American University Law Review

Volume 62 | Issue 5 Article 4

2013

When Cyberweapons End up on Private Networks: Third Amendment Implications for Cybersecurity Policy

Alan Butler

Recommended Citation

Butler, Alan. "When Cyberweapons End up on Private Networks: Third Amendment Implications for Cybersecurity Policy." American University Law Review 62, no.5 (2013): 1203-1242.

When Cyberweapons End up on Private Networks: Third Amendment Implications for Cybersecurity Policy

Keywords
America the Virtual: Security, Privacy, and Interoperability in an Interconnected World, United States. Constitution. 3rd Amendment, United States. Supreme Court, Cyberweapons, Computer viruses, Cyberspace -- Security measures -- Government policy, Private networks, Malware (Computer software), Property rights -- United States

WHEN CYBERWEAPONS END UP ON PRIVATE NETWORKS: THIRD AMENDMENT IMPLICATIONS FOR CYBERSECURITY POLICY

ALAN BUTLER[*]

TABLE OF CONTENTS

[*] Appellate Advocacy Counsel, Electronic Privacy Information Center (EPIC); J.D. *UCLA School of Law*; B.A. *Washington University in St. Louis*. I would like to thank Nicolle Kownacki for her love, support, and superior editing on this piece; Julia Horwitz for extensive research assistance and editing; Pasha Sternberg for helping to hatch the concept and suggesting my participation in the *AULR* symposium; the editors at *AULR* for turning my draft into a finished product; and the staff at EPIC for supporting the research and writing involved.

INTRODUCTION

In the summer of 2010, Microsoft reported a new "zero-day" vulnerability[1] in Windows XP that allowed malicious software to be executed from USB drives.[2] Two months later, it was discovered that a sophisticated computer worm called "Stuxnet" had taken advantage of this vulnerability to infect industrial control systems within Iran's nuclear facilities.[3] Security researchers posited that Stuxnet was "created by a government and [wa]s a prime example of clandestine digital warfare."[4]

Although Stuxnet initially targeted specific Iranian nuclear facilities, its widespread infection left it "splattered on thousands of computer systems around the world,"[5] including Chevron's network.[6] Nearly two years after

[1] A zero-day is a security hole that the software developer is unaware of and has not had an opportunity to patch. *See* LEYLA BILGE & TUDOR DUMITRAS, BEFORE WE KNEW IT: AN EMPIRICAL STUDY OF ZERO-DAY ATTACKS IN THE REAL WORLD 1 (2012), *available at* http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf (explaining that there is practically no defense against such an attack); ADAM KLIARSKY, SANS INST., RESPONDING TO ZERO DAY THREATS 2–3 (2011), *available at* http://www.sans.org/reading_room/whitepapers/incident/responding-zero-day-threats_33709 (describing how zero-day threats have allowed hackers to take advantage of the vulnerabilities caused by organizations developing and employing new technologies and stating that the term zero-day refers to "the amount of time the community has to respond to a newly discovered and/or disclosed threat"). Zero-day exploits are now frequently sold to the highest bidder by the third parties who identify them, and, as a result, are being used to facilitate attacks rather than improve overall security. *See* Bruce Schneier, *The Vulnerabilities Market and the Future of Security*, FORBES (May 30, 2012, 12:43 PM), http://www.forbes.com/sites/bruce schneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security (concluding that the lucrative nature of selling zero-day exploits combined with the vulnerabilities remaining "secret and unpatched" attracts hackers to this path).

[2] Gregg Keizer, *Microsoft Confirms 'Nasty' Windows Zero-Day Bug*, REUTERS (July 17, 2010, 8:37 PM), http://www.reuters.com/article/2010/07/18/urnidgns852573c4 00693880002577630070b-idUS57900582720100718.

[3] *See* David E. Sanger, *Iran Fights Malware Attacking Computers*, N.Y. TIMES, Sept. 26, 2010, at 4, 14 (indicating that "[a] worm is a self-replicating malware computer program"); Riva Richmond, *Malware Hits Computerized Industrial Equipment*, N.Y. TIMES BITS BLOG (Sept. 24, 2010, 8:41 PM), http://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment (stating that Stuxnet was discovered by a Belarussian computer security firm).

[4] John Markoff, *A Silent Attack, but Not a Subtle One*, N.Y. TIMES, Sept. 27, 2010, at A6.

[5] *Id.*

Stuxnet was discovered, a New York Times exposé revealed that the United States and Israel had developed the worm as part of a project codenamed "Olympic Games."[7] This news clearly signaled the shift in cyberoperations from rogue groups to the nation-state level.[8] Representatives from the United States and other nations have begun discussing frameworks for analyzing cyberoperations under international law.[9] However, discussions of the constitutional limitations and the civil liberties implications of military cyberoperations have been limited.[10] Many recent articles have attempted to provide answers to how traditional legal principles governing military action will apply in cyberspace;[11] this Article is another along that vein.

[6] Rachael King, *Virus Aimed at Iran Infected Chevron's Network*, WALL ST. J., Nov. 9, 2012, at B1.

[7] *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1 (describing President Obama's adoption of the Bush-era "Olympic Games" program and his decision to accelerate the Stuxnet attack on Iran).

[8] *See* Misha Glenny, Op-Ed., *A Weapon We Can't Control*, N.Y. TIMES, June 25, 2012, at A19 (calling the joint effort by Israel and the United States to develop and deploy the Stuxnet worm a "significant and dangerous turning point in the gradual militarization of the Internet").

[9] *See, e.g.*, Harold Hongju Koh, Legal Advisor, U.S. Dep't of State, Remarks at the USCYBERCOM Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), *available at* http://www.state.gov/s/l/releases/remarks/197924.htm (addressing the Obama Administration's views on how international law applies in cyberspace and applying customary international law to argue for the right of national self-defense and proportionality in addressing cyberattacks); *see also* Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and* Tallinn Manual *Juxtaposed*, 54 HARV. INT'L. L.J. ONLINE 13 (2012) (discussing the differences between the U.S. views expressed by Professor Koh and those adopted by the International Group of Experts convened by the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE)). The *Tallinn Manual* is the result of a long-term cooperative effort by NATO to provide legal clarity in this area. INT'L GRP. OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 1, 3–4 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

[10] The domestic legal implications of cyber "counterstriking" were addressed in a recent article. Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 488–510 (2012). A few other articles have briefly addressed civil liberties issues in this context. *See, e.g.*, Sean M. Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 403, 416 (2007) ("The law must . . . adjust traditional understandings of the right to privacy, the right to protection against an unreasonable search, and the right to due process, given the practical necessity of responding to cyberattacks before determining the attacker's identity and intent." (footnotes omitted)); Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SEC. L. & POL'Y 155, 158 (2010) (advocating for additional congressional checks on the President's war powers as applied in cyberspace); John N. Greer, *Square Legal Pegs in Round Cyber Holes: The NSA, Lawfulness, and the Protection of Privacy Rights and Civil Liberties in Cyberspace*, 4 J. NAT'L SEC. L. & POL'Y 139, 143 (2010) (noting that "NSA lawyers need to be sure that the agency's IA [Information Assurance] computer monitoring operations are conducted in strict conformity with the . . . Fourth Amendment to the Constitution").

[11] *See, e.g.*, Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 526 (2012) (referring to cyberspace as a "new battleground for warfare" governed by unsettled laws but pointing to existing international instruments that govern the laws of war for guidance).

This Article takes a novel approach to cybersecurity policy by considering the implications of the Third Amendment of the U.S. Constitution.[12] While the Third Amendment's anti-quartering provision has been historically overlooked—in over two hundred years, very few federal cases have reviewed the provision at length[13]—it is the subject of a growing body of academic literature.[14] The Supreme Court has recognized that the Third

[12] "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." U.S. Const. amend. III.

[13] *See* Custer Cnty. Action Ass'n v. Garvey, 256 F.3d 1024, 1042–44 (10th Cir. 2001) (stating that "[j]udicial interpretation of the Third Amendment is nearly nonexistent" and rejecting as "border[ing] on frivolous" the petitioners' claim that military flights over their land constituted military occupation without consent in violation of the Third Amendment); Engblom v. Carey, 677 F.2d 957, 961–64 (2d. Cir. 1982) (noting "[t]he absence of any case law directly construing" the Third Amendment and holding that correctional officers had a Third Amendment right to exclude National Guardsmen from the officers' state-owned housing).

[14] *See, e.g.*, Tom W. Bell, *"Property" in the Constitution: The View from the Third Amendment*, 20 Wm. & Mary Bill Rts. J. 1243, 1245–46 (2012) [hereinafter Bell, *"Property" in the Constitution*] (contemplating the varying meanings of "property" in the Constitution and invoking the Third Amendment to argue that personal and real property merit the same protection under the Takings Clause); Tom W. Bell, *The Third Amendment: Forgotten but Not Gone*, 2 Wm. & Mary Bill Rts. J. 117, 117 (1993) [hereinafter Bell, *Forgotten but Not Gone*] (seeking to "fill the most glaring . . . gaps in Third Amendment scholarship"); William S. Fields & David T. Hardy, *The Third Amendment and the Issue of the Maintenance of Standing Armies: A Legal History*, 35 Am. J. Legal Hist. 393, 430 (1991) ("The third amendment, then, served as a broadly accepted basic right upon which a structure of newer, more enigmatic and controversial rights could ultimately be built."); Robert A. Gross, *Public and Private in the Third Amendment*, 26 Val. U. L. Rev. 215, 220 (1991) (defining the historical significance of the Third Amendment as "carv[ing] out a sharp distinction between public and private that is the hallmark of the modern capitalist, middle-class, social order"); Morton J. Horwitz, *Is the Third Amendment Obsolete?*, 26 Val. U. L. Rev. 209, 212 (1991) (pointing out "important struggles over the scope of the Third Amendment"); Andrew P. Morriss & Richard L. Stroup, *Quartering Species: The "Living Constitution," the Third Amendment, and the Endangered Species Act*, 30 Envtl. L. 769, 770–71 (2000) (analogizing the Endangered Species Act to the quartering provision of the Third Amendment); Nicholas Quinn Rosenkranz, *The Objects of the Constitution*, 63 Stan. L. Rev. 1005, 1028–33 (2011) (exploring the "object" of the Third Amendment and the role it plays in the Bill of Rights); Robert A. Rutland, *The Trivialization of the Bill of Rights: One Historian's View of How the Purposes of the First Ten Amendments Have Been Defiled*, 31 Wm. & Mary L. Rev. 287, 293–94 (1990) (calling for "an end to the trivialization of the Bill of Rights"); Christopher J. Schmidt, *Could a CIA or FBI Agent Be Quartered in Your House During a War on Terrorism, Iraq or North Korea?*, 48 St. Louis U. L.J. 587, 590 (2004) (examining the text of the Third Amendment to resolve the possibility of compelled quartering of CIA and FBI agents in connection with the U.S. fight against terrorism); Geoffrey M. Wyatt, *The Third Amendment in the Twenty-First Century: Military Recruiting on Private Campuses*, 40 New Eng. L. Rev. 113, 113–14, 123 (2005) (proposing the Third Amendment as the foundation for a successful attack against laws that require private universities to allow military recruiters on their campuses); Josh Dugan, Note, *When Is a Search Not a Search? When It's a Quarter: The Third Amendment, Originalism, and NSA Wiretapping*, 97 Geo. L.J. 555, 558 (2009) (calling for a modern and broader application of the Third Amendment by arguing that "the Founders used the word 'quartering' to expansively refer to a practical and substantial intrusion that threatened the legitimacy of government and the rule of law"); James P. Rogers, Note, *Third Amendment Protections in Domestic Disasters*, 17 Cornell J.L. & Pub. Pol'y 747, 750 (2008) (considering the "possibility that Third Amendment violations occurred in Louisiana or

Amendment creates a "zone of privacy" similar to those in the First and Fourth Amendments.[15] This zone of privacy protects individuals from military intrusions absent consent or special wartime legislative mandate.[16] Given the potential of military cyberoperations to intrude upon innocent domestic systems, as demonstrated by the Stuxnet example, the Third Amendment's constitutional prohibitions must be taken into account. This Article is intended to supplement existing discussions of cybersecurity policy while considering the principles of the Third Amendment in this new context. Because the history and purpose of the Third Amendment is discussed at length in other literature,[17] it will be summarized only briefly in this Article.

Part I discusses in detail recent cyberoperations and cyberstrategies that affect civilian networks and hardware. Part II addresses the structure and history of the Third Amendment and its relevance to the division between military and civilian realms. And Part III analyzes the effect of military cyberoperations on civilian devices—such as a server, network router, or personal computer—under the Third Amendment. Finally, Part IV discusses the implications of the Third Amendment's consent and wartime proscription requirements on the current cybersecurity policy debate.

This Article concludes that there are strict constitutional limitations to the cyberspace actions that the President can authorize, including in the recently-proposed cybersecurity Executive Order.[18] The President cannot authorize military actions in cyberspace that affect private domestic systems without the safeguards of congressional approval or a public-private partnership. These safeguards require increased public engagement in and knowledge of the decisionmaking process related to cyberoperations.[19]

Mississippi in the aftermath of Hurricane Katrina"); Thomas G. Sprankling, Note, *Does Five Equal Three? Reading the Takings Clause in Light of the Third Amendment's Protection of Houses*, 112 COLUM. L. REV. 112, 114 (2012) (arguing that "the Third Amendment provides a constitutional basis for distinguishing between homes and the other types of 'private property' covered by the Takings Clause").

[15] *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (explaining that various guarantees create a zone of privacy, including the right of association in the First Amendment, the prohibition against quartering "Soldier[s]" in the Third Amendment, and the right to be free from unreasonable searches in the Fourth Amendment).

[16] U.S. CONST. amend. III.

[17] For a review of the seventeenth century British common law on quartering, see Bell, *Forgotten but Not Gone*, *supra* note 14, at 118–24; Fields & Hardy, *supra* note 14, at 395–413; and Wyatt, *supra* note 14, at 125–29. For an in-depth discussion of the meaning at the time the Constitution was ratified, see Dugan, *supra* note 14, at 574–81.

[18] Exec. Order No. 13,636, 78 Fed. Reg. 11,737 (Feb. 19, 2013).

[19] *See, e.g.*, David E. Sanger & Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, N.Y. TIMES, Feb. 4, 2013, at A1 (describing a "secret legal review," conducted to assess President Obama's powers in relation to U.S. use of cyberweapons, which declared that President Obama "has the broad power to order a pre-emptive strike" if a threat is detected).

I. THE UNITED STATES AND OTHER NATIONS NOW HAVE AN ACTIVE MILITARY INVOLVEMENT IN CYBERSPACE

The United States is now actively engaged in military cyberoperations. The Secretary of Defense directed the U.S. Strategic Command to establish the U.S. Cyber Command (USCYBERCOM) on June 23, 2009.[20] This command center, located in Fort Meade, Maryland, became fully operational in October 2010.[21] USCYBERCOM is now focused on building additional capabilities for its "cyber warrior[s]."[22] This is necessary because, according to the Department of Defense's (DoD) most recent assessment, "cyber attacks will be a significant component of any future conflict."[23] Thus the DoD's strategy requires "[t]reating cyberspace as an operational domain like land, air, sea and space, operating and defending department networks and training and equipping forces for cyber missions."[24]

In his remarks on cybersecurity in the fall of 2012, Secretary of Defense Leon Panetta acknowledged that the DoD has the capability to conduct operations in response to cyberspace threats.[25] These efforts are certainly focused on combating the threat of what Secretary Panetta and others have described as "a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life."[26] However, the recent discovery of state-sponsored cyberattacks targeting Iran indicates that the United States is already involved in cyberoperations that stretch beyond its defensive boundary.[27] Given that these cyberoperations have already infected civilian

[20] *U.S. Cyber Command*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/cyber_command (last updated Dec. 2011).

[21] *Id*. The mission of USCYBERCOM is as 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.

Id.

[22] Donna Miles, *Cyber Command Builds 'Cyber Warrior' Capabilities*, U.S. DEP'T DEF. (Sept. 27, 2011), http://www.defense.gov/news/newsarticle.aspx?id=65459.

[23] Cheryl Pellerin, *DOD Releases First Strategy for Operating in Cyberspace*, U.S. DEP'T DEF. (July 14, 2011), http://www.defense.gov/news/newsarticle.aspx?id=64686.

[24] *Id.*; *see also* U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 934, at 1 (2011), *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf (detailing the DoD's strategic initiatives relating to cyberspace).

[25] Leon Panetta, U.S. Sec'y of Def., Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[26] *Id.*

[27] *See infra* Part I.A–B (describing the Stuxnet and Flame cyberattacks and suggesting that the United States participated).

infrastructure,[28] it is worth exploring the constitutional implications of the impact of military cyberoperations on civilian computers and networks.

Computer security researchers have recently uncovered several new cyberattacks and cyberoperations. Some of these attacks involve malware designed to alter the functions of industrial control systems that can cause physical damage.[29] Other attacks involve the use of sophisticated cyberespionage tools that can be controlled and deployed remotely.[30] Still other operations involve "hacking back" in response to an external cyberattack.[31] All of these cyberoperations have the potential to intrude upon and affect private civilian networks, which would implicate the Third Amendment.

A. Cyberattacks Targeted at Critical Infrastructure Typically Require Aggressive Self-Replication of a Computer Virus or Worm, Which Can Lead to Collateral Infection

At the time Stuxnet was discovered in mid-2010, it was one of the "most complex threats . . . [ever] analyzed."[32] Stuxnet is an example of a cyberattack that targets an industrial control system (ICS) used to manage critical infrastructure.[33] Such an attack requires multiple phases, exploits,[34] and infection vectors[35] in order to circumvent both physical and digital

[28] *See* King, *supra* note 6 (reporting that Stuxnet infiltrated American corporations' IT systems, including that of Chevron). Viruses and worms are two types of malware that can typically self-replicate, causing widespread infection. *What Is the Difference: Viruses, Worms, Trojans, and Bots?*, CISCO, http://www.cisco.com/web/ about/security/intelligence/virus-worm-diffs.html (last visited June 15, 2013).

[29] *See Incident Response Activity*, ICS-CERT MONITOR (Indus. Control Sys., Cyber Emergency Response Team, Wash., D.C.), Oct.–Dec. 2012, at 1–2, *available at* http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf (describing that an infected USB drive spread malware to approximately ten computers owned by a power plant, delaying plant operations for approximately three weeks).

[30] *See* Lee Ferran et al., *Flame Cyber Attack: Israel Behind Largest Cyber Spy Weapon Ever?*, ABC NEWS (May 29, 2012), http://abcnews.go.com/Blotter/flame-cyber-attack-israel-largest-cyber-spy-weapon/story?id=16449339 (explaining that Flame could receive remote commands to take screenshots, record audio and keystrokes, and perform other "sophisticated capabilities").

[31] *See* Hannah Lobel, Note, *Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict*, 47 TEX. INT'L L.J. 617, 633 (2012) ("[A]ctive defenses can go beyond simply warding off an attack with passive security measures like firewalls and instead involve actively attacking the attacker.").

[32] NICOLAS FALLIERE ET AL., SYMANTEC, W32.STUXNET DOSSIER 1 (2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/ whitepapers/w32_stuxnet_dossier.pdf.

[33] *See* Sanger, *supra* note 7 (describing that, specifically, the Stuxnet virus was used to target Iran's Natanz nuclear plant and it managed to disable "nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium").

[34] *See* JOHN ROLLINS & CLAY WILSON, CONG. RESEARCH SERV., RL33123, TERRORIST CAPABILITIES FOR CYBERATTACK: OVERVIEW AND POLICY ISSUES 18 (2007), *available at* http://www.fas.org/sgp/crs/terror/RL33123.pdf (defining zero-day exploits as "unknown computer vulnerabilities," which can be sold by hackers).

[35] An infection vector is a general term for the method used to place a virus on a

security measures.[36] In the case of Stuxnet, the self-executing virus was so aggressive in propagating itself that, by September 2010, it had infected more than 100,000 hosts, including thousands in the United States.[37]

The term ICS describes a broad range of systems used to control everything from power plants to gas pipelines.[38] These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and Programmable Logic Controllers (PLC).[39] The SCADA systems are necessary to control geographically dispersed equipment using centralized data, such as electrical grids or gas pipelines.[40] The DCS operates on a more localized scale, and the PLCs are the "computer-based solid-state devices" that ultimately control the industrial equipment.[41] Another critical component of any ICS is the Human-Machine Interface (HMI), which allows human operators to monitor and control the system configurations.[42]

The ultimate goal of a targeted ICS attack like Stuxnet is to "reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment."[43] The result would be to sabotage a high-value target by controlling specific industrial machines.[44] Achieving this goal would require intimate knowledge of the target network and ICS to configure the software; the infection of the target network by a third party; the spread and control of the virus throughout the network; and a self-executing function enabled by the virus when it reaches its final destination (disconnected from any command server).[45]

The first phase of such an operation requires extensive industrial

system. *See generally* Paul Schmehl, *Malware Infection Vectors: Past, Present, and Future*, http://www.symantec.com/connect/articles/malware-infection-vectors-past-present-and-future (last updated Nov. 2, 2010) (detailing the history of modern computer viruses by focusing on how they are spread).

[36] For example, the ICS targeted by Stuxnet would likely not have had direct Internet access, so the virus would have to be transported from the broader industrial network onto a specific computer used to control the ICS. FALLIERE ET AL., *supra* note 32, at 3.

[37] *Id.* at 5 & fig.1.

[38] NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, SPEC. PUB. NO. 800-82, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY 1-1 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

[39] *Id.*

[40] *Id.* at 2-1.

[41] *Id.*

[42] *Id.* at 2-4.

[43] FALLIERE ET AL., *supra* note 32, at 1. For more information on ICS, see generally Brendan Galloway & Gerhard P. Hancke, *Introduction to Industrial Control Networks*, IEEE: COMM. SURVS. & TUTORIALS 1 (2012).

[44] FALLIERE ET AL., *supra* note 32, at 3 (indicating that the final goal of Stuxnet was sabotaging ICSs).

[45] *See id.* (explaining the likely "attack scenario" for Stuxnet).

espionage, which is a common component of many cyberattacks.[46] The second and third phases, however, require rapid and aggressive expansion of the virus within a network, which can lead to widespread infection.[47] This can create a problem because "[o]nce self-replicating code is released, it's difficult to exercise complete control over where it goes, what it does, and how far it spreads"; in addition, once the public becomes aware of the virus, people are better able to protect themselves, and the virus's usefulness "in terms of payload delivery" is diminished.[48]

Stuxnet was capable of spreading so rapidly in part because it made use of a group of zero-day exploits within Microsoft Windows that allowed it to spread across the network using peer-to-peer connections, databases, and shared network drives.[49] It also used a key zero-day exploit, the "LNK Vulnerability," to copy itself to remote USB drives inserted into infected computers.[50] Stuxnet then infected other computers with those drives—eventually deleting itself and covering up the traces.[51] Stuxnet was also designed to connect to a remote server after infection; upload information about the infected system; and download any available patches, updates, or new instructions.[52]

Cyberattacks, like Stuxnet, used to target ICS are incredibly complex and include a variety of functions to inject themselves into critical systems. The same functions that can serve to spread the necessary viruses to ICS modules and target PLCs can also cause the viruses to become widely distributed over broader networks.[53] As a result, cyberattacks targeting industrial systems can become widespread on civilian networks.[54]

B. Other Offensive Cyberoperations Spread Throughout Targeted Networks To Gather Sensitive Information

Offensive cyberoperations include "actions taken against an adversary's

[46] *See infra* Part I.B (discussing the recently-discovered Red October and Flame malware packages).

[47] *See* ALEKSANDR MATROSOV ET AL., ESET, STUXNET UNDER THE MICROSCOPE 10 (2011), *available at* http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf (describing the propagation of malware as "promiscuous").

[48] *Id.*

[49] *See* FALLIERE ET AL., *supra* note 32, at 25–28 (describing the various ways that Stuxnet propagated).

[50] *Id.* at 29–30.

[51] *Id.*

[52] *Id.* at 21–23.

[53] Galloway & Hancke, *supra* note 43, at 16.

[54] Many scholars warn of attacks that have the secondary effect of attacking private sector networks. *See, e.g.*, Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 A.F. L. REV. 167, 170–71 (2012) (describing how an attack on DoD domains could jump to civilian networks because DoD networks are "largely reliant" on outside networks that "include national critical infrastructure").

computer systems or networks that harm the adversary's interests."[55] Many military cyberoperations are not intended to cause physical destruction.[56] For example, cyberexploitations are used to facilitate quiet and undetectable information-gathering.[57] These operations take advantage of the same vulnerabilities and access paths as targeted cyberattacks.[58] The viruses used in cyberexploits can infect computers and systems across the globe, and these viruses can remain dormant for years without detection.[59] Recently uncovered cyberexploitation attacks used sophisticated malware to gather troves of confidential data from a broad range of computers and devices.[60]

In May 2012, security firms uncovered a large and complex malware set referred to as "Flame," "Flamer," or "sKyWIper."[61] This program enables such a broad range of espionage functions that it has been referred to as the "Swiss-Army knife of cyberspying."[62] Security researchers eventually linked Flame with Stuxnet and other recently discovered programs through common code functions and the "Command and Control" (C&C) servers used to remotely configure and direct the attacks.[63] The same officials who

[55] Herbert Lin, *Escalation Dynamics and Conflict Termination in Cyberspace*, STRATEGIC STUD. Q., Fall 2012, at 46, 46, *available at* http://www.au.af.mil/au/ssq/2012/fall/lin.pdf.

[56] *See id.* at 48 (explaining that the intent of the cyberintruder varies).

[57] *Id.* at 48–49. As Dr. Lin describes, "*Cyber exploitation* is the use of deliberate IT-related actions—perhaps over an extended period of time—to support the goals and missions of the party conducting the exploitation, usually for the purpose of obtaining information resident on or transiting through an adversary's computer system or network." *Id.* at 48. These cyberexploitations are different than cyberattacks because the goal is to remain undetected and not to disrupt normal functions or user experiences. *Id.*; *see also* COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 12 box 1.1 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT] (listing the difference between cyberattacks and cyberexploits).

[58] Lin, *supra* note 55, at 48.

[59] *See Next-Generation Threats*, FIREEYE, http://www.fireeye.com/threat-protection (last visited June 15, 2013) (proposing that "advanced malware" is usually successful because "few technologies monitor outbound malware transmissions").

[60] NRC REPORT, *supra* note 57, at 85.

[61] *See* LAB. OF CRYPTOGRAPHY & SYS. SEC., BUDAPEST UNIV. OF TECH. & ECON., SKYWIPER (A.K.A. FLAME A.K.A. FLAMER): A COMPLEX MALWARE FOR TARGETED ATTACKS 2 (2012) [hereinafter SKYWIPER], *available at* http://www.crysys.hu/skywiper/skywiper.pdf (investigating a then-unknown malware and revealing that the malware impacted several countries); *Identification of a New Targeted Cyber-Attack*, IRAN NAT'L COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CTR. (May 28, 2012), http://www.certcc.ir/index.php?name=news&file=article&sid=1894 (announcing the detection of Flame and development of removal tools).

[62] Andy Greenberg, *To Spy on Offline Computers, Flame Malware Was Designed To Turn Humans into 'Data Mules,'* FORBES (June 12, 2012, 9:30 AM), http://www.forbes.com/sites/andygreenberg/2012/06/12/to-spy-on-offline-computers-flame-malware-was-designed-to-turn-humans-into-data-mules.

[63] *Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers Are Connected*, KASPERSKY LAB (June 11, 2012), http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected (acknowledging the existence of evidence demonstrating that the same

acknowledged U.S. involvement in the Stuxnet attack declined to confirm whether the United States was also the source of Flame.[64] Attribution of a cyberattack, especially a clandestine exploitation focused on espionage, is very difficult due to the limited information available.[65]

Regardless of the source of these attacks, Flame and other related programs[66] reveal the capacities to capture credentials, communications, audio, video, and a wide range of other sensitive data from a broad range of devices and networks.[67] The attack vector used by Flame is especially troubling because it relies upon a vulnerability in the digital certificates that everyday computers depended on to guarantee secure updates for Microsoft Windows.[68] The Flame toolkit is relatively large compared to other malware, which allows it to be incredibly versatile and gives the remote

team that developed Stuxnet also designed Flame); *see* Kim Zetter, *Researchers Connect Flame to US-Israel Stuxnet Attack*, Wired: Threat Level (June 11, 2012, 9:30 AM), http://www.wired.com/threatlevel/2012/06/flame-tied-to-stuxnet (reporting the "discover[y] that a part of the module that allows Flame to spread via USB sticks using the autorun function on a Windows machine contains the same code that was used in a version of Stuxnet"); *New Investigation Points to Three New Flame-related Malicious Programs: At Least One Still in the Wild*, Kaspersky Lab (Sept. 17, 2012), http://www.kaspersky.com/about/news/virus/2012/New_investigation_points_to_three_new_Flame_related_malicious_programs_at_least_one_still_in_the_wild (unveiling the results of a follow-up study that revealed that the development of Flame began as early as 2006).

[64] Sanger, *supra* note 7.

[65] *See* Lin, *supra* note 55, at 49–50 (describing the difficulties associated with both "technical" and "all source" attribution, including lack of forensic clues, unknown motivations, and the intruder's operational security); *see also* David E. Sanger, *Mutually Assured Cyberdestruction?*, N.Y. Times, June 3, 2012, at SR4 (ascribing the difficulty in deterring cyberattacks to the complexity involved in discovering where attacks originated).

[66] *See* Global Research & Analysis Team, Kaspersky Lab, Gauss: Abnormal Distribution 3 (2012) [hereinafter Kaspersky, Gauss], *available at* http://www.securelist.com/en/downloads/vlpdfs/kaspersky-lab-gauss.pdf (explaining Gauss, a malware discovered primarily in Lebanon); Global Research & Analysis Team, Kaspersky Lab, *miniFlame aka SPE: "Elvis and His Friends*,*"* Securelist (Oct. 15, 2012), http://www.securelist.com/en/analysis/204792247/miniFlame_aka_SPE_Elvis_and_his_friends [hereinafter Kaspersky, *miniFlame*] (discussing miniFlame, a smaller module connected to the same C&C servers as Flame).

[67] *See* Ferran et al., *supra* note 30 (referring to Flame as "a veritable 'toolkit' of cyber spying programs"). *See generally* sKyWIper, *supra* note 61, at 2 (characterizing sKyWIper as "complex with a large number of components" including numerous compression and encryption techniques).

[68] Chester Wisniewski, *Flame Malware Used Man-in-the-Middle Attack Against Windows Update*, Naked Sec., Sophos (June 4, 2012), http://nakedsecurity.sophos.com/2012/06/04/flame-malware-used-man-in-the-middle-attack-against-windows-update. This vulnerability depended on the discovery of a rare "MD5 hash collision" that could be used to sign a digital certificate. Richard Stiennon, *Flame's MD5 Collision Is the Most Worrisome Security Discovery of 2012*, Forbes (June 14, 2012, 6:45 AM), http://www.forbes.com/sites/richardstiennon/2012/06/14/flames-md5-collision-is-the-most-worrisome-security-discovery-of-2012; *see* Alexander Sotirov et al., *MD5 Considered Harmful Today: Creating a Rogue CA Certificate*, HashClash Project, http://www.win.tue.nl/hashclash/rogue-ca (last modified June 16, 2011) (identifying a vulnerability and providing a proof-of-concept attack that takes advantage of a weakness in the MD5 cryptographic hash algorithm to forge digital certificates).

operators a great deal of control over its actions.[69]

This modular structure and its tiered approach to infection are the prominent features of the Flame-related cyberexploits.[70] Forensic analysis of the servers controlling Flame uncovered at least three other cyberespionage or cybersabotage tools that the same author created and controlled.[71] These different tools are able to interact and coordinate; some modules can relay stolen data to the C&C servers while others infect removable drives and report back once data has been collected from remote devices.[72]

It appears that the hierarchical control structure of Flame helped to prevent the widespread infection problem that Stuxnet suffered.[73] Flame even included a "kill switch" command, which was sent within a week of its initial discovery.[74] This command from the C&C servers orders the deletion of the majority of files and folders used by the malware.[75] The C&C servers then remove any trace that the files and folders ever existed.[76] Due to this "suicide" functionality, it is impossible to know the total number of Flame-related infections, but forensic research on the C&C servers indicates that these programs were focused primarily on targets in Iran, Lebanon, Sudan, and a few other countries in the Middle East.[77] All three of the Flame-related programs analyzed by the Global Research and Analysis Team at the Kaspersky Lab included infections from IP addresses

[69] *See* Alexander Gostev, *The Flame: Questions and Answers*, SECURELIST (May 28, 2012), http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers (asserting that "Flame is one of the most complex threats ever discovered" partially because of its large size, complex algorithms, and scripting programming language); Neil Roiter, *Flame Is the Mother of All Spyware, but While It May Raise the Stakes, It Doesn't Change the Game*, SEC. BISTRO (May 29, 2012), http://www.securitybistro.com/blog/?p=1605 (contrasting Flame with other spyware such as Stuxnet and noting that although Flame has similar functionality, it is relatively "huge and highly versatile" by comparison).

[70] Gostev, *supra* note 69.

[71] Kaspersky, *miniFlame*, *supra* note 66.

[72] *Id.*

[73] *See* Symantec Sec. Response, *Flamer: Urgent Suicide*, SYMANTEC, http://www.symantec.com/connect/blogs/flamer-urgent-suicide (last updated June 6, 2012) (explaining that the Flamer control servers sent updated commands "designed to completely remove Flamer from the compromised computer," thereby halting the infection from spreading more).

[74] *See* John Naughton, *How Flame Virus Has Changed Everything for Online Security Firms*, GUARDIAN (June 16, 2012), http://www.guardian.co.uk/technology/2012/jun/17/flame-virus-online-security (questioning whether the writers of Flame would ever be discovered because the "kill switch" had been activated to remove all traces of the malware); Symantec Sec. Response, *supra* note 73 (referring to this command as the "uninstaller").

[75] Symantec Sec. Response, *supra* note 73.

[76] *Id.*

[77] *See* Kaspersky, *miniFlame*, *supra* note 66 (distinguishing miniFlame as not having a "geographical bias" compared to Flame, which was mostly found in Iran and Sudan, and Gauss, which had a majority of its infections recorded in Lebanon).

traced to the United States.[78]

Simple spyware has been used for more than two decades to collect and send private data over the Internet, and more advanced cyberespionage tools have been constantly evolving over that same period.[79] However, it appears that sophisticated C&C modules are now being deployed on a global scale.[80] In fact, in early 2013, researchers uncovered a new campaign referred to as "Red October," which contains intricacies in its infrastructure that rival those found in the Flame malware.[81] Red October currently remains active and dates "as far back as May 2007."[82] It is unclear whether this new attack is the work of a nation-state, but its victims include government agencies, diplomats, research institutions, and major industrial sectors.[83] The Red October attack demonstrates that it is highly unlikely that cyberspying has yet reached its peak, and there are no indications that it will end any time soon.

[78] *See* KASPERSKY, GAUSS, *supra* note 66, at 5–6 (elaborating that forty-three infected IPs were linked to the United States but articulating Kaspersky's belief that "in the majority of cases linked to the USA and Germany the affected users were actually in the Middle East too—using VPNs (or the Tor anonymity network)"); Kaspersky, *miniFlame*, *supra* note 66 (showing that the distribution of victims' IPs infected with miniFlame includes nearly ten from the United States); *see also* Global Research & Analysis Team, Kaspersky Lab, *Full Analysis of Flame's Command & Control Servers*, SECURELIST (Sept. 17, 2012, 1:00 PM), http://www.securelist.com/en/blog/750/Full_Analysis_of_Flame_s_Command_Control_servers (detailing that during a one-week period, sixty-eight IPs in the United States connected to one Flame server).

[79] *See* CTR. FOR SEC. & PRIVACY SOLUTIONS, DELOITTE, CYBER ESPIONAGE: THE HARSH REALITY OF ADVANCED SECURITY THREATS (2011), *available at* http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_sp_cyber_espionage_screen_friendly_100511.pdf (describing ongoing cyberthreats as evolving and recommending that organizations similarly evolve to include proactive protection and monitoring).

[80] *See* Benjamin Cruz, *Botnet Control Servers Span the Globe*, MCAFEE LABS (Jan. 23, 2013, 4:17 PM), http://blogs.mcafee.com/mcafee-labs/botnet-control-servers-span-the-globe (revealing that the majority of the C&C servers monitored were located in the United States); *see also* Matt Vasilogambros, *America's 3 Biggest Cybersecurity Vulnerabilities*, NAT'L J. (Mar. 13, 2013, 4:00 PM), http://www.nationaljournal.com/whitehouse/america-s-3-biggest-cybersecurity-vunerabilities-20130313 ("The Obama administration has put cyberattacks at the top of the list of global threats, and concerns are rising about at-risk infrastructure.").

[81] Global Research & Analysis Team, Kaspersky Lab, *The "Red October" Campaign—An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies*, SECURELIST (Jan. 14, 2013, 1:00 PM), http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies.

[82] *Id.*

[83] *See id.* (asserting that while infections are mostly distributed in Eastern Europe, reports are coming from Switzerland and Luxembourg, as well as North America). The victims are classified into eight main categories: government; research/embassies; research institutions; trade and commerce; nuclear/energy research; oil and gas companies; aerospace; military. *Id.*

C. Active Defense Countermeasures Also Include Offensive Capabilities That Can Affect Innocent Third-Party Systems

While the United States may be engaged in certain limited cyberoperations, the primary focus of the DoD is currently on ensuring the safety of government networks and critical infrastructure.[84] This effort is being coordinated by the USCYBERCOM, which operates in conjunction with the National Security Agency (NSA).[85] These defense components are still in the process of developing and implementing a comprehensive strategy to address current cyberthreats.[86]

One strategy that has been discussed for more than fifteen years[87] is "active defense" and the use of cyber "counterstrikes."[88] Active defense involves a three-step process: "(1) detecting an intrusion, (2) tracing the intruder, and (3) some form of cyber counterstrike."[89] The primary goal of an active defense system is deterrence.[90] This can be achieved through retribution after the fact or mitigation at the time of attack.[91] Retaliatory counterstrikes are still very controversial and many have questioned their

[84] *See* U.S DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 1, 5 (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf (listing the DoD's need to "[m]anage cyberspace risk through efforts such as increased training," and to "[e]nsure the development of integrated capabilities . . . to rapidly deliver and deploy innovative capabilities" as reasons to establish USCYBERCOM).

[85] *See id.* at 5 (indicating that the United States Strategic Command (USSTRATCOM) charged USCYBERCOM with coordinating cyberservice components within all military cybercommands).

[86] *See id.* at 6 (outlining the five initiatives comprising the DoD's strategic development for responding to cyberthreats and for operating in cyberspace); Sanger & Shanker, *supra* note 19 (disclosing that in February 2013, Congress was in the process of promulgating new, classified policies on how the United States can defend against cyberattacks).

[87] *See, e.g.*, DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 392–93 (1999) (identifying an in-kind response as a type of offensive strategy used to retaliate against cyberattacks); Deborah Radcliff, *Can You Hack Back?*, CNN (June 1, 2000, 10:30 AM), http://edition.cnn.com/2000/TECH/computing/06/01/hack.back.idg (discussing the complexity of retaliation in cyberspace). Security researcher Dave Dittrich has compiled a list of resources dating back to 1998 related to the "active response continuum." *Articles/Papers/Audio Related to the Active Response Continuum*, UNIV. OF WASH., http://staff.washington.edu/dittrich/activedefense.html (last updated Jan. 8, 2013, 2:25 PM).

[88] Kesan & Hayes, *supra* note 10, at 433.

[89] *Id.* (citing Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense*, 38 STAN. J. INT'L L. 207, 231 (2002); Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 182 (2005)).

[90] *Id.* at 420; *see also* U.S. ARMY TRAINING & DOCTRINE COMMAND, U.S. DEP'T OF THE ARMY, THE UNITED STATES ARMY CONCEPT CAPABILITY PLAN FOR ARMY ELECTRONIC WARFARE OPERATIONS FOR THE FUTURE MODULAR FORCE 2015–2024, at 9 (Aug. 16, 2007), *available at* http://www.tradoc.army.mil/tpubs/pams/p525-7-6.pdf (defining "deterrence" as a maneuver to "convince adversaries not to take actions that threaten U.S. vital interests by means of decisive influence over their decisionmaking," which is achieved through credible threats "to deny benefits . . . or impose costs, while encouraging restraint by convincing the adversary that restraint will result in an acceptable outcome").

[91] Kesan & Hayes, *supra* note 10, at 420.

legal basis under domestic and international law.[92]

The components of an active defense strategy have already been outlined at length in a number of prominent reports and articles.[93] The critical first steps involve detecting an attack and tracing it back to its source.[94] Computer security firms have already developed advanced Intrusion Detection Systems (IDS) that can take the first step.[95] The traceback step is more difficult, but there have been significant recent advances in traceback technology.[96] Still, many reject the idea that cyberattacks can be accurately attributed using current technical methods.[97]

[92] *Id.* at 421; *see, e.g.*, Susan Brenner, *Offensive Economic Espionage?*, 54 HARV. INT'L L.J. ONLINE 92, 99 (2012) (articulating that because the current government system is not effective in combating cyberattacks, the private sector will offer increasing offensive protection measures that may escalate to "online vigilantism" if it continues without regulation); Katharine C. Hinkle, Essay, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. ONLINE 11, 11–12 (2011) (addressing the growing debate about which international law applies to cyberattacks and what acts constitute an "armed attack" under the law); *see also* Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 83 (2009) (describing active defenses as a "new frontier" that will be controversial in any situation).

[93] *See, e.g.*, NRC REPORT, *supra* note 57, at 16 (explaining the potential for an active defense to be construed as an offensive attack through hypotheticals involving two imaginary nations); Condron, *supra* note 10, at 410–11 (advancing that active defense measures typically utilize an in-kind response, where the attacked party will instigate an offensive attack on the perpetrator using a similar strategy to what was used against them); 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, 177–78 (2009) (addressing the military's use of cyberspace in both offensive and defensive roles and discussing the need to manage the availability of access to cyberspace for conducting operations); Kesan & Hayes, *supra* note 10, at 460–73 (arguing that passive methods are ineffective in addressing cyberattacks, that active defense is the most effective response in some circumstances, and that, to effectuate such a response, more advanced technologies and policy guidelines are needed); Sklerov, *supra* note 92, at 25 (assessing the specifics of how active computer attack measures can function by detailing the transmission of a virus that disrupts the attacking hacker's machine).

[94] Kesan & Hayes, *supra* note 10, at 467–69.

[95] *See* Karen Kent Frederick, *Network Intrusion Detection Signatures, Part One*, SYMANTEC, http://www.symantec.com/connect/articles/network-intrusion-detection-signatures-part-one (last updated Nov. 3, 2010) (detailing that an IDS signature could be configured to detect "abnormal or suspicious traffic in general, not just attacks and probes").

[96] *See* Ethan Katz-Bassett et al., *Reverse Traceroute*, *in* PROCEEDINGS OF NSDI '10: 7TH USENIX SYMPOSIUM ON NETWORKED SYSTEMS DESIGN AND IMPLEMENTATION 219, 230 (2010), *available at* http://static.usenix.org/events/nsdi10/tech/full_papers/nsdi10_proceedings.pdf (elaborating on the creation of a better "reverse traceroute" system).

[97] *See* NRC REPORT, *supra* note 57, at 37 (warning that the technical difficulties of attribution create a danger that a third party will be wrongfully targeted during a counterattack); Condron, *supra* note 10, at 417 (asserting that while it may be possible to easily attribute the source of a cyberattack to a computer system, it is oftentimes difficult to attribute the fault to the specific person behind the attack because hackers often route attacks through innocent third-party systems); Kesan & Hayes, *supra* note 10, at 464–65 (insisting that technological advancements are necessary to facilitate more precise attribution and thereby ensure more accurate counterattacks).

The counterstrike phase of active defense is most relevant for the purposes of the Third Amendment analysis. Any counterstrike will necessarily impose risk of harm to innocent third parties, including domestic companies and individuals, as has been discussed extensively in self-help literature about cybersecurity.[98] This is due, in part, to the difficulty of attributing attacks to a specific source.[99] Any attribution errors in a U.S. counterstrike could thus result in harm to or intrusion of domestic systems.

While current military cyberstrike capabilities remain classified, there are already public sector security systems that implement hack-back capabilities.[100] One possibility, described in a post by Stewart Baker, is a system that can "stake out the victim's system, ready to give the attacker bad files, to monitor the command and control machine, and to copy, corrupt, or modify ex-filtrated material."[101] One problem with such a system, as Baker acknowledges, occurs when the attacker "is using a cutout—an intermediate command and control computer that actually belongs to someone else."[102] Collecting from or sending files to an intermediate computer could violate an innocent party's privacy.[103] This *theoretical* privacy invasion is much more significant than Baker is willing to admit, and the legal consequences of hacking back could be substantial.[104]

[98] *See* Jensen, *supra* note 89, at 237 (emphasizing the risk of destruction to systems of neutral third-party nations in using an active computer network defense response); Neal Katyal, *Community Self-Help*, 1 J.L. ECON. & POL'Y 33, 60–67 (2005) (advocating for a more community-based preventative approach to cyberattacks due to the severe risks and repercussions involved with counterattacks); Smith, *supra* note 89, at 183 (analogizing modern cybercounterattacks to excessive old English landowner self-help measures, such as a loaded spring gun set up to deter illegal intruders); Eugene Volokh, *The Rhetoric of Opposition to Self-Help*, VOLOKH CONSPIRACY (Apr. 11, 2007, 3:22 PM), http://www.volokh.com/posts/1176319370.shtml (summarizing the most common arguments against counterattacks).

[99] *See supra* note 97 and accompanying text.

[100] For example, ForeScout's "ActiveResponse" technology is capable of performing "perimeter defense" and actively identifying and blocking attackers. Jensen, *supra* note 89, at 230.

[101] Stewart Baker, *RATs and Poison: Can Cyberespionage Victims Counterhack?*, VOLOKH CONSPIRACY (Oct. 13, 2012, 8:05 PM), http://www.volokh.com/2012/10/15/the-legal-case-against-hack-back-a-response-to-stewart-baker. Baker describes this system as "RAT poison" because tools frequently used in cyberattacks are known as Remote Access Tools (RATs). *Id.*

[102] *Id.*

[103] *Id.*

[104] *See* Orin Kerr, *The Legal Case Against Hack-Back: A Response to Stewart Baker*, VOLOKH CONSPIRACY (Oct. 15, 2012, 5:41 PM), http://www.volokh.com/2012/10/15/the-legal-case-against-hack-back-a-response-to-stewart-baker (arguing that the Computer Fraud and Abuse Act (CFAA) unambiguously prohibits *all* hacking, including hacking back, and that authorizing such counterattacks is ill-advised given the difficulty in locating the source of an attack).

The threats posed by hack-backs are so significant that, according to security experts, hacking back "is one of those things that's not even up for discussion as far as security is concerned" and is "one thing you don't do."[105] This is because accurate attribution of an attack is "close to impossible."[106] Inaccurate attribution could occur, for example, where a malicious hacker uses an intermediate "zombie" system to carry out an attack.[107] A defensive system that hacks back could "strike" the apparent source of the attack, but it would actually be harming an innocent third-party system.[108]

These hack-back tactics pose distinct threats to innocent third parties, including those within the United States. As some commentators have already discussed, an active cyberdefense operation by the U.S. military against citizens might infringe civil liberties, including rights conferred by the Fourth Amendment Search and Seizure Clause, the Fifth Amendment Due Process and Takings Clauses, and the Posse Comitatus Act.[109] This Article is meant to supplement that analysis by considering the Third Amendment implications of hack-backs, cyberattacks, and cyberexploitations.

II. THE THIRD AMENDMENT AND THE CIVILIAN-MILITARY DIVIDE

The Third Amendment to the U.S. Constitution states: "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."[110] While the full scope of Third Amendment protection has not been clearly defined,[111] its text and its history throughout the revolutionary period are

[105] Michael Mimoso, *Avoid the Landmine That Is Hacking Back*, THREATPOST, KASPERSKY LAB SECURITY NEWS SERVICE (Jan. 22, 2013, 11:45 AM), http://threatost.com /en_us/blogs/avoid-landmine-hacking-back-012213.

[106] *Id.* (noting that hacking back also violates the CFAA to the same extent that the original attack did).

[107] *See* Kesan & Hayes, *supra* note 10, at 442, 538–39 (describing the use of "zombies" for Distributed Denial of Service (DDoS) attacks and noting the potential effects of a counterstrike on such innocent systems).

[108] *Id.* at 539.

[109] 18 U.S.C. § 1385 (2006); *see, e.g.*, Condron, *supra* note 10, at 416–21 (explaining due process and Posse Comitatus Act implications); Kesan & Hayes, *supra* note 10, at 520–24, 452–55 (discussing statutory protections under the Electronic Communications Privacy Act (ECPA), the CFAA, the Computer Security Act of 1987, and the Posse Comitatus Act, as well as constitutional protections under the Fourth Amendment, the War Powers Clause, the Due Process Clause, and the Takings Clause). The Posse Comitatus Act prohibits the use of military personnel to enforce domestic laws absent express constitutional or congressional authorization. 18 U.S.C. § 1385; *see also id.* § 375 (requiring that the Secretary of Defense proscribe regulations to ensure that no military member participate in "search, seizure, arrest, or other similar activity unless . . . otherwise authorized").

[110] U.S. CONST. amend. III.

[111] The Second Circuit noted at the outset in its Third Amendment analysis in *Engblom v. Carey*, 677 F.2d 957 (2d Cir. 1982), that "[t]he absence of any case law directly construing this provision presents a serious interpretive problem, and little illumination can be gleaned from the

sufficient to guide its modern application.[112] At its core, the anti-quartering provision draws a clear line between private and public domains.[113] It protects individuals from the harms associated with military occupation, especially during peacetime.[114] It also strengthens common law property rights by creating an absolute bar to military quartering under certain circumstances.[115] What remains uncertain is how far those protections extend in a modern context where an expansive military and evolving private spaces overlap more than any other time in history.

A. Third Amendment Basics

There are three primary sources of Third Amendment law: the text of the amendment itself,[116] federal and state cases published since its adoption,[117] and English common law prior to its adoption.[118] A review of these sources will aid application of the Third Amendment's key terms: "quartered," "Soldier," and "any house."[119] In its simplest form, the Third Amendment prohibits quartering troops in a home during peacetime

debates of the Constitutional Convention." *Id.* at 962.

[112] For a thorough analysis of the history of the Third Amendment, see Fields & Hardy, *supra* note 14. There are also a number of articles focused on analyzing the Third Amendment from a historical perspective. *See generally* Bell, *"Property" in the Constitution*, *supra* note 14; Bell, *Forgotten but Not Gone*, *supra* note 14; Gross, *supra* note 14; Schmidt, *supra* note 14; Wyatt, *supra* note 14.

[113] Gross, *supra* note 14, at 219; *see also* Padilla v. Rumsfeld, 352 F.3d 695, 714–15 (2d Cir. 2003) ("[T]he Third Amendment's prohibition on the quartering of troops during times of peace reflected the Framers' deep-seated beliefs about the sanctity of the home and the need to prevent military intrusion into civilian life."), *rev'd on other grounds*, 542 U.S. 426 (2004).

[114] *See Padilla*, 352 F.3d at 714–15 (noting that the Framers prohibited military intrusions during times of peace based on their "deep-seated beliefs about the sanctity of the home," but recognized that military needs could prevail during times of war).

[115] *See* Bell, *Forgotten but Not Gone*, *supra* note 14, at 121 & n.28 (demonstrating that the Third Amendment stemmed from a need to protect property rights); *see also Engblom*, 677 F.2d at 962 (rejecting the literal reading of the Third Amendment to apply solely to citizens who possess a fee simple ownership in their house and instead assessing other privacy interests found in the Constitution to comparatively interpret the Third Amendment).

[116] U.S. CONST. amend. III.

[117] *See, e.g.*, *Padilla*, 352 F.3d at 714–15 (finding that despite the Founders' deeply-rooted beliefs against quartering, they provided for congressionally approved war-time quartering based on military necessity); *Engblom*, 677 F.2d at 964 (ruling that the eviction of correctional officers during a statewide strike and subsequent quartering of New York State National Guardsmen in their state-provided homes could constitute a violation of the Third Amendment); Fluke v. Canton, 123 P. 1049, 1053–54 31 (Okla. 1912) (discussing the English roots of the anti-quartering right and noting that its nearly universal inclusion in state constitutions "demonstrates the continued jealousy of the American people against the encroachment by the military against civil authority").

[118] *See* Fields & Hardy, *supra* note 14 (detailing the rich history and development of anti-quartering provisions in pre-revolutionary England); *infra* notes 124–28 and accompanying text.

[119] U.S. CONST. amend. III.

without the consent of the "Owner."[120]

From this basic structure, a review of any Third Amendment issue will analyze the nature of the imposition (quartering), upon some private property (any house), by a military element (Soldier).[121] The Amendment only permits quartering activity by either consent—in time of peace—or a manner prescribed by law—in time of war.[122] Adding to the complexity, the Amendment and the jurisprudence lack a clear rule to apply during times that could rightly be described as in between peace and war.[123]

The richest history and development of the anti-quartering provision occurred in pre-revolutionary England.[124] At the time when Congress passed the Bill of Rights, the Third Amendment's "roots were grounded in the common law so thoroughly that Blackstone was able to state with clarity, that '. . . the petition of right enacts, that no soldier shall be quartered on the subject without his own consent.'"[125] Given its long history, English courts had numerous opportunities to interpret the scope of the anti-quartering provision before it was incorporated into the Third Amendment.[126] These courts held that the term "houses" applies to both private homes and buildings kept as inns.[127] Additionally, the courts also held that provisions related to the quartering of "Soldiers" were sufficiently

[120] *Id.*; *see* Gross, *supra* note 14, at 217 (stating that the fundamental principle that quartering in homes is not allowed without consent stemmed from seventh century British Parliament).

[121] *See, e.g.*, *Engblom*, 677 F.2d at 961–62.

[122] U.S. CONST. amend. III.

[123] *See Engblom*, 677 F.2d at 961–62 (failing to discuss or establish a bright-line rule for interpreting the Third Amendment in times in between peace and war); Schmidt, *supra* note 14, at 616 (suggesting that compelling the quartering of soldiers without a clear declaration of war would implicate due process concerns).

[124] *See* Fields & Hardy, *supra* note 14, at 404–05, 411–12 (relating the "quartering problem" back to the time of King Charles I and advancing that the anti-quartering provision stemmed from the larger "individual rights" movement).

[125] *Id.* at 411. The protection from involuntary quartering was included in the Declaration of Rights enacted as the Bill of Rights by the English Parliament in 1689. *Id.* at 405. It was "drafted, not to introduce new principles of law, but merely as a recital of the existing rights of Parliament and the subject, which [King] James had outraged, and which [King] William must promise to observe." *Id.* (quoting G.M. TREVELYAN, THE ENGLISH REVOLUTION, 1688–1689, at 179–90 (1979)).

[126] *See* Bell, *Forgotten but Not Gone*, *supra* note 14, at 117–29 (analyzing the origins of the Third Amendment from its European roots to its entry into American constitutional law); Fields & Hardy, *supra* note 14, at 394–95 (providing a detailed history of the rise in legislation prohibiting the quartering of soldiers in times of peace and asserting that the right against involuntary quartering was deeply embedded in English common law before the American Revolution); Wyatt, *supra* note 14, at 124–33 (discussing history of English cases on soldier quartering provisions).

[127] *See, e.g.*, Parker v. Flint, (1780) 88 Eng. Rep. 1303 (K.B.) 1303; 12 Mod. 254, 254–55. The court held that a superseding war-time statute allowing constables to quarter soldiers upon innkeepers should be "construed favourably without great necessity" and that the building at issue did not count as an inn. *Id.* As a result, the constable who attempted to quarter a dragoon and horse upon the (non-qualifying) inn was guilty of trespass. *Id.*

broad as to also implicate the quartering of soldiers' horses.[128]

Various federal and state courts have made passing references to the Third Amendment, but to date only the U.S. Court of Appeals for the Second Circuit has conducted an in-depth analysis of its application. In *Engblom v. Carey*,[129] correction officers at the Mid-Orange Correctional Facility in New York brought an action against the Governor and other state officials for violations of their Third Amendment and due process rights.[130] The plaintiffs were evicted from their facility-residences during a statewide strike of correction officers, and members of the National Guard were housed there without the consent of the correctional officers.[131] The Second Circuit ruled in favor of the correction officers at the summary judgment stage and made three key Third Amendment holdings: first, that the Third Amendment was incorporated for application to the states under the Fourteenth Amendment;[132] second, that under the Third Amendment, National Guardsmen qualified as "Soldiers";[133] and third, that the plaintiff-tenants were "Owner[s]" of their residences, which qualified as a "house" for the purposes of the Third Amendment.[134]

B. Implications of Third Amendment History

The boundaries of the Third Amendment can be better understood in light of the history of its adoption and application throughout America and England during the pre-revolutionary period.[135] The anti-quartering provision was first adopted in England in response to the growing concern over standing armies maintained by the King.[136] The doctrine then evolved to incorporate principles of control over private property and compensation for government impositions.[137] The quartering of troops in pre-

[128] *See, e.g.*, Read v. Willan, (1780) 99 Eng. Rep. 271 (K.B.) 273; 2 Dougl. 422, 426.

[129] 677 F.3d 957 (2d Cir. 2003).

[130] *Id.* at 958.

[131] *Id.* at 958–59.

[132] *Id.* at 961.

[133] *Id.*

[134] *Id.* at 962–64.

[135] The history of this period relevant to the adoption of the Third Amendment is covered extensively in prior literature, so this section only provides a brief summary of relevant portions. For a more in depth review of the history, see Bell, *Forgotten but Not Gone*, *supra* note 14; and Fields & Hardy, *supra* note 14.

[136] *See* Bell, *Forgotten but Not Gone*, *supra* note 14, at 123–24 (discussing the role that the English common law played in the development of the Third Amendment and the historical circumstances from which it arose).

[137] According to Justice Story:

> [The Third Amendment] speaks for itself. Its plain object is to secure the perfect enjoyment of that great right of the common law, that a man's house shall be his own castle, privileged against all civil and military intrusion. The billeting of soldiers in time of peace upon the people has been a common resort of arbitrary princes, and is full of inconvenience and peril.

3 JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES § 1893, at

revolutionary America was considered an unbearable imposition and was cited as a key grievance by the colonists.[138]

The problems presented by the presence of soldiers among the civilian population are "as old as antiquity,"[139] but the quartering problem came into special focus during the seventeenth century upheavals in England.[140] The source of this civilian grievance was inextricably linked with the political issue of the use and maintenance of standing armies.[141] Trouble between soldiers and the civilian population continued to be an issue and resulted in the addition of an anti-quartering right in the 1689 Declaration of Rights.[142]

The Third Amendment was derived from the same anti-quartering sentiment that arose in seventeenth century England following the civil war and the Third Anglo-Dutch War.[143] The 1679 Anti-Quartering Act[144] protected British citizens from military intrusion for more than a hundred years before the law changed for the colonists. During the pre-revolutionary period, the British Parliament passed the Quartering Act of 1765,[145] which required colonists to provide barracks and supplies for soldiers stationed in the Colonies.[146] The British later expanded this provision with the Quartering Act of 1774,[147] which provided for further military housing in "uninhabited houses, out-houses, barns, or other buildings."[148]

The colonists strongly rejected even the possibility of quartering in their private property, and the British had "scrupulously avoided" the use of

747 (Boston, Hillard, Gray & Co. 1833).

[138] *See* Fields & Hardy, *supra* note 14, at 416. As Fields and Hardy describe, resentment against "the involuntary quartering of soldiers found expression in the First Continental Congress's Declaration of Resolves of 1774, and in the Declaration of Independence of 1776." *Id.* at 417 (citation omitted).

[139] *See id.* at 395.

[140] *See id.* at 402–13 (explaining that the quartering problem advanced England towards civil war).

[141] *See* Bell, *Forgotten but Not Gone*, *supra* note 14, at 117–29 (explaining that guarantees such as the one provided in the Third Amendment have historically been used to prevent forced billeting of troops in civilians' homes); Fields & Hardy, *supra* note 14, at 402–06 (describing the right in England in relation to the King's desire to maintain a standing army).

[142] Bell, *Forgotten but Not Gone*, *supra* note 14, at 124.

[143] *Id.* at 124–25.

[144] Billeting Act, 1679, 31 Car. 2, c. 1, § 32 ("[N]oe officer Military or Civill nor any other person whatever shall from henceforth presume to place quarter or billet any Souldier or Souldiers upon any Subject or Inhabitant of this Realme . . . without his consent . . . .").

[145] An Act for Punishing Mutiny and Desertion, and for the Better Payment of the Army and Their Quarters, 1765, 5 Geo. 3, c. 33 (Eng.).

[146] *Id.*; Bell, *Forgotten but Not Gone*, *supra* note 14, at 126.

[147] An Act for the Better Providing Suitable Quarters for Officers and Soldiers in His Majesty's Service in North America, 1774, 14 Geo. 3, c. 54 (Eng.).

[148] *Id.* § 2.

private homes under the 1765 Act.[149] Nonetheless, the First Congress made sure to include a sweeping anti-quartering provision in the Bill of Rights. The objections that gave rise to the Third Amendment's nearly universal adoption were rooted in control over private property and the ability to exclude military influences and impositions.[150]

This right to control property has been recognized by modern courts as establishing important "zones of privacy" along with the First, Fourth, and Fifth Amendments. In *Griswold v. Connecticut*,[151] the U.S. Supreme Court recognized the Third Amendment's prohibition against quartering as one of the many "facet[s]" of privacy incorporated into the Bill of Rights.[152] Similarly, the Court in *Katz v. United States*[153] emphasized that the Third Amendment is one of a handful of provisions in the Constitution that protects "personal privacy" from "government intrusion."[154]

C. Interaction Between the Third, Fourth, and Fifth Amendments

The Third Amendment, like the Fourth Amendment[155] and Fifth Amendment,[156] creates "zones of privacy."[157] These zones are complimentary, and courts will generally avoid interpretations that would bring them into disharmony.[158] Many actions that infringe one right may also infringe another. For example, the quartering of troops on private property without consent or compensation might constitute both a violation of the Third Amendment and a violation of the Fifth Amendment Takings Clause.[159] The actions of quartered troops might also run afoul of the

[149] J. Alan Rogers, *Colonial Opposition to the Quartering of Troops During the French and Indian War*, 34 MIL. AFF. 7, 10 (1970).

[150] *See* Dugan, *supra* note 14, at 560–71 (discussing the meaning of the quartering right based on founding-era documents).

[151] 381 U.S. 479 (1965).

[152] *Id.* at 484.

[153] 389 U.S. 347 (1967).

[154] *Id.* at 350 n.5.

[155] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

[156] *Id.* amend. V ("No person shall . . . be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.").

[157] *Griswold*, 381 U.S. at 484; *see supra* note 15 and accompanying text.

[158] *See id.* at 484–86 (stating that the citizen has a zone of privacy stemming from the collection of all privacy rights and that the Ninth Amendment does not allow for one right to be disparaged over the other).

[159] *See* Bell, *Forgotten but Not Gone*, *supra* note 14, at 146–48 (analyzing the distinction between quartering and takings and arguing that "the Fifth Amendment should guarantee that those who suffer quartering receive just compensation for their losses").

Fourth Amendment Search and Seizure Clause[160] or the First Amendment Free Association Clause.[161]

Still it is important to analyze each of these rights separately. It is particularly important to distinguish between the application of the Third Amendment quartering provision and the Fifth Amendment Takings Clause for several reasons. First, the quartering provision covers a narrower range of government actions.[162] Second, the Takings Clause is more permissive than the quartering provision and could allow occupation of private property even absent consent.[163] And third, while the quartering and takings provisions are not mutually exclusive, they can provide independent and distinct remedies.[164]

The analysis of Third Amendment protections may occasionally overlap with analysis under the Fourth Amendment right to be free from unreasonable searches and seizures,[165] and the Fifth Amendment right to due process.[166] While these rights might also provide relief in some circumstances, they will be inapplicable in many cases where the clear prohibition of the Third Amendment remains in force.[167] This is especially true where matters of national security are concerned.[168]

III. APPLYING THE THIRD AMENDMENT TO MILITARY CYBEROPERATIONS

The Third Amendment prohibitions govern military intrusions onto private property. Cyberoperations can affect private computers and networks, including innocent third-party systems.[169] As the U.S. military develops its strategy and begins to conduct cyberoperations, its actions

[160] Schmidt, *supra* note 14, at 663–65.

[161] *Id.*

[162] *See* Bell, *Forgotten but Not Gone*, *supra* note 14, at 118, 146–49 (evaluating the Third Amendment as a "form of taking" and applying analysis from Fifth Amendment cases).

[163] *See* Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 421 (1982) (holding that the physical occupation of a building by cable company facilities was a "taking" requiring just compensation). The Takings Clause provides for compensation for public uses, rather than relying on "Owner" consent. U.S. CONST. amend. V.

[164] Bell, *Forgotten but Not Gone*, *supra* note 14, at 146–48.

[165] *See, e.g.*, Dugan, *supra* note 14, at 575–82 (discussing the different protections of and purposes behind the Fourth and Third Amendments).

[166] *See, e.g.*, Schmidt, *supra* note 14, at 616, 663–65 (evaluating possible due process issues and asserting that the Third Amendment's application must remain narrower than the Fourth Amendment's because, to find otherwise, "would essentially delete the term soldier in the amendment and replace it with government agent").

[167] *See, e.g.*, James P. Rogers, Note, *Third Amendment Protections in Domestic Disasters*, 17 CORNELL J.L. & PUB. POL'Y 747, 748–50 (2008) (describing military relief efforts in post-Katrina New Orleans and arguing that they constituted unlawful quartering even though they did not violate Fourth or Fifth Amendment rights).

[168] *See generally* Dugan, *supra* note 14, at 584–86 (assessing the implications of Third Amendment prohibitions for the NSA's warrantless wiretapping program).

[169] *See id.* at 587 (concluding that the Third Amendment is highly relevant today and could apply to government intrusions on civilian life, such as wiretapping).

affecting domestic systems must comply with Third Amendment principles.

Each category of cyberoperations has the potential to affect private systems in the United States. The use of a self-replicating virus or worm, such as Stuxnet, can result in widespread infection beyond the intended military target. Even more targeted cyberexploits, such as Flame or Red October, use intermediate networks and devices to gain access to their targets. Additionally, a retaliatory strike or hack-back may harm an innocent third-party system rather than the actual attacker. The Third Amendment governs all of these situations if the affected system belongs to someone under U.S. jurisdiction.

To determine whether the Third Amendment prohibits a given military cyberoperation, the relevant inquiry would be: (1) is the computer or network device property protected as part of "any house," and (2) does the military intrusion constitute "quartering" by a "Soldier"? If the network or device is protected, and the military intrusion constitutes quartering, then consent is required under the Third Amendment during times of peace and a formal legal enactment is required during times of war.

A. The Private Property Protected by the Third Amendment Includes Computer and Network Infrastructure

The first issue relevant to the Third Amendment analysis of military cyberoperations is whether civilian computers and networks are protected. The Third Amendment prohibits quartering "in any house."[170] This provision could be interpreted as protecting only residential buildings, as opposed to the "persons, houses, papers, and effects" protected by the Fourth Amendment.[171] However, the history of the Third Amendment indicates that it governs "quartering" on excludable private property generally, regardless of the specific structure or parcel used.[172] In respecting the "Owner['s]" right to exclude, the scope of the Third Amendment may in fact be broader than the Fourth Amendment.[173] The only federal court to fully analyze and apply the Third Amendment in a modern context took a similarly broad view of the protected property right.[174]

[170] U.S. CONST. amend. III.

[171] *Id.* amend. IV.

[172] *See* Dugan, *supra* note 14, at 581 (employing the history of the Third Amendment, along with an interpretation of the Fourth Amendment to "suggest that the term [any house] was meant to cover all areas in which an individual has a right to exclude").

[173] *See id.* at 582 (rejecting a narrow view of the term "any house" and instead arguing that the term has been broadly interpreted throughout history to protect "'any' private area in which an individual 'Owner' can claim a right to exclude," contrary to the Fourth Amendment, which protects only "persons, houses, papers, and effects").

[174] *See* Engblom v. Carey, 677 F.2d 957, 961–64 (2d Cir. 1982) (characterizing the

The history surrounding the ratification of the Third Amendment also suggests that a broad view is appropriate. The English quartering statutes traditionally provided for quartering in "public houses" during wartime,[175] including the 1765 provision governing quartering in the Colonies.[176] These statutes specifically listed the types of structures that could be used for quartering.[177] This was even true of the Quartering Act of 1774, one of the "intolerable acts" that revolutionary colonists cited in the lead up to the war.[178] Notably, British soldiers "were not quartered in private colonial houses" during the pre-revolutionary period.[179] When the Third Amendment was enacted, however, Congress rejected an alternative proposal that would have allowed billeting of soldiers in public houses and inns.[180] Rather than provide specific rules based on the classification of property, Congress adopted a general prohibition governing "any house."[181]

The Second Circuit adopted a broad view of the Third Amendment's property protections in *Engblom*.[182] There, the court analyzed the Third Amendment's application based on its role in assuring "a fundamental right to privacy," as noted by the Supreme Court in *Griswold*.[183] The Second Circuit rejected a rigid application of the term "Owner" because it "would be wholly anomalous when viewed, for example, alongside established Fourth Amendment doctrine" that protects tenants.[184] The court ultimately held that the Third Amendment's property-based privacy interests are not

Third Amendment as applying to tenants in addition to "Owner[s]" that possess a fee simple interest in their homes). The U.S. Court of Appeals for the Tenth Circuit, however, relied on *Engblom*'s Third Amendment analysis and found that the Air Force did not violate the Third Amendment by flying over plaintiff's property because there is no right to exclude aircraft in the navigable airspace. Custer Cnty. Action Ass'n v. Garvey, 256 F.3d 1024, 1043 (10th Cir. 2001).

[175] Wyatt, *supra* note 14, at 142–43.

[176] An Act for Punishing Mutiny and Desertion, and for the Better Payment of the Army and Their Quarters, 1765, 5 Geo. 3, c. 33 (Eng.).

[177] *See* An Act for the Better Providing Suitable Quarters for Officers and Soldiers in His Majesty's Service in North America, 1774, 14 Geo. 3, c. 54 (Eng.) (specifying "uninhabited house, outhouse, [and] barns"); An Act for Punishing Mutiny and Desertion, and for the Better Payment of the Army and Their Quarters, 1765, 5 Geo. 3, c. 33 (Eng.) (listing, among other places, "inns, livery stables, ale-houses, victualling-houses, . . . uninhabited houses, outhouses, [and] barns").

[178] An Act for the Better Providing Suitable Quarters for Officers and Soldiers in His Majesty's Service in North America, 1774, 14 Geo. 3, c. 54 (Eng.); *see* Wyatt, *supra* note 14, at 143. Resentment against "the involuntary quartering of soldiers found expression in the First Continental Congress's Declaration of Resolves of 1774, and in the Declaration of Independence of 1776." Fields & Hardy, *supra* note 14, at 417 (citation omitted).

[179] JOHN PHILLIP REID, CONSTITUTIONAL HISTORY OF THE AMERICAN REVOLUTION: THE AUTHORITY OF RIGHTS 194 (1986); *see* Rogers, *supra* note 149, at 10 (noting that "[q]uartering in private homes was scrupulously avoided" under the 1765 Act).

[180] THE COMPLETE BILL OF RIGHTS: THE DRAFTS, DEBATES, SOURCES, AND ORIGINS 217–19 (Neil H. Cogan ed., 1997).

[181] U.S. CONST. amend. III.

[182] 677 F.2d 957 (2d Cir. 1982).

[183] *Id.* at 962 (citing Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965)).

[184] *Id.*

limited only to those "Owner[s]" who possess a fee simple ownership of their residence but instead protect citizens who lawfully occupy or possess a residence.[185]

In a more recent case, *Custer County Action Ass'n v. Garvey*,[186] the U.S. Court of Appeals for the Tenth Circuit rejected a claim under the Third Amendment based on the military use of airspace over a plaintiff's home.[187] The court reviewed the claim under the *Engblom* framework and found that the plaintiffs had no general right to exclude planes traversing the airspace over their property.[188] The Supreme Court had reached a similar conclusion under the Fifth Amendment Takings Clause years earlier in *United States v. Causby*.[189] Thus, the Tenth Circuit followed a similar analysis of the Third Amendment where "any home" was defined as a property area in which an individual has a right to exclude others.[190]

When framed as a right to exclude the military from private property, it is clear that computers, networks, and other systems fall within the scope of the Third Amendment. The phrase "any house" encompasses all forms of property that fit within the typical paradigm. Rather than include or exclude certain types of property, the Framers opted for broad language.[191] Civilian networked devices will necessarily fall within this category because they are maintained within, and are a component of, private property. Hacking is analogous to a trespass,[192] and typical home and corporate systems can also rightfully be classified as private property.[193]

[185] *Id.*

[186] 256 F.3d 1024 (10th Cir. 2001).

[187] *Id.* at 1042–44.

[188] *Id.*

[189] 328 U.S. 256, 261 (1946) (noting that Congress declared "[t]he air is a public highway" and that "[c]ommon sense revolts at the idea" of aircraft operators being subject to trespass suits based on property ownership interests stretching into the sky).

[190] *Garvey*, 256 F.3d at 1043.

[191] *See* Wyatt, *supra* note 14, at 142–47 (reviewing the possible interpretations relevant to whether university property would be protected under the Third Amendment and arguing that the term "any house" should be interpreted broadly to include such property).

[192] Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, 4 CAL. CRIM. L. REV. 1, ¶ 81 (2001); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1606 (2003); *see* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1021 (2001) ("The crime of unauthorized access is one of simply invading another's workspace.").

[193] *See, e.g.*, Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 471–73 (Ct. App. 1996) (imposing liability under a claim for trespass on personal property where a child hacked into a phone company's computer system to make free long-distance telephone calls); *see also* Daniel Benoliel, *Law, Geography, and Cyberspace: The Case of On-Line Territorial Privacy*, 23 CARDOZO ARTS & ENT. L.J. 125, 181 (2005) (discussing the *Bezenek* case); Wendy Leibowitz, *Imposing Order on E-Chaos: It's Time To Seize the Bull by the Horns and Set Sound E-mail Policies for the Workplace*, LAW PRAC. MGMT., Nov.–Dec. 2002, at 8, 10 (recognizing that "company computers are private property"); Cody Wamsley, *Internet Transmissions: Who Owns the Data and Who Protects It?*, J. INTERNET LAW, Feb. 2008, at 3, 7 ("It is settled law that someone can own a computer as chattel."). *See generally* Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*,

Invasion of these systems is prohibited by comprehensive federal laws that recognize this general right to exclude.[194]

B. Military Software Placed on a Home or Business Network or Computer Device Is "Quartered" for Third Amendment Purposes

Having established that the Third Amendment protects private networks and computer systems, it is necessary to consider whether military cyberoperations can be "quartered" on these systems. While the conclusion that a military cyberoperation constitutes quartering in a system would be a novel application of the quartering provision,[195] it would be consistent with the purposes and principles underlying the Third Amendment. There are at least two interpretive hurdles relevant to this inquiry: (1) whether computer software and files can be "quartered" at all, and (2) whether these elements are indeed an extension of the regulated "Soldier" used in the Third Amendment. The language can be reasonably interpreted to apply to certain military cyberoperations, especially given the underlying concern of the Third Amendment: that military personnel will cause harm to civilians by imposing on their private property.[196]

As it relates to the first hurdle, cyberoperations may constitute quartering because they involve trespassing into and placing files on a private system. The long history of quartering was focused primarily on the provision of lodging to members of the military.[197] The modern usage of the term

17 BERKELEY TECH. L.J. 421, 430–35 (2002) (summarizing four cases concerning trespass to chattels in cyberspace).

[194] *See, e.g.*, Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006 & Supp. V 2012) (providing victims with a civil cause of action against cyber criminals); Telephone Records and Privacy Protection Act of 2006, *id.* § 1039 (2006) (providing a right to exclude in the context of confidential phone records information). *See generally* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164 (2004) (reviewing the current legal framework for protecting "cyberproperty").

[195] This application, however, is not as novel as Third Amendment claims suggested by other commentators. *See, e.g.*, Morriss & Stroup, *supra* note 14, at 798 (arguing that the Third Amendment should be interpreted to invalidate the Endangered Species Act).

[196] U.S. CONST. amend. III; *see* Laird v. Tatum, 408 U.S. 1, 15–16 (1972) (asserting that the Third Amendment empowers the federal courts to provide redress for claims of "judicially cognizable injury resulting from military intrusion into the civilian sector"); *see also* Whalen v. Roe, 429 U.S. 589, 607 n.* (1977) (Stewart, J., concurring) ("The Third Amendment's prohibition against the unconsented peacetime quartering of soldiers protects another aspect of privacy from governmental intrusion."); Katz v. United States, 389 U.S. 347, 350 n.5 (1967) (same); Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (same); Poe v. Ullman, 367 U.S. 497, 549 (1961) (recognizing that the Third Amendment protects the privacy of the home); Wyatt, *supra* note 14, at 124–33 (arguing that the Third Amendment protects property rather than privacy).

[197] William Sutton Fields, *The Third Amendment: Constitutional Protection from the Involuntary Quartering of Soldiers*, 124 MIL. L. REV. 195, 195–204 (1989) (reviewing English and American history to pinpoint the meaning of "quartering" for purposes of the Third Amendment); Rogers, *supra* note 14, at 767 (using Samuel Johnson's 1755 *Dictionary of the English Language* to ascertain the scope of the term "quarter"); Wyatt, *supra* note 14, at 147–51 (analyzing late seventeenth and early eighteenth century English

"quarter,"—to "lodge, or dwell,"[198]—generally matches the traditional definition of "quarter" at the time of the framing—"to lodge; to fix on a temporary dwelling."[199] Furthermore, the modern definition of "to lodge"—"to provide temporary quarters for" or "to establish or settle in a place"[200]—also tracks the traditional definition of "to lodge"—"[t]o place in a temporary habitation" or "[t]o afford place to."[201] At a minimum, it is clear that the quartering concept encompasses "something less than a permanent occupation."[202] It is unclear whether any mere trespass would suffice, or whether there must be some extended use of the private property to constitute quartering.[203]

Given the definition and purpose of the quartering provision, it is likely that cyberoperations could constitute quartering to the extent that they involve intruding into and placing files on a private system. These files can cause damage and impose costs on the "Owners" similar to the "Soldier[s]" quartered in a traditional Third Amendment case.

The second issue involves whether these cyberoperations fall within the Third Amendment because they are carried out by "Soldier[s]." The problem of applying the traditional legal principles of warfare to the cyberspace domain is not a new one. A great deal of recent scholarship has focused on the application of international law in cyberspace.[204] While the analysis of cyberattacks under customary international law and the law of war focus on the use of physical force, the military attribution of these operations is a baseline assumption of all the analysis.[205] The term cyberoperations is used throughout a forthcoming cyberwar manual to refer to the "employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace."[206] Cyberoperations are military operations to the extent that USCYBERCOM is executing or coordinating the operations. Consequently, the Third Amendment governs

jurisprudence and vocabulary to define "quartering" for purposes of the Third Amendment).

[198] MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 1018 (11th ed. 2003).

[199] 2 SAMUEL JOHNSON, A DICTIONARY OF THE ENGLISH LANGUAGE 1619 (1st ed. 1755).

[200] MERRIAM-WEBSTER'S, *supra* note 198, at 731.

[201] JOHNSON, *supra* note 199, at 1218.

[202] Wyatt, *supra* note 14, at 149.

[203] *But see* Luther v. Borden 48 U.S. 1, 48, 67 (1849) (Woodbury, J., dissenting) (arguing that forced entry of militiamen into a home constituted a Third Amendment violation).

[204] *See, e.g.*, Schmitt, *supra* note 9, at 14–15 (comparing Koh's approach against the *Tallinn Manual* in applying international law to cyberspace); Koh, *supra* note 9 (addressing the Obama Administration's views on how international law applies in cyberspace); *see also* TALLINN MANUAL, *supra* note 9 (identifying international law applicable to cyberwarfare and proposing ninety-five black letter rules to regulate cyberspace).

[205] *See, e.g.*, TALLINN MANUAL, *supra* note 9, at 51 ("A nexus between the cyber operation in question and military operations heightens the likelihood of characterization as a use of force.").

[206] *Id.* at 24.

a cyberoperation's invasion of private property.

This view is consistent with both a broad reading of the anti-quartering right in English cases as well as the Second Circuit's holding in *Engblom*.[207] There is English common law, for example, related to the quartering of horses in "actual service."[208] The horses were merely an instrumentality of war used by the soldiers, but they were considered quartered at common law.[209] Similarly, in *Engblom*, the Second Circuit held that the National Guardsmen were considered "Soldiers" within the meaning of the Third Amendment because they were "state employees under the control of the Governor."[210] The degree of military "control" was key in both cases.[211]

Under this analysis, quartering of "Soldiers" in private computer systems occurs when military operators directly or indirectly employ files or software that accesses and places itself upon a private system. Typically, a C&C server will direct cyberoperations that another group is responsible for configuring.[212] In the case of an active defense system, a remote or local system could also control the operation.[213] Regardless, USCYBERCOM closely controls and manages any cyberoperation that the United States currently undertakes.[214]

IV. DESIGNING A NATIONAL CYBERSECURITY POLICY INFORMED BY THIRD AMENDMENT PRINCIPLES

The preceding analysis of cyberoperations under the Third Amendment is focused primarily on the potential privacy impact of U.S. military intrusions into private networks. Given that the Third Amendment embodies the core value of protecting private property from military

[207] *See generally* Engblom v. Carey, 677 F.2d 957 (2d Cir. 1982) (providing a framework for interpreting the Third Amendment).

[208] *See, e.g.*, Read v. Willan, (1780) 99 Eng. Rep. 271 (K.B.) 273; 2 Dougl. 422, 426 ("Under the distinction that these horses were mustered, and to be considered, as in actual service, (which I think, upon the case stated, they were,) I am of opinion they were billetable.").

[209] *See, e.g.*, *id.* at 271, 273; 2 Dougl. at 423, 426.

[210] *Engblom*, 677 F.2d at 961.

[211] *See id.* (holding that National Guardsmen are "Soldiers" for Third Amendment purposes); *Read*, 99 Eng. Rep. at 271–73; 2 Dougl. at 422–26 (holding that the horses in question were billetable under the Mutiny Act because they were in "actual service" under a route from the commander in chief and rejecting the argument that the horses were not billetable because they were hired under contract rather than employed by the army).

[212] *See supra* Part I.A–B (discussing different types of cyberoperations that are directed by a C&C server configured by the responsible attacker).

[213] *See supra* text accompanying notes 101–02 (observing that one problem with an active defense system is that the responsible attacker can use an intermediate system that actually belongs to someone else).

[214] *See U.S. Cyber Command*, *supra* note 20 (explaining that USCYBERCOM is charged with U.S. military cyberspace operations).

intrusion, its principles should inform the broader debate over cybersecurity policy.

The President, the DoD, the Department of Homeland Security (DHS), and Congress are all currently involved in developing a comprehensive cybersecurity strategy.[215] The DoD established USCYBERCOM in 2009 to advance the technical and operational capabilities necessary to implement a comprehensive cybersecurity strategy.[216] Congress considered competing proposals in 2012—both of which focused on creating a new 'information sharing' environment between private companies and government.[217] The President has issued a directive establishing "principles and processes for the use of cyber operations,"[218] and conducted an internal legal analysis of his authority vis-à-vis cyberwarfare.[219]

Yet, so far, none of these efforts have adequately addressed the civil liberties impact of cyberoperations. Even though the White House issued a "Cyberspace Policy Review" stressing the need to "conduct a national dialogue on cybersecurity" and reaffirming "the national commitment to privacy rights and civil liberties guaranteed by the Constitution and law,"[220] the administration has not yet engaged in such a dialogue. Some within the DoD have acknowledged that there will be difficult questions in applying traditional legal rules to cyberspace, but so far, the DoD has not provided solutions.[221] Congress has focused on eliminating privacy rules that it claims would hamper corporate information sharing with the DHS and NSA.[222]

[215] *See generally* Kesan & Hayes, *supra* note 10, at 460–62 (discussing recent federal initiatives by the President, DHS, DoD, and Congress).

[216] U.S. DEP'T OF DEFENSE, U.S. CYBER COMMAND FACT SHEET (May 25, 2010).

[217] *See* Brendan Sasso, *Longtime Friends Lieberman, McCain Divided Over Cybersecurity Legislation*, HILL (Mar. 14, 2012, 4:00 AM), http://thehill.com/blogs/hillicon-valley/technology/215907-senators-mccain-lieberman-disagree-its-a-real-doozy (reporting that while Senators Lieberman and McCain introduced opposing bills for cybersecurity regulation, both proposals contain an information sharing component).

[218] *Obama Signs Secret Cybersecurity Directive*, NAT'L J. (Nov. 14, 2012, 3:35 PM), http://www.nationaljournal.com/blogs/techdailydose/2012/11/obama-signs-secret-cybersecurity-directive-14.

[219] Sanger & Shanker, *supra* note 19.

[220] EXEC. OFFICE OF THE PRESIDENT, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE, at i (2009) [hereinafter CYBERSPACE POLICY REVIEW], *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[221] *See, e.g.*, Greer, *supra* note 10, at 141 (arguing that the NSA must "allay concerns about civil liberties violations" by "maintaining transparency, by continuing oversight, and by establishing clarity of roles and missions").

[222] *See* Hayley Tsukayama, *CISPA: Who's for It, Who's Against It and How It Could Affect You*, WASH. POST (Apr. 27, 2012), http://www.washingtonpost.com/business/technology/cispa-whos-for-it-whos-against-it-and-how-it-could-affect-you/2012/04/27/gIQA5ur0lT_story.html (observing that CISPA "could be interpreted to allow companies to share any of their customers' personal data as long as the companies say that the information is related to a 'cyber threat'").

The Third Amendment implications of military cyberoperations raise three important questions that should guide the development of cybersecurity policy going forward: (1) Can the President alone authorize military actions that have the potential to intrude upon civilian networks? (2) How can "consent" be granted for such cyberspace operations? (3) Would the United States be forced to admit attribution for a given attack if it intruded upon an innocent third-party network? These questions address the three key elements of a comprehensive cybersecurity strategy: authority, cooperation, and transparency.

A. Authority: Congress Must Be Involved in Establishing Any Framework for the Authorization of Cyberoperations

Given that the Third Amendment requires war-time quartering be conducted "in a manner to be prescribed by law,"[223] Congress must have a role in establishing the framework used to authorize any offensive cyberoperation. This legislative involvement would not only ensure that all cyberoperations have adequate legal authorization but it would also promote the broader goals of transparency and cooperation that the President has emphasized throughout this process.

So far Congress has focused its energy on perceived problems rather than real solutions.[224] A debate raged in the 112th Congress over whether to let DHS or NSA take the lead on a proposed information-sharing environment.[225] This turf war was quite tangential from the problems of substandard security for critical systems and a lack of legal clarity as to the role of each government agency in responding to an external threat or strategic opportunity.[226] The only congressional involvement in developing a cybersecurity framework so far has been its brief affirmance in the 2012 National Defense Authorization Act[227] that the President may conduct "operations in cyberspace" subject to the traditional legal regimes applicable to kinetic warfare.[228] Congress's active role in setting our

[223] U.S. CONST. amend. III.

[224] *See, e.g.*, Sasso, *supra* note 217 (discussing Senators Lieberman and McCain's focus on whether a civilian or military agency should coordinate the cybersecurity program rather than on improved security standards).

[225] *Id.*

[226] *See* CYBERSPACE POLICY REVIEW, *supra* note 220, at i (recognizing that the "[r]esponsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way"); *see also* Kesan & Hayes, *supra* note 10, at 458–60 (describing the current danger to critical national infrastructure).

[227] National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, 125 Stat. 1298 (2011).

[228] *Id.* § 954. The provision states:

> Congress affirms that the Department of Defense has the capability, and upon

nation's military actions in cyberspace is the only way to have a national dialogue and to avoid relying on secret legal interpretations about important national security matters.

The President took steps to begin a national dialogue when he issued an Executive Order on the same day as the 2013 State of the Union Address.[229] The Executive Order focused on improving critical infrastructure cybersecurity while promoting privacy, civil liberties, and the economy.[230] The Order also provided for sharing of "cyber threat information" from executive branch agencies to private sector entities,[231] and the development of a framework by the National Institute of Standards and Technology (NIST) to establish baseline security standards for government agencies and critical infrastructure companies.[232] The Order also required that privacy and civil liberties protections be incorporated into the cybersecurity program and that the Chief Privacy Officer of DHS assess the privacy risks and publish a report.[233]

The Executive Order did not address the "information sharing environment" proposed in Congress during 2012 and again in 2013.[234] The Order also did not address the legal determination of when and how cyberoperations can be authorized, which has apparently already been made in an internal executive-branch memorandum.[235] The President's Executive Order is a step in the right direction but it does not provide sufficient authority for cyberoperations that could intrude upon civilian systems; only Congress can authorize such quartering.

B. Cooperation: The Private Sector Has an Interest in Increasing

> direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to—
>
> (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and
>
> (2) the War Powers Resolution (50 U.S.C. 1541 et seq.).

Id.

[229] Exec. Order No. 13,636, 78 Fed. Reg. 11,737 (Feb. 19, 2013); *see* Andy Greenberg, *President Obama's Cybersecurity Executive Order Scores Much Better than CISPA on Privacy*, FORBES (Feb. 12, 2013, 10:37 PM), http://www.forbes.com/sites/andygreenberg/2013/02/12/president-obamas-cybersecurity-executive-order-scores-much-better-than-cispa-on-privacy.

[230] Exec. Order No. 13,636, 78 Fed. Reg. at 11,739.

[231] *Id.* at 11,739–40.

[232] *Id.* at 11,740–41.

[233] *Id.* at 11,740.

[234] *See* Chris O'Brien, *CISPA Passes House Committee, Angering Privacy Activists*, L.A. TIMES (Apr. 10, 2013, 4:38 PM), http://www.latimes.com/business/technology/la-fi-tn-cispa-passes-house-committee-20130410,0,7554885.story.

[235] *See* Sanger & Shanker, *supra* note 19 ("A secret legal review on the use of America's growing arsenal of cyberweapons has concluded that President Obama has the broad power to order a pre-emptive strike if the United States detects credible evidence of a major digital attack looming from abroad, according to officials involved in the review.").

Security, and Public-Private Collaboration Is Necessary To Address This Issue

The current cybersecurity frameworks being considered by Congress and the President both rely on broad private-sector cooperation to improve security standards and limit the risk of future attacks.[236] This collaborative process not only makes good practical sense, because private companies directly control many target systems,[237] but the process also facilitates a consent mechanism that limits the Third Amendment implications of cyberoperations.[238] An intrusion, whether intentional or inadvertent, would be permissible under the Third Amendment with the "Owner['s]" consent.[239]

There may be circumstances where threat detection is coordinated by both military and private sector entities, and these relationships will necessarily involve consent. The alternative is giving only military agencies control over the standards-setting process, which some members of Congress have proposed[240] but the President's Executive Order rejected.[241] Under the military-control system, USCYBERCOM would be able to engage in "active defense" operations without public notice or consent.

The more difficult question involves the extent to which third-party companies will provide the DoD access to private customer data as part of the "threat detection" effort. These users have strong privacy interests in their data, and also an expectation that they can control who has access to it.[242] The Executive Order's proposed framework lead by NIST solves both problems by providing a consent mechanism that is both cooperative and transparent.[243]

[236] *See* Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. NAT'L SEC. L. & POL'Y 233, 240–41 (2010) (arguing that it is critical to create a safe space for public-private collaboration and to promote proper security standards).

[237] *Id.*

[238] *See id.* at 240 (stating that eighty-five percent of the nation's infrastructure is owned by the private sector).

[239] U.S. CONST. amend. III.

[240] Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, S. 3342, 112th Cong. (2012) (proposing cybersecurity centers managed by the President in the interests of national security to collect and share cyber "threat information").

[241] Exec. Order No. 13,636, 78 Fed. Reg. 11,737, 11,741 (Feb. 19, 2013) (indicating that the Secretary of Homeland Security, a civilian agency, shall coordinate the new cybersecurity program).

[242] *See, e.g.*, Tsukayama, *supra* note 222 (warning Internet users about how the White House's passage of the Cyber Intelligence Sharing and Protection Act could affect them).

[243] Exec. Order No. 13,636, 78 Fed. Reg. at 11,741 ("The Cybersecurity Framework . . . shall meet the requirements of the National Institute of Standards and Technology Act . . . .").

C. Transparency: Any Comprehensive Cybersecurity Strategy Must Include Both Public Accountability and Open Discussion of the Civil Liberties Impacts

Given the important public interests at stake in the cybersecurity debate—security, privacy, and civil rights—it will be critical that there be adequate transparency and accountability in the comprehensive framework. The cyberattack attribution problem should not be treated like a double-edged sword that can prevent identification of foreign attackers and lead to mistaken retaliation against innocent intermediaries, while shielding the United States from accountability when it makes a mistake. If military cyberoperations intrude upon civilian property, there could very well be legal consequences including public attribution and accountability. It is better to embrace this accountability than to run from it.

An attribution requirement would challenge the current national security orthodoxy. For more than sixty years the DoD has focused on controlling information: more of it for them, less of it for everyone else.[244] The state secrets privilege, classification, and other methods of executive branch secrecy have created a secret-war framework built on a "shaky legal and political foundation" according to Professor Jack Goldsmith.[245] In order to maintain political and constitutional legitimacy, it is necessary to revise the current military decisionmaking process to enable greater transparency and accountability.[246] Justification for military operations cannot rely solely on classified legal interpretations or sealed court filings; the ongoing development of constitutional rights requires that citizens know what the government is doing.[247] Military secrecy would otherwise negate the very

[244] *See generally* Carrie Newton Lyons, *The State Secrets Privilege: Expanding Its Scope Through Government Misuse*, 11 LEWIS & CLARK L. REV. 99 (2007) (arguing that the government has misapplied the state secrets privilege doctrine to obtain broad protection of its information collection activities, intruding upon private constitutional and statutory rights); Jeremy Telman, *Intolerable Abuses: Rendition for Torture and the State Secrets Privilege*, 63 ALA. L. REV. 429 (2012).

[245] *See* Jack Goldsmith, *U.S. Needs a Rulebook for Secret Warfare*, WASH. POST (Feb. 5, 2013), http://www.washingtonpost.com/opinions/us-needs-rules-of-engagement-for-secret-warfare/2013/02/05/449f786e-6a78-11e2-95b3-272d604a10a3_story.html (identifying some recent secret wars fought on tenuous legal grounds and how the government has secretly assessed its own authority in cyberwarfare).

[246] *See id.* (proposing new statutory provisions that would render covert military actions more transparent and accountable to the public).

[247] *See e.g.*, United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 308, 324 (1972) (rejecting the motion of the United States to vacate a judge's order to make full disclosure of monitored telephone conversations and holding that the President's power to safeguard national security does not outweigh the Fourth Amendment protections for private telephone conversations); *see also* Clapper v. Amnesty Int'l, USA, 133 S. Ct. 1138 (2013) (rejecting a constitutional challenge to warrantless collection of private telephone conversations pursuant to the Foreign Intelligence Surveillance Act (FISA) Amendments Act because plaintiffs could not provide sufficient evidence to show that they had been subject to surveillance).

protections guaranteed by the Third Amendment—imagine the Department of Justice responding to a quartering claim by arguing that they can neither confirm nor deny whether a member of the U.S. military was quartered in the plaintiff's home.

Another symptom and source of this transparency problem is the growth in classification without adequate oversight.[248] Experts have put forth proposals to address this problem by implementing classification audits, improving training materials, and changing the incentives by reducing default classification.[249] These proposals along with efforts to implement the 2010 Reducing Over-Classification Act[250] should provide a step in the right direction,[251] but that cannot be the end of the process.

In the cybersecurity context, transparency at both ends will serve to ensure the type of "national dialogue" that the White House promoted in 2009.[252] Accountability for military overreach through attribution would be exactly the relief "necessary to effectuate"[253] the underlying policy of the Third Amendment.[254] It would ensure that any intrusions are either conducted through a legal framework that was approved and understood by the public (through Congress), or identified and remedied after the fact. The alternative is a system where overextended military operations are only brought to light by selective leaks, which are then subject to intense scrutiny by federal law enforcement.[255] In that system, military decisions

[248] *See* ELIZABETH GOITEIN & DAVID M. SHAPIRO, BRENNAN CTR. FOR JUSTICE, REDUCING OVERCLASSIFICATION THROUGH ACCOUNTABILITY 4–11 (2011), *available at* http://www.brennancenter.org/sites/default/files/legacy/Justice/LNS/Brennan_Overclassification_Final.pdf (outlining the history and costs of overclassification). The DoD recently issued a memo related to the Inspector General's evaluation of the overclassification problem, but even that memo was marked "For Official Use Only." Mike Masnick, *Defense Department Overclassifies Memo on Avoiding Overclassification*, TECHDIRT (Dec. 4, 2012, 11:58 AM), http://www.techdirt.com/articles/20121126/01371621143/defense-department-overclassifies-memo-avoiding-overclassification.shtml.

[249] *See* GOITEIN & SHAPIRO, *supra* note 248, at 33–50 (describing a six-part proposal to reduce overclassification by implementing new and more efficient systems for processing potentially classified material).

[250] Pub. L. No. 111-258, 124 Stat. 2648 (2010) (codified in scattered sections of 6 U.S.C. and 50 U.S.C. (Supp. IV 2011)).

[251] *See, e.g.*, Steven Aftergood, *Pentagon Classification General to Probe Overclassification,* SECRECY NEWS (Nov. 5, 2012), http://blogs.fas.org/secrecy/2012/11/dodig_overclass.

[252] CYBERSPACE POLICY REVIEW, *supra* note 220.

[253] Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 402 (1971) (Harlan, J., concurring in the judgment).

[254] *See* John C. Dehn, *The "Costs" of Accountability in War*, OPINIO JURIS (Aug. 16, 2011, 1:01 PM), http://opiniojuris.org/2011/08/16/the-costs-of-accountability-in-war (discussing the importance of accountability during war to "preserv[e] the rights of citizens against their government").

[255] *See, e.g.*, Peter Finn, *FBI Is Increasing Pressure on Suspects in Stuxnet Inquiry*, WASH. POST (Jan. 26, 2013), http://www.washingtonpost.com/world/national-security/fbi-is-increasing-pressure-on-suspects-in-stuxnet-inquiry/2013/01/26/f475095e-6733-11e2-93e1-475791032daf_story.html (reporting that the Federal Bureau of Investigation and prosecutors are pursuing current and former senior government officials in connection

trump civil rights,[256] which is clearly the opposite of what those who drafted the Third Amendment intended.

CONCLUSION

Although the Third Amendment is commonly forgotten, it is not gone, and the principles that underlie its protections should guide our military decisions impacting property and privacy. The recent focus on cybersecurity in particular would benefit from Third Amendment insights. Digital devices are modern-day equivalents of "castles" that deserve the strongest protections from outside intrusion.

Military cyberoperations threaten to intrude upon civilian networks and devices more frequently and easily than troops during traditional physical warfare. As a result, we must increase accountability and transparency to ensure that civil liberties are not compromised. The legislature and private sector must be involved in the standards-setting and decision-making processes to maintain the balance between civilian and military power that the Third Amendment embodies. The President's Executive Order on cybersecurity is a step in the right direction, but so far Congress has not provided adequate guidance or legal balance to executive power in this area.

There need to be clear rules about what the President can and cannot authorize in cyberoperations, and systems put in place to account for the inevitable mistakes that will be made.

with disclosures to the press of classified information about the Stuxnet cyberoperation).

[256] *See supra* note 10 and accompanying text (listing law journal articles that discuss the lack of consideration of civil liberties in conducting military cyberoperations and noting the dearth of conversation about civil rights in this area).