AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

CYBERSPACE AND POSSE COMITATUS: LEGAL IMPLICATIONS OF A BORDERLESS DOMAIN

By

Andrew K. Hosler, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors: Majors Don Davis and Ryan Oakley

Maxwell Air Force Base, Alabama

March 2010

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

Cyberspace is a domain shared by the entire world. The features which distinguish cyberspace from the traditional domains of air, land, sea, and space also raise legal questions about jurisdiction and attribution of offenses. This paper reviews some of the key distinguishing features of cyberspace and assesses the relevance of posse comitatus within the domain. It proposes invocation of the Insurrection Act of 1807 as legislation more compatible with the properties of cyberspace and offers potential applications.

In the spring of 2007, the nation of Estonia suffered a significant cyber attack.[1] The effects were felt on government command and control, the minds of the people, and stopped just short of shutting down economic markets.[2] Though never admitted, all indications point to a coordinated attack from Russia as the cause.[3] There was no prior indication of a pending attack. The swift attack on command and control, breaking the ties between the government and its military forces and people, hindered response and destabilized a population that felt insecure[4].

To date there is still legal and technical "murkiness" in holding a nation, organization, or individual ultimately responsible for an attack in cyberspace.[5] Cyberspace is not just a domain shared among all warfighting services; it is also a domain shared with individual citizens, business, the whole of government, and the world.[6] Tasks ranging from grade school book report turn-ins to public utility controls orders, and from stock purchases to military command and control orders transit many of the same, generally commercially-owned, routers, switches, computers, and wires, each with the goal of passing information from one location to another. According to the National Military Strategy for Cyberspace Operations, "operations in cyberspace are a critical aspect of our military operations around the globe."[7] The Estonia example shows how fragile both military response and population security are with an unknown enemy staging from an unknown location in light of the new cyber reality. It provides an opportunity and backdrop for reviewing the rules of borders and jurisdiction as it relates to cyberspace. Though the Estonian example allegedly implicates the Russians, in light of the new realities of our interconnected world, this paper presents an argument for a waiver of posse comitatus as a rule, rather than an exception, in the murkiness of cyberspace.

In order to effectively address this phenomenon, one must understand cyberspace. The definition of "cyberspace" itself is often contentious, however two sources provide adequate

understanding of the depth and breadth of the issue.[8] The Department of Defense defines "cyberspace" as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[9] This definition relates both the global aspect of the domain and introduces the concept of information as an environment. One can assume, and the Estonian example supports, that the information environment may be peaceful or contentious. The second telling definition comes from a 2001 Congressional Research Service Report for Congress: "the total interconnectedness of human beings through computers and telecommunication without regard to physical geography."[10] This definition highlights the lack of reliance on physical geography for cyberspace. In cyberspace, information travels physical connections around the world without regard to territorial borders and jurisdiction.

Other features of cyberspace further distinguish it from the traditional domains of land, sea, air, and space. Features of interest to a discussion of national defense include speed, attribution, low entry cost for relative effect, and public and private sector interrelatedness, each a benefit to a potential adversary.[11] Speed is apparent to anyone who has sent an email, accessed an Internet web page, or participated in a video telecommunication session. Data often travels at the speed of light in cyberspace. Adversaries attempt to exploit speed in all domains during wartime, but the speed-of-light capability of cyberspace provides an environment tailor-made for an intrusion of any sort. Experts in cyberspace can manipulate data and routing to hide their identity and location.[12] The non-attributable aspect of cyberspace offers a lush environment for an adversary to map networks, conduct espionage, and even modify data within US networks with little risk of retaliation.[13] Additionally, for the relatively low cost of a computer and an

Internet connection, a skilled adversary in cyberspace could conduct any and all their operations.[14] While increasing the scale of an adversary's cyberspace operation would create a larger threat, the low cost of entry into cyberspace combined with a capacity for non-attribution allows for threats to scale out as well (i.e., individuals, organizations, and countries that would otherwise not attempt intrusion or espionage against the US government may take the opportunity). Finally, the matter of information ownership must be addressed. While the US military often shares roads, ports, and airfields with commercial and civilian traffic, military installations are traditionally self-contained safe-haven environments for military-only operations. In most instances, a military installation commander, acting on behalf of the federal government, has some level of jurisdiction or authority to legislate and enforce laws on that installation.[15] Though military networks often contain boundaries to block certain traffic from entering the networks within an installation's geographic area, the essence of the cyberspace domain is information.[16] Informational traffic necessarily passes across the same wires and hardware as civilian data almost exclusively on privately-owned, government-leased lines cross-country.[17] In short, the military network and information paths cannot be completely physically separated from the private sector network. The lack of international law, potential speed of attack, capacity for non-attribution, breadth and depth of adversaries, and lack of clearly defined national borders, much less civilian versus military information, in cyberspace helps to explain the problems faced in defending and legislating cyberspace.

Despite the scare to Estonia and later exemplified in a similar Georgian event, there is "no universally legally binding instrument that would address cyber attacks as threats to national security."[18] However, the attacks in Estonia and Georgia clearly threatened security and peace-of-mind in those sovereign nations. The US has addressed the problem internally by assigning

the Department of Homeland Security as the caretakers of cyberspace within the US for domestic issues and assigning the Department of Defense as caretakers of cyberspace for military networks.[19] As described above, the delineations of what is of military interest and what is of Homeland Security interest are hidden in the confusion of cyberspace "borders." Posse comitatus, by law and for lack of a better system, creates a guideline.

Posse comitatus, Title 18, Section 1385 of the US Code reads, "whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both."[20] In short, the military may not conduct law enforcement operations. The translation of the law to cyberspace requires that whenever an intrusion on a military network is tracked back to a computer located within the United States, the military must stop its efforts and turn the information over to Department of Homeland Security (or other agency) personnel for further tracking and law enforcement actions.[21] This seems a simple and fair solution.

Within cyberspace, however, evidence of traveling through a geographic site does not mean that it originated from that site. The attack aimed at Estonia, for instance, is known as a distributed denial of service attack (DDoS).[22] Malicious code, developed allegedly in Russia, was released to the Internet, spread around the world through cyberspace, and affected computers without their owners knowing.[23] On demand, the "slave" computers sitting on desks around the world sent continuous communication requests to the targeted computers within Estonia, overwhelming their ability to respond.[24] Most owners of "slave" computers were likely unaware of their computer's role and the individuals themselves were also not complicit in the act. The problem, however, was very real to Estonia and was one to which they had to react. One

year later, when networks in Georgia were affected, the event preceded a Russian military assault on Georgia.[25] If such an event hit US military bases and the military tracked intrusion attempts and attacks to computers within the US, the military could take no action except attempt to block the offending computers and pass the information along to law enforcement.[26] Meanwhile, the attacks would continue and the US would get no closer to determining attribution.

United States Code offers a potential solution contained in the Insurrection Act in Title 10, Section 332 of US Code.[27] Initially established in 1807, the Insurrection Act allows the President to mobilize the armed forces within the US when "unlawful obstructions, combinations, or assemblages, or rebellion against the authority of the United States, make it impracticable to enforce the laws of the United States in any State by the ordinary course of judicial proceedings"…"to enforce those laws or to suppress the rebellion."[28] Actors in cyberspace are neither measured by their geographic location nor by positive identification raising both jurisdiction and attribution issues in the law. Furthermore, an intrusion or attack initiating outside the US is subject to no internationally recognized law today.[29] A distributed denial of service attack affecting a military installation likely offers no chance at legal resolution, no information about who was trying to attack, and potentially no lessons learned to combat the next attack. Thus, if the attack sufficiently degrades capabilities, the President could deem the attack "unlawful" or a "rebellion" allowing for the initiation of the Insurrection Act and further allowing the military to take necessary actions to put down the insurrection. However, the speed-of-light quickness associated with cyberspace and pure mass of intrusion attempts against US government computer networks suggests that Presidential approval would not be granted in a timely or consistent manner.

While subject to posse comitatus for network intrusion, the quality of the investigation relies on urgency and skills of the Department of Homeland Security or delegated local law enforcement and proper communication of the intrusion received from the Department of Defense. In the best of circumstances, an investigation is neither quick nor sufficient to provide lessons learned. At worst, military network investigations may be prioritized behind other departments' networks, public utilities, and economic and transportation system intrusions and the only success that may be claimed is persistence and survival through a network attack.

A military network active defense able to track intruders back to their origination in spite of their path, however, could make the networks drastically better.[30] Given rights modeled on the Insurrection Act of 1807, the military could both clear US civilians who were not complicit in an intrusion without a Homeland Security investigation, and track an intruder back to his originating source. The investigation could identify vulnerabilities in networked systems which could be turned into lessons learned and lead to better protected network technologies or training in the future. The investigation could also identify who wanted to intrude in US networks and potentially uncover reasons why resulting in valuable military intelligence.

Thomas Wingfield and James Michael have identified three legal prisms through which to view computer network intrusions: law enforcement, intelligence collection, or military operations.[31] Furthermore, they wrote that any given intrusion may have components of any two or all three aspects of law.[32] The dilemma, as spelled out by Major Bonnie Adkins, is in quickly discerning the type of attack and taking appropriate response.[33] Given the limitations of speed, anonymity, and jurisdictional confusion, legal action seems inappropriate as the initial response for at least some coordinated cyberspace attacks, such as those targeted at Estonia and Georgia. Rather, the US government, recognizing the criticality of the threat against national systems,

should allow its fighting force the ability to track and identify their attackers, regardless of the path the attackers chose. In the initial moments of a cyberspace intrusion, there is not time to haggle over jurisdiction. In the immediate moments thereafter, there is not time to investigate a criminal allegation against an American citizen while the adversary hides behind a slave machine in a path that invokes posse comitatus. Cyberspace intrusion attempts against the US military need to be defended and tracked to their source by US military as they are happening. The actions of the military would include a planned series of responses such as an immediate block of the far-end computer from the military network it is trying to connect to, tracking and localization through any slave machines back to the originating host, and placing a virtual tag on any US system for Department of Homeland Security to follow-up for potential legal action. Most importantly, the military would take action immediately to give US forces the best opportunity to survive a cyberspace attack and retaliate, if ordered.

The United States government has never been 1) so reliant on a single, specific technology for its everyday and warfighting posture, 2) so reliant on the private sector for its everyday and warfighting posture, and, perhaps most importantly to this argument, 3) so closely held at risk by its international enemies, as the military is within the cyberspace domain[34]. Additionally, never has a weapon with such great risk to United States forces been so easily accessible and ubiquitous as the tools of cyberspace warriors. Enemy troops massing on borders, enemy ships and submarines setting sail, and enemy airplanes scrambling provide clear warning of aggression in traditional domains. Cyberspace does not necessarily provide such clear warning; an enemy that has previously mapped a network within the United States likely needs only a few keystrokes to affect their target. Geographic location of the adversary is inconsequential to their capabilities; a home-grown team of hackers my affect military operations

by hacking utilities, plans carried on unclassified networks, or telephone systems, for instance, just as easily as individuals residing outside the country. Reliance on commercial entities, the borderless reality of the domain, and the global reach and speed of an enemy in cyberspace requires the United States to review its laws regarding posse comitatus as it relates to cyberspace. The United States military must be allowed to function without threat from inside its geographic borders or from the outside.

---

[1] Landler and Markoff, "Digital Fears."
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Convertino, DeMattei, and Kneirim, *Flying and Fighting*, 15.
[7] US Department of Defense, *National Military Strategy for Cyberspace*, vii.
[8] Schaap, "Cyber Warfare Operations," 125.
[9] JP 1-02, *DoD Dictionary*, 139.
[10] Hildreth, *Cyberwarfare*, 1.
[11] DCSINT, *Cyber Operations*, II-7.
[12] Ibid., II-3 – II-7.
[13] Ibid., II-3 – II-7.
[14] Ibid., II-3 – II-7.
[15] Judge Advocate General School, *Military Commander and the Law*, 105.
[16] JP 1-02, *DoD Dictionary*, 139.
[17] Brown, "Legal Propriety," 212.
[18] Tikk, et al., *Cyber Attacks*, 22.
[19] President, *National Strategy, ix*; Brown, "Legal Propriety", 222; US Department of Defense, *National Military Strategy for Cyberspace*, 1-2.
[20] USC 18, Section 1385, "Use of Army."
[21] Adkins, "Spectrum of Cyber Conflict," 19-21.
[22] Landler and Markoff, "Digital Fears."
[23] Ibid.
[24] Ibid.
[25] Schaap, "Cyber Warfare Operations," 145.
[26] Adkins, "Spectrum of Cyber Conflict," 19-21.
[27] USC 10, Section 332, "Use of Militia;" Wikipedia, "Insurrection Act."
[28] USC 10, Section 332, "Use of Militia."
[29] Tikk, et al., *Cyber Attacks*, 22.
[30] US Department of Defense, General Counsel, "An Assessment of Interenational," 20-25. The General Counsel discusses the legalities of implementing an active defense on networks and suggests that they may be considered for the most critical networks at the risk of unintentional active response to cross-border network actions.

[31] Wingfield and Michael, "An Introduction to Legal," 1-2.
[32] Ibid., 2.
[33] Adkins, "The Spectrum of Cyber," vii.
[34] Miller and Kuehl, "Cyberspace and the 'First Battle'," 1. The authors address the increased dependence of the military on other national infrastructures.

Bibliography

Adkins, Major Bonnie N. "The Spectrum of Cyber Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?" Maxwell AFB, Alabama: Air University, Air Command and Staff College, April 2001.

Brown, LtCol Todd A. "Legal Propriety of Protecting Defense Industrial Base Information Infrastructure." *Air Force Law Review: CyberLaw Edition*, Volume 64 (2009): 211-257. Accessed via: http://www.afjag.af.mil/library. 26 March 2010.

Convertino, Lt Col Sebastian M., II, Lou Anne DeMattei, and Lt Col Tammy M. Knierim. *Flying and Fighting in Cyberspace*. Maxwell Air Force Base, AL: Air University Press, 2007.

Deputy Chief of Staff for Intelligence (DCSINT) Handbook No. 1.02. *Cyber Operations and Cyber Terrorism.* US Army Training and Doctrine Command, Ft Leavenworth, Kansas. 15 August 2005.

Hildreth, Steven A. *Congressional Research Service Report for Congress No. RL30735: Cyberwarfare.* 19 June 2001. Accessed at: http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL30735_06192001.pdf on 29 March 2010.

Landler, Mark and John Markoff. "Digital Fears Emerge After Data Siege in Estonia." The New York Times. 29 May 2007. Accessed at: www.nytimes.com/2007/05/29/technology/29estonia.html on 29 March 2010.

President. *The National Strategy to Secure Cyberspace*. February 2003.

Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 12 April 2001 (Amended 31 October 2009).

Miller, Robert A. and Daniel T. Kuehl. "Cyberspace and the 'First Battle' in 21st-century War." Defense Horizons, Number 68 (September 2009): 1-6.

Schaap, Major Arie J. "Cyber Warfare Operations: Development and Use Under International Law." *Air Force Law Review: CyberLaw Edition*, Volume 64 (2009): 121-173. Accessed via: http://www.afjag.af.mil/library. 26 March 2010.

Tikk, Eneken, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharm, Lils Vihul. *Cyber Attacks Against Georgia: Legal Lessons Identified.* Written for Cooperative Cyber Defence Centre of Excellence, North Atlantic Treaty Organization. Tallinn, Estonia. November 2008.

USC Title 10, Section 332. "Use of Militia and Armed Forces to Enforce Federal Authority." Accessed via Internet on Cornell University Law School web page: http://www.law.cornell.edu/uscode/10/332.html Accessed 26 March 2010.

USC Title 18, Section 1385. "Use of Army and Air Force as Posse Comitatus." Accessed via Internet on Cornell University Law School web page: http://www.law.cornell.edu/uscode/18/1385.html Accessed 26 March 2010.

US Department of Defense. *An Assessment of International Legal Issues in Information Operations.* Washington, D.C.: Office of General Counsel, May 1999.

US Department of Defense. *The National Military Strategy for Cyberspace Operations (U).* Washington, D.C.: Chairman of the Joint Chiefs of Staff, December 2006.

Wikipedia. "Insurrection Act." http://en.wikipedia.org/wiki/Insurrection_Act. Accessed 26 March 2010.

Wingfield, Thomas C. and James B. Michael. "An Introduction to Legal Aspects of Operations in Cyberspace." Monterrey, California: Naval Postgraduate School, 28 April 2004.