and, in particular, the ability of U.S. citizens to conduct cyber commerce. This is exemplified by the experience of the U.S. in the 2003 Iraq War mentioned above.[326] The interdependence within the financial system of the United States and its allies was enough to deter the United States from attacking Saddam Hussein's finances.[327]

The same argument works to lesser degrees with countries with which the United States' trade is less. Increasing the economic and other interdependence with these countries may increase the incentive for them to prevent serious cyber attacks that emanate from within their borders that would have serious effects on the United States.

Additionally, countries like China and Russia, which are now the attackers, may quickly become the attacked, necessitating increased cooperation.[328] In a recent visit by Chinese Defense Minister Gen. Liang Guanglie, he and U.S. Secretary of Defense Leon Panetta "discussed ways their countries can 'jointly work' to boost cybersecurity . . . ."[329]

---

322 *U.S. Trade Balance, by Partner Country 2011*, U.S. INT'L TRADE COMM'N, http://dataweb.usitc.gov/scripts/cy_m3_run.asp (last visited Sept. 19, 2011); *see also* Ryan Fisher, *U.S.–China Cyber Policy: Fighting a Tiger with Wings* (unpublished manuscript) (on file with author).

323 *U.S. Trade Balance, by Partner Country 2011*, *supra* note 322.

324 Caroline L. Freund & Diana Weinhold, *The Effect of the Internet on International Trade*, 62 J. INT'L ECON. 171, 171–72 (2004).

325 *Budget Request for Information Technology and Cyber Operations Programs*, *supra* note 17, at 3 (statement of General Keith B. Alexander, Commander, United States Cyber Command); *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*, OFFICE OF NAT'L COUNTERINTELLIGENCE EXEC. (Oct. 2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; Lisa Daniels, *DOD Needs Industry's Help to Catch Cyber Attacks, Commander Says*, AM. FORCES PRESS SERV. (Mar. 27, 2012), http://www.defense.gov/news/newsarticle.aspx?id=67713.

326 *See supra* notes 313–15 and accompanying text.

327 Markoff & Shanker, *supra* note 313, at A1.

328 *See* Adrian Croft, *Russia Says Many States Arming for Cyber Warfare*, REUTERS, Apr. 25, 2012, *available at* http://www.reuters.com/article/2012/04/25/germany-cyber-idUSL6E8FP40M20120425 (noting that while Russia has allegedly used cyber espionage against the United States, it now supports a globally binding treaty on cyber security).

329 Bill Gertz, *PLA General Denies Cyber War*, WASH. TIMES (May 9, 2012), http://www.washingtontimes.com/news/2012/may/9/inside-the-ring-pla-general-denies-cyberwar; *see also* Cheryl Pellerin,

b. Legal Issues

Legal issues in this area revolve mostly around gaining and maintaining interdependence. In order to gain cyber interdependence and its resulting deterrence, the United States may have to engage in technology transfer, as discussed above.[330] In the past, the United States has been hesitant to share technology,[331] such as encryption,[332] and has prevented such transfers. Over time, the United States has relaxed those restrictions,[333] but future developments might trigger similar legal impediments in the future.

Similarly, when the United States allows the sale of sensitive technology, it usually requires the receiving nation to make commitments to not transfer that technology any further.[334] A similar regime might exist in the case of technology designed to facilitate interdependence, causing the establishment of some means of verification that no further transfer to another nation or entity takes place.

Another legal issue with increasing interdependence is liability. As networks and systems become more interdependent, determining liability for damage and/or losses becomes more difficult.[335] This is true due to cascading effects on interdependent systems, as was the worry in the case of the aborted Iraq attack,[336] but also because some issues may be caused simply from the intertwining of multiple systems and their interaction. Establishing a basis for determining legal liability for losses and damage will present a technological and diplomatic hurdle.

U.S., China Must Work Together on Cyber, Panetta Says, AM. FORCES PRESS SERV. (May 7, 2012), http://www.defense.gov/news/newsarticle.aspx?id=116235.

330 *See supra* Part III.B.1.b.

331 *See* Matthew Crane, *U.S. Export Controls on Technology Transfers*, 2001 DUKE L. & TECH. REV. 0030, ¶¶ 4–7; Steven R. Weisman, *Tech Sales to China Questioned*, N.Y. TIMES, Jan 1, 2012, at C1; *Illegal Technology Transfer*, U.S. DEPT. OF AGRI., http://www.dm.usda.gov/ocpm/Security%20Guide/T1threat/Techtran.htm (last visited Nov. 16, 2012).

332 *See* Ira S. Rubinstein & Michael Hintze, *Export Controls on Encryption Software*, *in* COPING WITH U.S. EXPORT CONTROLS, 2000, at 505 (Evan R. Berlack & Cecil Hunt eds., 2000).

333 *See* Crane, *supra* note 331, ¶ 2.

334 *See* Mal Zerden, Presentation, Department of State Directorate of Defense Trade Controls (on file with author); *Third Party Transfers*, AUSTL. GOV'T DEP'T DEF. http://www.defence.gov.au/deco/transfers.htm (last visited Sept. 19, 2011).

335 *See* Taipale, *supra* note 5, at 30.

336 Markoff & Shanker, *supra* note 313, at A1.

CONCLUSION

Just as the end of the Cold War did not mark the permanent cessation of hostilities,[337] it also did not end the need for deterrence. In the emerging cyber age, nations are subject to attacks in new and innovative ways, representing significant national security threats.[338] Even as cyber capabilities provide unique and innovative tools to accomplish national goals,[339] they also allow for distinctive methods of deterrence, both similar to traditional deterrence methodologies, such as retaliation, and some methodologies that are new and innovative, such as invulnerability, invisibility, resiliency, and interdependence.[340] As nations work to develop these methods of cyber deterrence, they will need to be cognizant of corresponding legal issues that will naturally arise.

These legal issues include aspects of international law, the LOAC, and U.S. domestic law. By understanding the theories of deterrence and their corresponding legal issues, nations can expand the role of cyber deterrence and work to accomplish national objectives more effectively in the cyber age.

---

337 Charles A. Kupchan, *NATO's Final Frontier: Why Russia Should Join the Atlantic Alliance*, FOREIGN AFF., Mar.–Apr. 2010, at 100, 100–01.

338 *See* Adams, *supra* note 121, at 98–99.

339 *See supra* note 22 and accompanying text.

340 *See supra* Part II.B.