THE AIR FORCE LAW REVIEW

CYBERLAW EDITION

VOLUME 64 2009

THE AIR FORCE LAW REVIEW

AFPAM 51-106

The Air Force Law Review is a publication of The Judge Advocate General, United States Air Force. It is published semiannually by The Judge Advocate General's School as a professional legal forum for articles of interest to military and civilian lawyers. The *Law Review* encourages frank discussion of relevant legislative, administrative, and judicial developments.

The Air Force Law Review does not promulgate Department of the Air Force policy. The opinions and conclusions expressed in this publication are solely those of the author and do not necessarily reflect the opinion of The Judge Advocate General, The Judge Advocate General's Corps, or any other department or agency of the United States Government.

The *Law Review* solicits contributions from its readers. Information for contributors is provided on the inside back cover of this issue.

Readers who desire reprint permission or further information should contact the Editor, *The Air Force Law Review*, The Judge Advocate General's School, 150 Chennault Circle, Maxwell Air Force Base, Alabama 36112-6418. Official governmental requests for free copies, not under the depository program, also should be sent to the above address.

Cite this Law Review as 64 A.F. L. REV. (page number) (2009).

Paid subscriptions to the Air Force Law Review are available from the Superintendent of Documents, U.S. Government Printing Office, Stop IDCC, Washington DC 20402.

Individual copies of this edition may be purchased through the U.S. Government Bookstore at http:// bookstore.gpo.gov or by phone at (866) 512-1800 (DC area (202) 512-1800). Email: contactcenter@gpo.gov. Fax: (202)-512-2104.

THE AIR FORCE LAW REVIEW

VOL. 64 **2009**

CYBERLAW EDITION

THE AIR FORCE LAW REVIEW

Authority to publish automatically expires unless otherwise authorized by the approving authority. Distribution: members of The Judge Advocate General's Corps, USAF; judge advocates of the Army, Navy, Marine Corps, and Coast Guard; law schools; and professional bar association libraries.

SOVEREIGNTY IN CYBERSPACE: CAN IT EXIST?

LIEUTENANT COLONEL PATRICK W. FRANZESE

Lieutenant Colonel Patrick W. Franzese (B.S., Washington University (1993); J.D., University of Minnesota (1996); M.A., Air Command and Staff College (2008);M.A., School of Advanced Air and Space Studies (SAAS) (2009)) is currently assigned to United States Strategic Command. He is a member of the Minnesota Bar. *This article is based on the author's SAAS thesis. The author thanks Dr. John Sheldon, Lt Col (Dr.) John Davis, Ms. Susan Turley, Capt Scott Hodges, and Capt Mark Rosenow for their valuable assistance and insights in creating this article. The author also wishes to thank his wife Christina and his children for their continuing love and support.*

I. INTRODUCTION

Imagine if 15 years ago a foreign analyst stated he could accomplish the following: (a) gain access to, and possibly alter, U.S. military plans; (b) monitor U.S. military operations and communications; (c) disable vital U.S. military command and control systems either immediately or at any chosen future moment; (d) target specific U.S. military personnel via their financial, medical, or family information; (e) seriously degrade, if not render wholly inoperable, some computer-dependent conventional weapons, thereby significantly negating the United States' conventional advantage; (f) strike at the United States' critical infrastructure such as financial markets, power plants and grids, communication nodes, and transportation systems; and (g) achieve this all non-kinetically, without being physically present in the United States, leaving the United States unable to trace these activities back to the potential adversary's country generally, or its military specifically. Fifteen years ago, his superiors would probably have summarily dismissed this plan as too far-fetched. Yet today, due to the rapid maturity and expansion of cyberspace and the extent to which it increasingly permeates every aspect of society, potential enemies of the United States could possibly accomplish every one of the scenarios listed above.

A. On-Going Cyberwar?

Every day, countries, organizations, and individuals are exploiting, or attempting to exploit, the opportunities and advantages that cyberspace offers, and the United States serves as a rich target for these endeavors. For example, on a single day in 2008, the Pentagon was "attacked" electronically six million times by people seeking access.[1] Although the Pentagon has not publicly provided specifics as to the number of successful intrusions, these attacks reportedly disrupted an internal e-mail system for two days.[2] Moreover, "[m]ultiple Congressional computers have been hacked from multiple Chinese locations."[3] This cyberwar, however, is not limited to government networks, computers, and computer systems. For example, an executive with one New York-based financial house said his company had been attacked one million times in a 24-hour period.[4] This staggering

[1] Ardaud de Borchgrave, *Silent Cyberwar*, WASH. TIMES, Feb. 19, 2009, *available at* http://www.washingtontimes.com/news/2009/feb/19/silent-cyberwar/.
[2] *Id.*
[3] *Id.*
[4] *Id.*

number of incidents underscores the threat the United States faces in cyberspace.

The United States, though, is not the world's lone cyberattack victim. In Britain, for example, e-mail across most, if not all, of the military was shut down in January 2009, after the discovery that a hybrid virus or worm infected their systems and sent e-mails to "IP addresses traced back to Russia."[5] In the summer of 2008, Canadian researchers discovered a large electronic spying operation that had infiltrated at least 1,295 computers in 103 countries—including many belonging to embassies, foreign ministries and other government offices—and stolen documents from hundreds of government and private offices.[6] Not only was the operation searching for particular important targets, but the software used had the capability to turn on the camera and audio recording functions of an infected computer, allowing individuals to see and hear what was going on in a room.[7] "Although the Canadian researchers said that most of the computers behind the spying were in China, they cautioned against concluding that China's government was involved. The spying could be a nonstate, for-profit operation, for example, or one run by private citizens in China known as 'patriotic hackers.'"[8]

In addition to infiltrating computer systems and gathering information, nations, organizations, and individuals have used cyberattacks to affect state behavior. Most notably Estonia, Georgia, and Kyrgyzstan were subjected to cyberattacks that significantly affected Internet service—and the corresponding government, banking and communication services, and operations—throughout those countries. These three cyberattacks demonstrate how outsiders can exploit cyberspace to influence state actions across a wide range of situations.

In 2007, the government of Estonia removed the Bronze Soldier, a statue of a Soviet soldier created as a memorial to the fallen soldiers of World War II, in their capital city Tallinn, prompting protests and riots by ethnic Russians living in Estonia. Coinciding with these public demonstrations was a cyberattack against Estonia, primarily in the form of a "DDoS, or Distributed Denial of Service, attack, where websites are suddenly swamped by tens of thousands of visits, jamming and disabling them by overcrowding the bandwidths for the servers

---

[5] Kevin Coleman, *UK Cyber Attack Reported*, DEFENSETECH.ORG, Jan. 20, 2009, http://www.defensetech.org/archives/004644.html (last visited Sept. 12, 2009).
[6] John Markoff, *Vast Spy System Loots Computers in 103 Countries*, N.Y. TIMES.COM, Mar. 29, 2009, http://www.nytimes.com/2009/03/29/technology/29spy.html (last visited Sept. 12, 2009).
[7] *Id.*
[8] *Id.*

running the sites."[9] "The main targets inside of Estonia were: the Estonian presidency and its parliament; almost all of the country's government ministries; political parties; three of the country's six big news organisations; two of the biggest banks; and firms specializing in communications."[10] While the cyberattack was largely traced back to Russia, questions still surround whether, and to what extent, the Russian government was involved.[11]

In 2008, Russia invaded Georgia over disputes in the Georgian provinces of South Ossetia and Abkhazia. Before the invasion by Russian forces, Georgia was subject to a cyberattack, once again primarily in the form of DDoS attacks. This attack spread after the physical fighting began, and the targets included government websites as well as media, communications, and transportation companies.[12] Overall, "Georgia, with a population of just 4.6 million and a relative latecomer to the Internet, saw little effect beyond inaccessibility to many of its government Web sites, which limited the government's ability to spread its message online and to connect with sympathizers around the world during the fighting with Russia."[13] Like Estonia's attack, the attack on Georgia largely originated from Russia, although again debate continues concerning whether, and to what extent, the Russian government was involved.[14] However, unlike Estonia, Georgia engaged in its own cyberattacks by initiating DDoS attacks against pro-Russian websites.[15]

Finally, in 2009, DDoS attacks resulted in two of Kyrgyzstan's four Internet service providers (ISPs) being shut down, taking as much as 80% of the Internet traffic to the West offline.[16] Again, while analysts agree that this cyberattack involved Russian computers, questions remain as to whether the Russian government was involved

---

[9] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN, May 17, 2007, *available at* http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

[10] *Id.*

[11] Borchgrave, *supra* note 1; *see also* Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FIN. TIMES, Mar. 11, 2009, *available at* http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html.

[12] John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES.COM, Aug. 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html (last visited Sept. 12, 2009).

[13] *Id.*

[14] Markoff, *supra* note 12; *see also* Borchgrave, *supra* note 1.

[15] Timothy L. Thomas, *The Bear Went Through the Mountain: Russia Appraises Its Five-Day War in South Ossetia*, 22 J. SLAVIC MIL. STUD. 31, 56 (2009).

[16] Danny Bradbury, *The Fog of Cyberwar*, THE GUARDIAN, Feb. 5, 2009, *available at* http://www.guardian.co.uk/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access.

and, if so, the extent of its involvement.[17] Moreover, experts disagree as to the purpose of the cyberattack. Many have speculated that Russia initiated the cyberattack as a means of coercing the Kyrgyz Government to close Manas Air Force Base, thus removing the United States military from Kyrgyzstan.[18] However, others believe that Kyrgyzstan's government actually initiated the cyberattack, using organizations within Russia to execute this attack, as a means of silencing government opposition.[19]

In sum, states, organizations, and individuals continually act in cyberspace to both probe networks and gather information on other actors. Actors are also continually realizing, developing, and exploiting the potential power of cyberspace to influence, and respond to, the actions of other states. States must thus focus on developing an appropriate framework that will address the multitude of issues raised by cyberspace.

B. International Law and Cyberspace

Currently, commentators analyzing cyberattacks emphasize questions such as the following: When does a cyberattack constitute "use of force" under Article 2(4) of the United Nations (UN) Charter?[20] When does a cyberattack constitute an "armed attack" under Article 51 of the UN Charter?[21] When can a state respond in self-defense with a cyberattack of its own? When can a state respond in self-defense with physical force to a cyberattack? And what is the appropriate, proportional response to a cyberattack?[22] The answers to these

---

[17] Robert Mackey, *Are 'Cyber-Militias' Attacking Kyrgyzstan?*, N.Y. TIMES NEWS BLOG, THE LEDE, Feb. 5, 2009, http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/?ref=asia (last visited Sept. 12, 2009).

[18] *Id.*; *see also* Christopher Rhoads, *Kyrgyzstan Knocked Offline*, WALL ST. J.COM, Jan. 28, 2009, http://online.wsj.com/article/SB123310906904622741.html (last visited Sept. 12, 2009) (discussing cyberattack against Kyrgyzstan).

[19] Rhoads, *supra* note 18; *see also* Posting of Jeffrey Carr to IntelFusion, *Why I Believe That the Kyrgyzstan Government Hired Russian Hackers to Launch a DDOS Attack Against Itself*, Jan. 30, 2009, http://intelfusion.net/wordpress/?p=520 (last visited Aug. 25, 2009) (discussing cyberattack against Kyrgyzstan).

[20] U.N. Charter art. 2, para. 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

[21] U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security . . . . ").

[22] *See, e.g.*, WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (Aegis Res. Corp. 1999); THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL

questions are important for guiding both how a state will respond to a cyberattack and, equally important, how a state will conduct its own cyber operations. Applying these questions to the cyberattacks discussed above demonstrates both the complexity of these issues and the need for resolution. Specifically, did Russia use force in gaining access to the UK military's e-mail? Was Estonia subject to an armed attack from Russia? Did Russia's actions before the actual invasion of Georgia provide Georgia the right to use force in self-defense? What is the appropriate response for governments victimized by China's spying operation? What responsibility do Russia and China have for monitoring and preventing cyberattacks originating from their respective countries? Finally, could Russia and China be held responsible for not preventing cyberattacks originating from their territory and, if so, how?

Unfortunately, no consensus has developed in answering these questions. More troubling, various commentators still hold widely divergent views on basic, fundamental questions. For example, they cannot even agree on a framework when addressing the question of when a cyberattack constitutes an act of war, armed attack or use of force ("act of war"). Some believe that for a cyberattack to constitute an act of war, it must "accompany a military offensive in the real world."[23] Others argue that cyberattacks cause "widespread harm."[24] Even these interpretations are somewhat ambiguous because people could hold varying opinions as to what exactly the terms "a military offensive in the real world" and "widespread harm" mean. Applying these ideas to the cyberattacks discussed above, some could argue that only Russia's attack on Georgia constituted an act of war because it accompanied a military offensive in the real world; however, others could argue that each cyberattack was an act of war because each attack caused "widespread harm," depending on how that term is defined.

While many scholars have provided insightful analysis of how cyberspace might fit under current international law, the current international legal paradigm predates cyberspace and cannot adequately address the various issues raised by cyberspace. Moreover, the rapid growth of cyberspace has outpaced the ability of nations individually, and the international community as a whole, to understand and control it. These facts, however, are not remarkable. With any new technology, either existing international law addresses the new issues or the law evolves with the new technology. Thus, the question becomes how to

---

SECURITY LAW IN CYBERSPACE (Aegis Res. Corp. 2000). Both books discuss in detail these types of questions and their interpretation of how international law applies.

[23] *Marching Off to Cyberwar*, ECONOMIST, Dec. 4, 2008, *available at* http://www.economist.com/sciencetechnology/tq/displaystory.cfm?story_id=12673385.

[24] *Id.*

determine the appropriate basis or framework from which the international community can begin to address the issues raised by cyberspace. The answer, this article proposes, is recognizing and establishing state sovereignty in cyberspace.

C. Why Is Sovereignty Important?

The sovereignty of the state forms the fundamental basis of the current international order, something that most scholars trace back to the Peace of Westphalia in 1648.[25] Under the current international order, the state is the traditionally recognized actor that engages in war, fashions alliances, enters into treaties, and both creates and populates international organizations such as the United Nations. In fact, a key principle of the United Nations, and its Members, is that the United Nations "is based on the principle of the sovereign equality of all its Members."[26] Preserving state sovereignty is a vital goal of both state-based international organizations and individual countries. For example, when Iraq invaded Kuwait in 1990, the UN Security Council authorized the use of force to, in part, "restore the sovereignty, independence, and territorial integrity of Kuwait."[27] In 1960, the Soviet Union shot down an American U-2 airplane flying over Soviet airspace because the Soviet Union claimed the U-2 had violated its sovereignty.[28] While not every violation of sovereignty will necessarily result in the use of force, state practice evidences that a state can use force to defend its sovereignty.[29]

Moreover, the United Nations often uses "sovereignty" in conjunction with the traditional phrasing of Article 2(4) of the UN Charter, which reads, "[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations."[30] Numerous UN Security Council and General Assembly resolutions concerning state conflict use the

---

[25] *See* DANIEL PHILPOTT, REVOLUTIONS IN SOVEREIGNTY : HOW IDEAS SHAPED MODERN INTERNATIONAL RELATIONS, ch. 5 (Princeton Univ. Press 2001) (asserting the Peace of Westphalia as the origin of modern international relations).

[26] U.N. Charter art. 2, para. 1.

[27] S.C. Res. 661, U.N. Doc. S/RES/0661 (Aug. 6, 1990); *see also* S.C. Res. 674, U.N. Doc. S/RES/0674 (Oct. 29, 1990), *and* S.C. Res. 678, U.N. Doc. S/RES/0661 (Nov. 29, 1990).

[28] *See* Oliver J. Lissitzyn, *Some Legal Implications of the U-2 and RB-47 Incidents*, 56 AM. J. INT'L L. 135 (1962) (which discusses the legal issues and implications of the U-2 incident).

[29] *See infra* notes 154-156 and accompanying text.

[30] U.N. Charter art. 2, § 4.

phrase "sovereignty, territorial integrity and political independence."[31] This underscores the fundamental role sovereignty plays in the current international order.

D. What Is Sovereignty?

While understanding the fundamental role of sovereignty is important, the more difficult task is defining exactly what constitutes sovereignty. Black's Law Dictionary states that sovereignty is "1. Supreme dominion, authority or rule. 2. The supreme political authority of an independent state. 3. The state itself"."[32] While informative, the definition is too general for the purposes of this article. Stephen Krasner, a renowned international relations professor, however, provides a more practical and useful explanation of sovereignty. He posits that sovereignty is usually conceptualized in four different ways:

> Domestic sovereignty, referring to the organization of public authority within a state and to the level of effective control exercised by those holding authority; interdependence sovereignty, referring to the ability of public authorities to control transborder movements; international legal sovereignty, referring to the mutual recognition of states; and Westphalian sovereignty, referring to the exclusion of external actors from domestic authority configurations.[33]

Krasner also states that there are a "bundle of properties associated with sovereignty-territory, recognition, autonomy, and control" that characterize states in the international system.[34]

Both constructs are useful when thinking about how cyberspace impacts sovereignty and whether sovereignty can exist in cyberspace. For example, cyberspace tests a state's interdependence sovereignty because it challenges a state's ability to control transborder movements. With the interconnectivity of cyberspace, a person sitting in Africa can "enter" the United States and conduct numerous innocuous activities such as shopping, correspondence, and electronic records retrieval

---

[31] *See, e.g.*, S.C. Res. 1680, U.N. Doc. S/RES/1680 (May 17, 2006); G.A. Res. 47/121, U.N. DOC. A/RES/47/121 (Dec. 18, 1992); S.C. Res. 1234, U.N. Doc. S/RES/1234 (Apr. 9, 1999).

[32] BLACK'S LAW DICTIONARY 1430 (8th ed. 2004).

[33] STEPHEN D. KRASNER, PROBLEMATIC SOVEREIGNTY: CONTESTED RULES AND POLITICAL POSSIBILITIES 6-7 (Colum. Univ. Press 2001).

[34] STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 220 (Princeton Univ. Press 1999).

"inside" the United States, which result in transferring information outside the United States. That same person can "enter" the United States and engage in harmful activities such as hacking into government computer systems, altering computer code, or disabling computer run systems, such as power grids, inside the United States. However, because cyberspace presents a challenge to sovereignty does not mean that a state is powerless to exert sovereignty in cyberspace. To the contrary, state sovereignty in cyberspace will not only require that a state receive recognition of its sovereignty in cyberspace from other states but also that it is able to exert some measure of control over its cyberspace. Chapter Three explores this last idea more fully.

It is important to understand that Krasner argues that his four concepts of sovereignty are often in tension and not all four concepts have to be present together for sovereignty to exist.[35] Additionally, he states that all political entities have never concurrently possessed all four types of sovereignty. [36] Thus, while Krasner's proffered concepts and properties give shape to what constitutes sovereignty and provide a useful method for discussion, they are not a strict checklist of prerequisites.

E. Definition

In discussing cyberspace, a common point of contention is the question of its definition. For the purposes of this paper, the definition set forth in Joint Publication 1-02, "DOD Dictionary of Military and Associated Terms," will suffice. It 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."[37] While the Internet is a subset of cyberspace, and the terms are not interchangeable, this article focuses heavily on the Internet. That said, the principles developed here apply not only to the Internet, but to cyberspace as a whole.

With an understanding of the threats and issues raised by cyberspace, as well as the important role that sovereignty plays in our international order, the next step is analyzing the role of sovereignty and cyberspace. The remainder of this article focuses on whether states can assert their sovereignty in cyberspace, how states might achieve it, and the obstacles that stand in their way. Section II of this article explores

---

[35] *See generally* KRASNER, *supra* note 33; KRASNER, *supra* note 34 (providing further discussion of these concepts).
[36] KRASNER, *supra* note 34, at 238.
[37] U.S. DEP'T OF DEF. JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS, 12 Apr. 2001 (Mar. 17, 2009).

two concepts commonly discussed when examining the issue of sovereignty and cyberspace. Specifically, it explores the idea that cyberspace is immune from state sovereignty and the idea that cyberspace is a global commons. While both these notions initially appear promising, they both break down when analyzing the requirements and implications each respective notion entails. Section III examines how sovereignty has developed, and continues to develop, in the other recognized domains of sea, air, and space. While sovereignty in each domain developed independently and is unique, the establishment of sovereignty in each domain shares many characteristics. Lessons from how sovereignty developed in these domains give insight as to how sovereignty in cyberspace might develop. Section IV considers four key obstacles to states asserting sovereignty in cyberspace. Specifically, states must recognize cyberspace is a sovereign domain, decide that exerting state sovereignty in cyberspace is in their strategic interests, manage civilian expectations of state sovereignty in cyberspace, and develop the technical capability to exert their sovereignty in cyberspace.

II. STATE SOVEREIGNTY IN CYBERSPACE AND THE GLOBAL COMMONS

The organizations, purpose, and people behind the creation of cyberspace heavily influenced what it is today. Specifically, the academics and scientists looked at cyberspace in romanticized terms, seeing the promise it held for all of humankind. This belief naturally affected how people considered the issue of sovereignty and cyberspace, which resulted in essentially two competing theories in lieu of the idea of state sovereignty. The first theory is that cyberspace is immune from state sovereignty. However, this theory ignores the fact that cyberspace needs the stability and regulation that state sovereignty provides, and states have a valid interest in exercising their control in cyberspace. The second theory is that cyberspace is a global commons. This theory, however, distorts the essence of a global commons and discounts the role states play in creating them.

A. Cyberspace Development

The military and scientists played large roles in the early, foundational development of cyberspace, and both groups brought their own divergent ideas on how it should develop. The military brought its values "such as survivability, flexibility, and high performance, over commercial goals such as low cost, simplicity, or consumer appeal."[38]

[38] JANET ABBATE, INVENTING THE INTERNET 5 (MIT Press 1999).

Conversely, academic scientists "incorporated their own values of collegiality, decentralization of authority, and open exchange of information."[39] Thus, cyberspace in many ways combined what the military wanted from it and what academics wanted it to be.

In the mid-twentieth century, academics such as educator Herbert McLuhan viewed technology and the interconnectedness that was possible via electronic media as a means of creating a "global village."[40] More significantly, some academics believed technology would actually spur an evolution in human consciousness. Because they equated consciousness with information, through interconnectedness, they reasoned that "human beings [would] become units of information, each contributing to this new world sentience."[41] Additionally, these academics thought that technology would help replace the industrial age that valued and promoted competitiveness with an information age that valued and promoted cooperation between humans. [42] In their minds, "the more information is shared, the freer society is, the greater the potential is for cooperation. Perfect cooperation reaps the same results as perfect competition, and without losers."[43]

To reach this nirvana, academics and scientists believed that governments and corporations should not control the emerging information technology. This notion encompassed the belief that whoever controlled the communication or information systems also controlled the message. As Abbie Hoffman, a prominent political activist during the 1960s and 1970s, stated, "Freedom of the press belongs to those that own the distribution system."[44] Therefore, the key to ensuring that individuals could truly share information was to have communication/information systems that were free from government and corporate interference.

B. State Sovereignty in Cyberspace

The belief that cyberspace should be free from government interference, or sovereignty, led to the idea that cyberspace is, in fact, immune from state sovereignty. Perhaps the one statement that embodies this concept more than any other was made by John Perry Barlow, a lyricist for the Grateful Dead and founding member of the Electronic Frontier Foundation, an organization dedicated to defending

[39] *Id.*
[40] ADAM BRATE, TECHNOMANIFESTOS: VISIONS FROM THE INFORMATION REVOLUTIONARIES 197-203 (Texere 2002).
[41] *Id.* at 199.
[42] *Id.* at 207-08.
[43] *Id.* at 208.
[44] *Id.* at 209.

civil liberties on the Internet. Back in 1996, in response to the Communications Decency Act, Barlow wrote "A Declaration of the Independence of Cyberspace," which began, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[45]

Despite the rhetorical flair of Barlow's declaration, there are five key reasons why cyberspace is not immune from state sovereignty. The first is that some entity must control cyberspace for it to exist and function. Cyberspace requires a physical structure, because without it, users have no access. That physical structure, however, is terrestrially based and thus naturally falls under the purview of the state where those physical assets sit. Additionally, cyberspace itself requires regulation and oversight.[46] For example, the Internet Corporation of Assigned Names and Numbers (ICANN) is an organization responsible for such vital matters as assigning domain names and IP addresses.[47] This needed oversight will only increase, moreover, as the number of users continues to rapidly expand.[48]

The second reason cyberspace is not immune from state sovereignty is that financial relationships in cyberspace need laws to govern those relationships and transactions. [49] If cyberspace was immune from state sovereignty, any financial relationship established in cyberspace would be tenuous at best and fraught with peril for either side. The fact that business decisions are heavily influenced by the laws

---

[45] John Perry Barlow, A Cyberspace Independence Declaration, http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration (Feb. 9, 1996) (last visited Aug. 25, 2009).

[46] *See* Internet Assigned Numbers Authority, Introducing IANA, http://www.iana.org/about/ (last visited Aug. 24, 2009) ("[w]hilst the Internet is renowned for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated").

[47] Internet Corporation for Assigned Names and Numbers, ICANN Factsheet, http://www.icann.org/en/factsheets/fact-sheet.html (last visited Aug. 24, 2009). While this body is under contract with the United States, the intent is that ICANN will ultimately turn into a fully independent organization.

[48] As early as December 1995, 16 million people or .4 percent of the world population used the Internet. By June 2009, almost 1.7 billion people or 24.7 percent of the World population, used the Internet. Internet Word Stats: Usage and Population Statistics, Internet Growth Statistics, http://www.internetworldstats.com/emarketing.htm (last visited Sep. 9, 2009).

[49] *See generally* JACK L. GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 29-46 (Oxford Univ. Press 2006) (Discussing how companies such as eBay needed laws to help operate their business and how the laws of states influence their business practices).

of a respective state, evidences that cyberspace is not immune from state sovereignty.[50]

The third reason cyberspace is not immune from state sovereignty is that content sent through cyberspace holds significance in the "real" world. While cyberspace ideally allows for the free flow of information, no "cyberspace exemption" shields information from the valid interests of the state where information is sent, received, or stored. For example, the United States, along with many other countries, has a stated interest in preventing the possession and spread of child pornography, France has a stated interest in stopping the spread of Nazi memorabilia, and Australia has a stated interest in protecting its citizens from defamatory statements.[51] In each of the examples above, court systems ruled that information accessible to the individual located in those respective states via cyberspace is subject to the laws within that respective state.[52] Accordingly, a website located outside of France, which sells Nazi memorabilia, that people can access from France, is subject to the laws of France.[53] While this area of the law is still developing, it demonstrates that states have valid interests in and legitimate control over what occurs in cyberspace.

The fourth reason cyberspace is not immune from state sovereignty is that states are increasingly required to assert their presence in cyberspace as a matter of national security. Whether by design or neglect, many states connect to and operate some of their critical infrastructure in or through cyberspace.[54] This has left those states, including the United States, increasingly vulnerable. As the *National Strategy to Secure Cyberspace* succinctly states:

> In peacetime America's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping U.S. information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the Nation's political

[50] *Id.*
[51] *Id.* at 147-61.
[52] *Id.*
[53] *Id.*
[54] For example, *The National Strategy to Secure Cyberspace* lists a number of critical infrastructures that are dependent upon cyberspace. These include: Banking and Finance; Chemical; Oil and Gas; Electric; Law Enforcement; and Transportation (Rail); and Water. U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE xiii (2003).
.

> leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems.[55]

Because the potential to cause harm in cyberspace is real and continues to grow, states cannot leave cyberspace ungoverned but must find a way to exert their control and authority to reduce their vulnerability.

As discussed above, a driving force behind the early development of the Internet were scientists who viewed the Internet as a means of cooperation for the betterment of humankind and "were assumed to be uninterested in abusing the network."[56] However, not everyone who uses the Internet today shares that same vision and many of those users see the Internet as a means to exploit other individuals, create chaos, gain an advantage over a competitor, or disseminate a specific message of hate or violence. Consequently, much like the "real" world which requires state sovereignty to regulate, protect, and punish various actors, cyberspace needs this sovereign influence as well. Furthermore, since states currently exploit cyberspace as a means of gaining a strategic and military advantage over another state,[57] states must exert their control as a matter of national security. The end result is that cyberspace is not immune from state sovereignty.

C. Global Commons

A second theory often put forth is that cyberspace is part of the global commons. Even some U.S. government publications promote this idea. Specifically, the 2005 *Strategy for Homeland Defense and Civil Support* states that "the global commons consist of international waters and airspace, space, and cyberspace."[58] Additionally, while the 2008 National Defense Strategy does not specifically define global commons, it references "information transmitted under the ocean or through space," when discussing global commons.[59] Even the National Strategy to Secure Cyberspace uses the word "global" 20 times when discussing the nature of cyberspace, while at the same time it fails to mention the word "sovereignty" even once.[60]

---

[55] *Id.* at viii.
[56] *Id.*
[57] *See supra* notes 1-19 and accompanying text for a discussion of these types of activities.
[58] U.S. DEP'T OF DEF., THE STRATEGY FOR HOMELAND DEFENSE AND CIVIL SUPPORT 12 (2005), *available at* http://www.defenselink.mil/news/Jun2005.
[59] U.S. DEP'T OF DEF., NATIONAL DEFENSE STRATEGY 16 (2008), *available at* http://www.defenselink.mil/news/2008%20national%20defense%20strategy.pdf.
[60] U.S. DEP'T OF HOMELAND SEC., *supra* note 54.

The preliminary question is how to define the "global commons." No universally accepted definition exists, and depending upon which dictionary or non-governmental organization one consults, a slightly different or nuanced definition appears. Most definitions, however, focus on natural resources that are not under the control of a specific nation.[61] Fortunately, within international governmental organizations, there is a bit more uniformity. Specifically, bodies within both the United Nations and the Organization for Economic Cooperation and Development (OECD) define global commons as "natural assets outside national jurisdiction such as the oceans, outer space and the Antarctic."[62] However, in analyzing this definition, it becomes clear that the oceans, outer space, and the Antarctic are not global commons simply because they are "natural assets outside natural jurisdiction." Rather, five similarities exist among them that evidence what it means to be a global commons.

First, international treaties govern each of these natural assets. The UN Convention on the Law of the Sea (Law of the Sea) entered into force in 1994, and, as of 19 December 2008, 157 countries have signed the treaty.[63] The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty) entered into force in 1967, and, as of 1 January 2008, 98 states have ratified the treaty and 27 additional states have signed onto it.[64] Finally, in 1959, 12 countries

---

[61] *See, e.g.*, World Resources Institute, The Global Commons, Overview, http://www.wri.org/publication/content/8393 (last visited Sept. 12, 2009) ("the global commons – those natural systems and cycles that underpin the functioning of ecosystems everywhere"); THE OXFORD POCKET DICTIONARY OF CURRENT ENGLISH, Encyclopedia.com, *Global Common*, http://www.encyclopedia.com/doc/1O999-globalcommon.html (last visited Sept. 12, 2009) ("any of the earth's ubiquitous and unowned natural resources, such as the oceans, the atmosphere, and space").

[62] Organization for Economic Co-operation and Development, Glossary of Statistical Terms, *Global Commons*, http://stats.oecd.org/glossary/detail.asp?ID=1120 (last visited Sept. 12, 2009); United Nations Statistics Division, Global Commons Definition, http://unstats.un.org/unsd/environmentgl/gesform.asp?getitem=573 (last visited Aug. 24, 2009).

[63] United Nations Division for Ocean Affairs and Law of the Sea, Chronological Lists of Ratifications of, Accessions and Successions to the Convention and the Related Agreements as of 20 July 2009, http://www.un.org/Depts/los/reference_files/chronological_lists_of_ratifications.htm#The United Nations Convention on the Law of the Sea (last visited Aug. 24, 2009). Note, the Law of the Sea built upon earlier conventions such as the Convention on the High Seas that entered into force on 30 September 1962.

[64] *See* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, *available at* http://www.oosa.unvienna.org/oosa/SpaceLaw/outerspt.html [hereinafter Outer Space Treaty].

signed the Antarctic Treaty, and 47 countries are currently party to the treaty.[65]

Second, each of these treaties addresses specific permissible uses and prohibitions for the natural asset. The Antarctic Treaty states, in part, that nations can only use the Antarctic for peaceful purposes, including scientific research, and specifically prohibits nations from testing nuclear weapons or disposing nuclear waste in the Antarctic.[66] Similarly, the Outer Space Treaty states, in part, that nations can only use the moon and other celestial bodies for peaceful purposes, including scientific research, and prohibits nations from launching any nuclear weapon or other weapon of mass destruction into orbit.[67] Finally, the Law of the Sea covers a broad range of issues ranging from a nation's transit rights, to a nation's ability to lay submarine cables and pipeline, to a nation's fishing rights on the high seas.[68]

Third, each of the treaties specifically addresses the issue of sovereignty. The Antarctic Treaty states, "No new claim, or enlargement of an existing claim, to territorial sovereignty in Antarctica shall be asserted while the treaty is in force."[69] The Outer Space Treaty states, "Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."[70] Finally, the Law of the Sea states, "no State may validly purport to subject any part of the high seas to its sovereignty" and "no State shall claim or exercise sovereignty or sovereign rights over any part" of the seabed and ocean floor and subsoil thereof, beyond the limits of national jurisdiction "or its resources."[71]

Fourth, each treaty bounds, or defines, areas of sovereignty and thus areas that constitute the global commons. Under the Antarctic Treaty, the global commons is defined as "south of 60 [degrees] South Latitude, including all ice shelves."[72] The Law of the Sea has a myriad of provisions precisely defining areas that constitute territorial waters where a state has sovereignty as well as other areas of state interest such

---

[65] Secretariat of the Antarctic Treaty, The Antarctic Treaty, http://www.ats.aq/e/ats_treaty.htm (last visited Sept. 12, 2009).
[66] *See* The Antarctic Treaty, Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 72, *available at* http://www.ats.aq/documents/ats/treaty_original.pdf.
[67] Outer Space Treaty, *supra* note 64.
[68] *See* United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS]. Not surprisingly, since nuclear powered ships and ships carrying nuclear weapons existed when nations created the Law of the Sea, there is no prohibition, or other restrictions, placed on nuclear weapons on the high seas.
[69] The Antarctic Treaty, *supra* note 66, at 74.
[70] Outer Space Treaty, *supra* note 64, at 208.
[71] *See* UNCLOS, *supra* note 68, arts. 89, 139.
[72] The Antarctic Treaty, *supra* note 66, at 76.

as an exclusive economic zone, thereby generally leaving the remaining oceans as a global commons.[73] Finally, under the Outer Space Treaty, the global commons essentially constitutes all of "outer space, including the Moon and other natural celestial bodies," although there is no specific definition of outer space provided in the Outer Space Treaty and thus no clear line between airspace and outer space.[74]

Finally, states could not realistically expect to exercise sovereignty over these areas when they established these treaties. Even if a nation wanted to assert sovereignty over the entirety of the oceans, outer space, or the Antarctic, no nation realistically could exert control or enforce its sovereignty over the entirety of these natural assets. As Section III will discuss, the areas where a state could reasonably exert sovereignty were not likely to end up as part of the global commons. As states gain the ability to exert sovereignty over portions of the global commons, and have a commensurate desire to do so, sovereignty over these areas will likely become an issue again.

Thus, the prerequisite to becoming a global commons is not that the area is a "natural asset outside natural jurisdiction." Rather, a global commons is something that has five unique characteristics. First, a global commons has a governing international treaty. Second, this treaty provides specific permissible uses and prohibitions of that global commons. Third, the global commons has boundaries and is definable. Fourth, nations have agreed to forgo, or at least leave unasserted in the case of the Antarctic, claims of exclusive sovereignty over any portion of the global commons. Finally, no single state is capable of controlling the global commons. In other words, a global commons is not the absence of sovereignty but rather the presence of a shared global sovereignty. With this understanding, categorizing cyberspace as a global commons is problematic because all five of these unique characteristics are not present with regard to cyberspace.

Many of the designers and creators of cyberspace viewed it as an intellectual nirvana free from the constraints of the "real" world. However, in reality, cyberspace is part of the "real" world and thus subject to its constraints and order—in other words, subject to state sovereignty. The idea that cyberspace is immune from state sovereignty is impractical. Cyberspace is based upon a physical architecture and needs regulation, thus allowing states to exert their control. In fact, as discussed above, states are beginning to exert control. Similarly, the idea that cyberspace is part of the global commons is flawed. Putting aside that cyberspace is not a natural asset, cyberspace currently lacks the defining characteristics of a global commons. Significantly, states

[73] *See generally* UNCLOS, *supra* note 68.
[74] *See generally* Outer Space Treaty, supra note 64.

would need to agree on shared sovereignty over cyberspace if they want it to be a global commons. While cyberspace is not immune from state sovereignty and is not a global commons, the question remains as to whether cyberspace could ever be free from state sovereignty or become a global commons. Although both options seem theoretically possible, the existence of an international order fundamentally based upon the concept of state sovereignty renders both options impractical. While Section III develops this answer, the basic reason is that states' competing interests, namely security, will ultimately cause them to want to assert control in cyberspace.

III. DEVELOPMENT OF SOVEREIGNTY IN OTHER DOMAINS

Cyberspace is subject to the constraints of the "real" world, which lacks shared global sovereignty over cyberspace, thus this article turns now to how individual states might achieve sovereignty in cyberspace. Because sovereignty in cyberspace will be an extension of territorial sovereignty, analyzing the development of sovereignty within the domains of air, sea, and space—domains that all sprang forth from territorial sovereignty as well—can provide insight into how sovereignty in cyberspace might develop. Due to the historical breadth of this subject, this examination remains within certain parameters. Specifically, the analysis focuses on broad chronological developments, the major notions of state sovereignty in the various domains, and the significant issues within each domain relevant to this article. From this examination, this chapter draws some insights into how states might achieve sovereignty in cyberspace.

A. Sea Sovereignty

By at least the second century BC, Roman law considered the seas to be *communes omnium naturali jure*, or common to all humankind.[75] Roman Emperor Justinian I (483-565 AD) wrote the earliest recorded statement on the law of the sea and in it "declared that the sea and its fish were available to all and no state could extend its jurisdiction beyond the shore, which was defined as the high-water mark."[76] Of course, this concept of the seas being common to all humankind was easy to follow since the Mediterranean Sea was essentially a "Roman lake" due to the empire's territorial borders.[77] With the collapse of the Roman Empire, other actors asserted their

[75] SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 76 (Island Press 1998).
[76] *Id.*
[77] GEORGE GALDORISI & KEVIN R. VIENNA, BEYOND THE LAW OF THE SEA: NEW DIRECTIONS FOR U.S. OCEANS POLICY 8 (Praeger 1997).

sovereignty over the oceans at varying lengths from their shores "based on some mix of the commercial aspect of the claims, national security, protection of fisheries, and collection of tariffs."[78] Anarchy, in which the strongest navy prevailed, essentially ruled the oceans until the late sixteenth century and early seventeenth century.[79]

Starting in the late sixteenth century and early seventeenth century, the debate over control of the seas was refined between those who championed *mare liberum*, or "open seas," and those who championed *mare clausum*, or "closed seas." Although many writers contributed to the development and promotion of these theories, Hugo Grotius remains the dominant figure, and open seas became the dominant theory. In his work *Mare Liberum*, Grotius "defended the freedom of the seas by arguing that the seas cannot be owned, that 'the sea is one of those things which is not an article of merchandise, and which cannot become private property. Hence it follows, to speak strictly, that no part of the sea can be considered as territory of any people whatsoever.'"[80] However, most jurists adopted the position that states "enjoy some rights to regulate in their own interests activities in the seas adjoining their coasts," something that even Grotius acknowledged.[81] By the end of the seventeenth century, the idea of a distinction between "high seas, free and open to all, and coastal waters susceptible to appropriation by the adjacent State" was well established, and by the beginning of the nineteenth century it was a respected principle of international law.[82] Some trace the "shrinkage of maritime sovereignty…to changed concepts of the value of the sea to the world community. Originally regarded as an avenue of plunder and as a buffer area separating national territories, by the comparatively peaceful nineteenth century the sea had come primarily to signify a medium of trade" and states financially benefited from the increased trade made possible by free seas and open trade routes.[83]

Although the idea of limited maritime sovereignty was established, "two matters remained unresolved: first, the question of the width of those waters . . . , and secondly, the question of the precise

---

[78] BUCK, *supra* note 75, at 76-77.

[79] GALDORISI & VIENNA, *supra* note 77, at 8; *see also* Note, *National Sovereignty of Outer Space*, 74 HARV. L. REV. 1160 (1961). The only brief respite during this period was the Treaty of Tordesillas in 1494 between Portugal and Spain that audaciously split the world between the two countries. Not surprisingly, as other countries' maritime capabilities grew, Portugal and Spain could not enforce the treaty. BUCK, *supra* note 75, at 77-78.

[80] GALDORISI & VIENNA, *supra* note 77, at 10.

[81] R. R. CHURCHILL & A. V. LOWE, THE LAW OF THE SEA 59 (rev. ed., St. Martin's Press 1988) (1983).

[82] *Id.* at 59-60.

[83] Note, *supra* note 79, at 1161.

juridical nature of coastal States' rights over the territorial sea."[84] With regard to the width of territorial waters, the most notable historic position was that of three miles, which, according to the generally accepted rationale, was the distance a cannon shot would carry,[85] and was approximately the line of sight from the shoreline.[86]

For approximately two centuries, countries disputed the width of territorial waters. Some states wanted to minimize territorial waters to maximize freedom of navigation for their merchant fleets and warships, while other states wanted to maximize territorial waters to control such activities as fishing and smuggling near their coasts.[87] By 1960, most states claimed the width of territorial waters was less than twelve miles, however, by the 1980s, "the great majority of States claimed territorial seas of twelve miles or more . . . . The steady shift towards wider territorial seas . . . is a reflection of the desire to bring coastal waters—and the fishing, pollution and so on conducted, often by foreign vessels, within them—under national control."[88] Moreover, the discovery of mineral resources, notably oil, under the seabed also led states to extend their claims of sovereignty.[89] Eventually, the Law of the Sea established the width of territorial waters at twelve nautical miles.[90] However, a handful of countries still claim different distances or have unique circumstances that affect the twelve nautical mile width.[91]

With regard to the second unresolved issue concerning the precise juridical nature of coastal states' rights, two broad approaches initially developed. The first "claimed that coastal States either had proprietorial rights in their territorial seas, or at least enjoyed sovereignty or plenary jurisdiction over them."[92] This approach emphasized the notion of sovereignty over territorial waters. The second approach argued for a slightly different rule:

---

[84] CHURCHILL & LOWE, *supra* note 81, at 60.
[85] GALDORISI & VIENNA, *supra* note 77, at 10.
[86] *Id.* at 31; *see also* INGRID DETTER DELUPIS, INTERNATIONAL LAW AND THE INDEPENDENT STATE (Crane Russak 1974). Not all states subscribed to the three-mile rule. For example, Scandinavian states claimed dominion over a fixed distance, which had narrowed to four miles by the mid-eighteenth century. CHURCHILL & LOWE, *supra* note 81, at 65; DETTER DELUPIS, *supra* note 86, at 31.
[87] CHURCHILL & LOWE, *supra* note 81, at 65-66; *see also* DETTER DELUPIS, *supra* note 86, at 31-36.
[88] CHURCHILL & LOWE, *supra* note 81, at 67.
[89] Note, *supra* note 79, at 1162.
[90] UNCLOS, *supra* note 68, at pt. II, § 2.
[91] CHURCHILL & LOWE, *supra* note 81, at 65-68.
[92] *Id.* at 60.

> States enjoyed only a 'bundle of servitudes' (*faisceau de servitudes*) over coastal waters, permitting them to exercise jurisdiction in the measure necessary for the protection of their interests, and accepted the corollary that if the existence of a right of jurisdiction were to be questioned the burden lay upon the coastal State to prove that it did exist.[93]

This approach emphasized that states had rights in adjoining waters, short of sovereignty, that varied depending upon the specific interest and purpose.

Despite the two competing positions, more and more states moved to assert sovereignty, although some states continued to claim separate jurisdictional zones for various purposes even into the twentieth century.[94] Eventually, the concept of sovereignty was universally accepted and codified, first in the 1958 Convention on the High Seas and then most notably in the United Nations Convention on the Law of the Sea. Article 2 of the Law of the Sea specifically states, in part:

> The sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea. This sovereignty extends to the air space over the territorial sea as well as to its bed and subsoil.[95]

The Law of the Sea also has four other significant provisions that bear upon state sovereignty. First, it allows for innocent passage of ships from all states through the territorial sea of the other states.[96] Second, the Law of the Sea recognizes additional zones, such as contiguous zones and exclusive economic zones, that may extend farther out than 12 miles and are not considered part of sovereign territorial sea.[97] Third, the Law of the Sea requires states to monitor and control ships that are flying under their flags. [98] Among other duties, the treaty requires each state to "maintain a register of ships containing the names and particulars of ships flying its flag." [99] Finally, the Law of the Sea

---

[93] *Id.* at 60-61.
[94] *Id.* at 60-62.
[95] UNCLOS, *supra* note 68, at pt. II, § 1.
[96] *Id.* at pt. II, § 3.
[97] *Id.* at pt. II, § 4, *and* pt. V.
[98] *Id.* arts. 91-95.
[99] *Id.* art. 94.

established the International Tribunal for the Law of the Sea (ITLOS) as a forum to settle disputes.[100]

B. Air Sovereignty

Roman civil law considered the air *res omnium communes*, or something that "was incapable of being the object of a private right" and thus common to all.[101] However, as property rights continued to develop throughout the centuries, Western thought treated the owner of the land as the owner of the air above it. This thought was expressed via the maxim "*cujus est solum, ejus est summits usque ad coelum,"* or "he who owns the soil owns it up to the sky."[102] However, with the beginning of the age of flight, the law quickly recognized that the idea of the landowner owning all the air above the land would lead to absurd results such as the concept of aerial trespass.[103] Thus, courts began to acknowledge the fact that at some point in the undefined "upper air," private ownership ended.[104]

Whereas the age of flight curtailed the idea of private ownership of air, it also brought on the concept of air sovereignty.[105] In response to German balloons, mostly piloted by military aviators, crossing French borders without regulation or permission, France requested and held the first diplomatic conference regarding aviation in 1910.[106] This conference considered the question of sovereignty, yet reached no agreement.[107] The prevailing views broke down into two main categories, those who supported freedom of the air and those who supported air sovereignty.

These categories were further broken down and summarized during a meeting of the International Law Association. Specifically, "freedom of the air" encompassed: (a) air freedom without restriction, (b) air freedom restricted by some special rights (not limited by height) of the subjacent states, and (c) air freedom restricted by a territorial

---

[100] *Id.* at annex VI.
[101] Charles Anthony Roberts, Air Sovereignty and International Law, at 5-7 (1959) (unpublished M.A. thesis, on file with Muir S. Fairchild Research Information Center at Maxwell Air Force Base, Alabama).
[102] *Id.* at 5.
[103] During the early 1900s, international organizations such as the Institute for International Law and the International Law Association examined and contemplated appropriate legal principles governing air. *Id.* at 9.
[104] *Id.* at 9-12.
[105] *Id.* at 30-33.
[106] *Id.* at 37; *see also* JOHN C. COOPER, *Legal Problems of Upper Space, in* EXPLORATIONS IN AEROSPACE LAW: SELECTED ESSAYS BY JOHN COBB COOPER, 1946-1966, ch. 14 (Ivan A. Vlasic ed., McGill Univ. Press 1968).
[107] Roberts, *supra* note 101, at 37.

zone.[108] "Air sovereignty" encompassed: (a) full sovereignty up to a limited height, (b) full sovereignty restricted by the right of innocent passage for aerial navigation, and (c) full sovereignty without any restrictions.[109]

Early in the age of flight, the increasing number of flight across the borders of European countries and across the English Channel forced resolution of the issue of air sovereignty. With no international agreement governing air, state practice began to establish international law regarding air sovereignty. Britain acted first, passing regulatory statutes in 1911 and 1913 that established its claim of sovereignty of the air over all of its land and territorial water and its ability to regulate any foreign aircraft within its jurisdiction.[110] Soon, other states took actions—such as formal declarations or shooting at airplanes that flew over their territory—that established the idea of air sovereignty over their respective land and territorial waters as well.[111] The actions of various states throughout World War I (WWI), especially neutral countries' refusal to allow overflight, firmly established air sovereignty as customary international law by the end of the war.[112]

Eventually, in 1919, 27 contracting parties signed the Convention for the Regulation of Aerial Navigation in France.[113] Commonly known as the Paris Convention, this convention codified the existing customary international law of air sovereignty. Article 1 stated, in part, "The high contracting parties recognize that every Power has complete and exclusive sovereignty over the airspace above its territory."[114] Equally as important, the Convention nominally established the idea that states had the right of innocent passage across the airspace and above the territory of other states.[115] This fundamental concept of air sovereignty continued, specifically with the Convention on International Civil Aviation, commonly referred to as the Chicago Convention, which states first signed in 1944 and have updated eight times, most recently in 2006.[116] Regardless of how the Convention changed over the years, Article I of the Chicago Convention has consistently stated, "[t]he contracting States recognize that every State

---

[108] *Id*. at 39.
[109] *Id*. at 39.
[110] *Id*. at 45-46.
[111] Roberts, *supra* note 101, at 46-48; *see also* DAVID H. N. JOHNSON, RIGHTS IN AIR SPACE 32 (Manchester Univ. Press 1965).
[112] Roberts, *supra* note 101, at 49-55; *see also* JOHNSON, *supra* note 111, at 32-33.
[113] Convention for the Regulation of Aerial Navigation, Oct. 13, 1919, 11 LNTS 173.
[114] *Id*.
[115] *Id*. arts. 2 & 15.
[116] *See* The Convention on International Civil Aviation, December 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295, *available at* http://www.icao.int/icaonet/dcs/7300.html .

has complete and exclusive sovereignty above its territory."[117] However, the Chicago Convention does not recognize the right of innocent passage as set forth in the Paris Convention. Nonetheless, the Chicago Convention does address such matters as overflight rights and aircraft nationality, and also established the International Civil Aviation Organization to govern these issues.[118] Significantly, the Chicago Convention also requires aircraft to be registered in a state and "bear its appropriate nationality and registration marks," and further requires that States provide registration and ownership information upon request.[119]

C. Outer Space Sovereignty

While states ultimately resolved the issue of state sovereignty in air, they left unresolved the question of how high sovereignty extended. The implicit solution was to simply apply the Roman maxim quoted earlier that "he who owns the soil owns it up to the sky" to international law. However, as rocket technology developed and the promise of satellites grew, so did questions as to how far up a state's sovereignty extended.

Some people advocated the theory that sovereignty extended infinitely; however, scholars dismissed this theory when considering both its application and the laws of planetary science.[120] First, because the Earth rotates on its axis and further revolves around the sun, humans have no ability to mark a fixed location in space. Moreover, if states could extend their sovereignty infinitely, the moon and other celestial bodies would effectively transfer from the sovereign territory of one state to the next as the various bodies rotated and revolved.[121] Finally, some recognized the fact that sovereignty can only truly exist if states can exert control, or sovereignty over the areas they claim.[122]

---

[117] The Convention on International Civil Aviation, *supra* note 116, part I, chap. I, art. 1.
[118] *Id*. at part II.
[119] *Id*. at part I, chap. III.
[120] GYULA GÁL, SPACE LAW 61-70 (Oceana Publ'n 1969).
[121] Additionally, as one commentator noted, "the idea of sovereignty over the various sectors of the universe is just as ridiculous as if the Island of St. Helena claimed the Atlantic Ocean." *Id.* at 67.
[122] Despite these obvious problems, experts from the two leading space powers in the late 1950s and early 1960s—the Soviet Union and the United States—nonetheless continued to advocate the notion that state sovereignty extended into outer space. Specifically, "Soviet commentators, while declaring that Soviet satellites have not violated international law . . . simultaneously claimed that Soviet airspace sovereignty extends to infinity" while the "Legal Advisor to the United States State Department in 1958 suggested that American sovereignty may extend upward for ten thousand miles, which is far beyond many present satellite orbits." Note, *supra* note 79, at 1167. Amusingly, a Soviet legal expert suggested, perhaps facetiously, that Sputnik did not pass over other states, but that other states passed under Sputnik as the Earth rotated.

As the international community began to generally accept the idea that sovereignty could not extend infinitely into the sky, it turned its focus to two important questions: determining the legal status of outer space and drawing the demarcation line between airspace and outer space. With regard to the legal status of outer space, many scholars drew an analogy from the high seas, arguing that the upper atmosphere, which like the high seas is beyond any state's control, is a zone of "open air."[123] Additionally, some scholars also looked back directly to the same principle of *res communis omnium* from Roman civil law that scholars also used when analyzing sovereignty in airspace and on the seas.[124] While not explicitly using the phrase "*res communis omnium*," state practice evidenced the belief that state sovereignty did not extend to outer space.[125] One authority noted that "(1) neither the United States nor the Soviet Union asked permission of other states before launching satellites over their territory, (2) no state has protested against such flights, and (3) the United Nations has passed certain resolutions in which the principle of national sovereignty in space is implicitly rejected."[126]

In 1967, the Outer Space Treaty solidified the legal status of outer space as free from sovereignty.[127] Article II of the Outer Space Treaty specifically states, "Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."

The Outer Space Treaty included other provisions that bear on sovereignty. Specifically, it made clear that states were responsible for "national activities in outer space . . . whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the

---

Philip W. Quigg, *Open Skies and Open Space*, vol. 37, no. 1 FOREIGN AFF., Oct., 1958, at 95.

[123] For example, G.P. Zadorozhny, a Soviet professor of international law, stated days after Sputnik's launch, "By analogy to the principle of freedom of the high seas, which beyond the limits of territorial waters and special maritime zones do not belong to anyone and are in general use by all nations, the upper atmosphere, which is beyond the limits of effective air control by states, can likewise be considered a zone of open air, in general use by all nations." Gál, *supra* note 120, at 117.

[124] *Id*. at 122-129.

[125] As John C. Cooper, a noted legal scholar in both air and space, stated in March 1958, "The course of international conduct since the satellite flights were announced is consistent with no theory other than the acceptance of the principle that 'outer space' is not part of the territory of any state and may be used by all states as freely as the high seas are now used for surface shipping." Quigg, *supra* note 122, at 97.

[126] *Id*. at 97-98.

[127] Article II states, "Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means." Outer Space Treaty, *supra* note 64.

provisions set forth in the present Treaty."[128] Moreover, a later convention, the Convention on Registration of Objects Launched into Outer Space, requires states to provide information on every space launch to an international body.[129]

While the Outer Space Treaty explicitly discusses sovereignty in outer space, it does not resolve the issue of the demarcation line between airspace and outer space. Theories for where the demarcation line should be range from the outer limits of earth's gravitational field, to the earth's atmosphere, to the point where aerodynamic lift cannot be sustained, to where states can no longer exercise effective control.[130] Generally, these theories can be broken down into one group that establishes a demarcation line based upon function and one that bases the demarcation line on distance.[131] More than half a century ago, the United Nations established a committee to try to resolve this issue—an effort that remains unsuccessful.[132] This failure led to attempts by some states to extend state sovereignty far into outer space. For example, in the Bogota Declaration of 1976, "eight equatorial countries tried . . . to lay claim on the geosynchronous orbits (22,300 miles above the equator)." The reasoning put forth by these countries was that the demarcation line should be located outside Earth's gravitation pull, which objects in geosynchronous orbit use.[133] However, the international community soundly rejected their claim.[134] More conspicuously, even though China ratified the Outer Space Treaty, an "increasing number of publications by influential Chinese authors (are) advancing the principle that China's sovereignty extends through outer space."[135] The Chinese rationale for extending sovereignty into outer

---

[128] *Id*. art VI.

[129] *See* Convention on Registration of Objects Launched into Outer Space, Jan. 14, 1975, 28 U.S.T. 695, 1023 U.N.T.S. 15.

[130] GÁL, *supra* note 120, at 70-98

[131] *See generally* Alexandra Harris & Ray Harris, *The Need for Air Space and Outer Space Demarcation*, 22 SPACE POL'Y 4 (2006).

[132] To help resolve this issue, the Committee on the Peaceful Uses of Outer Space (COPUOS), which the United Nations created in 1959, and its legal subcommittee established a working group on the "definition and delimitation of outer space." Despite decades of debate, the group had been unable to resolve this issue and is unlikely to do so in the near future. *See* United Nations Office for Outer Space Affairs, United Nations Committee on the Peaceful Uses of Outer Space, http://www.oosa.unvienna.org/oosa/COPUOS/copuos.html (last visited Sept. 12, 2009).

[133] Declaration of the First Meeting of Equatorial Countries, 3 Dec., 1976, *available at* http://www.jaxa.jp/library/space_law/chapter_2/2-2-1-2_e.html.

[134] *See* Harris & Harris, *supra* note 131; *see also* NATHAN C. GOLDMAN, AMERICAN SPACE LAW: INTERNATIONAL AND DOMESTIC 68 (2d ed., Univelt 1996) (1988).

[135] Peter A. Dutton, Associate Professor, China Maritime Studies Institute, China's Views of Sovereignty and Methods of Access Control, Testimony before the U.S.-China Economic and Security Review Commission, (Feb. 27, 2008), *available at*

space is that "there is no legally accepted definition of 'outer space' that defines the demarcation point at which territorial airspace ends and outer space begins."[136]

D. Insights for Sovereignty in Cyberspace

After examining the development of sovereignty in the sea, air, and outer space, five main insights emerge.

Insight 1: An International Regime is Needed for the Development of Sovereignty in Cyberspace

Like many other concepts, there are various definitions of what constitutes a regime.[137] However, again, Stephen Krasner provides a useful construct. Specifically, he defines a regime as "a set of implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations."[138] Krasner defines the key terms as follows. "Principles are beliefs of fact, causation, and rectitude. Norms are standards of behavior defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice."[139] Krasner continues with the key observation that "*[c]hanges in principles and norms are changes of the regime itself*. When norms and principles are abandoned, there is either a change to a new regime or a disappearance of regimes from a given issue-area."[140]

Applying these definitions and concepts to sea, air, and outer space reveals that the development of sovereignty in these domains corresponded to the development of an international regime. A basic breakdown follows in table form.

---

http://www.uscc.gov/hearings/2008hearings/written_testimonies/08_02_27_wrts/08_02_27_dutton_statement.php.

[136] *Id.*

[137] STEPHEN D. KRASNER, *Structural Causes and Regime Consequences: Regimes as Intervening Variables*, *in* INTERNATIONAL REGIMES 2 (Cornell Univ. Press 1983).

[138] *Id.*

[139] *Id.*

[140] *Id.* at 3-4 (emphasis in original).

	Principles	Norms	Rules/Procedures
Sea	The high seas should be open to every state, although states have valid territorial interests beyond their coasts	The sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea.	The Law of the Sea and ITLOS
Air	The air above a state is part of the territory of that state	Every state has complete and exclusive sovereignty over the airspace above its territory	Chicago Convention and ICAO
Outer Space	Outer space belongs to all humankind	Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.	Outer Space Treaty and COPUOS

Table. International Regime Breakdown

Moreover, if the principles or norms change in any of the respective regimes, the regime itself would almost certainly disappear or change. For example, if a state claimed sovereignty over the moon in outer space and could reasonably be expected to enforce its claim, the outer space regime would likely dissolve because the basic principle that outer space belongs to all humankind would no longer be valid. Alternatively, states could collectively establish a new regime encompassing a new sovereignty principle norm. For example, the new principle might be "states can claim sovereignty over the moon and other celestial bodies" and the new norm might be "outer space is not subject to national appropriation by claim of sovereignty, but the moon and other celestial bodies are."

Thus, for sovereignty in cyberspace to become a reality, states must form a consensus regarding the underlying principles and norms from which an international regime would merge. A possible principle might be "every state has a right to access cyberspace for peaceful purposes, but states have a valid interest in asserting and protecting their

sovereignty in cyberspace." Failure to agree on underlying principles and norms, however, will prevent an international regime from forming. This insight underscores one of Krasner's concepts of sovereignty stated in the introduction: to have sovereignty other states must recognize that sovereignty.[141]

Insight 2: State Interests Eventually Trump Initial Utopian Ideals

When states and individuals started developing the technological capability to enter the domains of sea, air, and outer space, strong arguments existed for each of these domains to remain free from sovereign control. However, state interests, such as trade and national security, combined with a state's technological capabilities, ultimately prevailed over these arguments and determined the current legal status of these domains.[142]

Similarly, cyberspace is still in its infancy, and like the infant stages of other domains, people are strongly advocating against government interference, and assertion of sovereignty, in cyberspace. However, as discussed in Section II, states are beginning to recognize and assert their interests in cyberspace. As states' interests crystallize and grow as technology merges and matures, states will likely want to exert more and more control in cyberspace. As a result, borrowing from the style of John Barlow[143]: *People of the Cyber World, you light speed stream of ones and zeros. I come from the Real World, the home of the state. On behalf of the present, I demand you follow our rules or you will not be welcome here. We have absolute sovereignty wherever you gather.*

Insight 3: State Practice Matters

While the determination of sovereignty in the areas of sea, air, and outer space ultimately required an international regime, state practice influenced those emerging international regimes. In the sea domain, most states did not exert control over the high seas, but established control, or at least made claims of sovereignty, extending into the seas from their coasts.[144] In the air domain, neutral states in WWI made it clear that warring states could not use their airspace and

[141] *See supra* notes 32-33 and accompanying text.
[142] *See supra* notes 75-136 and accompanying text. Of course, this means that a change in state interests or technological capabilities might change the legal status of these domains.
[143] Barlow, *supra* note 45 (with apologies).
[144] *See supra* notes 75-100 and accompanying text.

most states claimed absolute sovereignty over their airspace.[145] In the outer space domain, very few states made claims of sovereignty into outer space and few states claimed that another state's space objects orbiting in outer space violated their sovereignty.[146]

Currently, states are essentially silent on the issue of state sovereignty in cyberspace. Specifically, although a state can often determine a cyberattack's country of origin, rarely, if ever, does a state claim that the country violated its sovereignty. States, furthermore, are not publicly responding to cyberattacks, which could establish precedents in practice. As one commentator noted, a few years ago United States officials were hesitant to talk about cyberattacks for fear that doing so would acknowledge that an act of war occurred, which required a similar response.[147] However, recently U.S. officials are more open about cyberattacks and do not respond as if there is a requirement for "any sort of offline retaliation."[148] Ultimately, such practices will influence future attempts to establish sovereignty in cyberspace.

Insight 4: Identification of Actors in Domain is Vital

In each respective domain, the ability for a state to track and identify actors is a fundamental requirement. In the sea domain, most vessels traveling in international waters are required to register with a state. More significantly, the Automatic Identification System (AIS), "a maritime navigation safety communications system standardized by the International Telecommunication Union (ITU) and adopted by the International Maritime Organization (IMO)" recently became operational.[149] The AIS "provides vessel information, including the vessel's identity, type, position, course, speed, navigational status and other safety-related information automatically to appropriately equipped shore stations, other ships, and aircraft; . . . and exchanges data with shore-based facilities" and "similarly fitted ships."[150] In the air domain, aircraft are required to register with a state and that state must provide information on that aircraft when required. Additionally, aircraft carry transponders that provide in-flight information pertaining to

[145] *See supra* notes 105-119 and accompanying text.
[146] *See supra* notes 120-136 and accompanying text.
[147] Ben Worthen, *Is a Cyber Attack an Act of War?*, WALL ST. J., Aug. 14, 2008, *available at* http://blogs.wsj.com/biztech/2008/08/14/is-a-cyber-attack-and-act-of-war/.
[148] *Id.*
[149] U.S. Dep't of Homeland Sec., U.S. Coast Guard, The Navigation Center of Excellence, Frequently Asked Questions, http://www.navcen.uscg.gov/enav/AIS/AISFAQ.htm#1 (last visited Aug. 24, 2009).
[150] *Id.*

identification, location, and heading. Finally, in the space domain, states are required to provide the following information when launching an object into space: the name of launching state or states, an appropriate designator of the space object or its registration number, date and territory or location of launch, basic orbital parameters, and the general function of the space object.[151] Moreover, the state is responsible for the activities of non-governmental entities in outer space.[152]

With regard to cyberspace, the lack of attribution is one of the greatest difficulties surrounding cyber attacks. While a state can often trace cyberattacks back to a specific country and a specific ISP, it typically cannot identify the individual actor without help from the country of origin, if at all. As demonstrated in the other domains, a key to establishing sovereignty in cyberspace is gaining the ability to identify actors and thus trace back cyberattacks, or other acts in cyberspace, to specific individuals or computers. Thus, if an international regime forms regarding sovereignty in cyberspace, an agreement between states on the need to track and identify specific actors in cyberspace will likely also emerge. Section IV will examine briefly the question of whether this is feasible.

Insight 5: States Must Be Able to Exert Control

As stated in Section I, the ability to control both territory and transborder movements is an important factor in establishing sovereignty, and control played an important role in the development of sovereignty in all three domains.[153] In the sea domain, the concept of territorial waters developed, in part, from the capability of a state to fire a cannon from its shore, and the concept of "open sea" developed from the lack of capability of states to exert control over the high seas.[154] Moreover, states have proved capable of addressing violations of their territorial waters by using force against the violator.[155] In the air domain, states have the capability to track violations of their air sovereignty and have proved capable of using force against violators to

[151] Convention on Registration of Objects Launched into Outer Space, *supra* note 129, Article IV.
[152] *See supra* notes 128-129 and accompanying text.
[153] *See supra* notes 33-36 and accompanying text.
[154] *See supra* notes 84-91 and accompanying text.
[155] For example, in March 2007, Iran detained 15 sailors from the United Kingdom for allegedly entering Iran's territorial waters. Associated Press, *U.K. Says 15 Sailors Detained by Iranian Navy*, MSNBC, Mar. 23, 2007, *available at* http://www.msnbc.msn.com/id/17752685/.

enforce that sovereignty.[156] Finally, in the outer space domain, the inability of any state to exert any sort of control in outer space significantly contributed to The Outer Space Treaty, prohibiting the extension of sovereignty into outer space.[157] However, as states gain the technological ability to assert control in outer space, the current outer space regime may be changed significantly, or disappear altogether.[158]

Similarly, for sovereignty to develop in cyberspace, states must be able to exert control in cyberspace. As with the other domains, this encompasses the capacity of a state to protect its borders. More importantly, this also encompasses the capacity of a state to respond directly to any violation of that sovereignty. While the exact means a state would use to address a specific violation of its sovereignty in cyberspace is beyond the scope of this article, it is important to note that states defend their sovereignty in other domains by resorting to force and similar responses could be expected for violations of sovereignty in cyberspace.[159]

The development of sovereignty in the sea, air, and outer space domains were all distinct, yet shared significant similarities. These similarities, in turn, provide significant insights into how sovereignty can develop in the cyberspace domain as well. First, the development of sovereignty in cyberspace requires an international regime. Second,

---

[156] *See supra* note 111 and accompanying text. In addition to the U-2 incident in 1960 previously mentioned in Chapter One, numerous other incidents have involved the shooting down of military aircraft that violated, or at least allegedly violated, another state's sovereignty. *See supra* note 28 and accompanying text; JOHNSON, *supra* note 111, 70-74. The most notable recent cases involved the incident between the US Navy EP-3 and Chinese F-8 in which China alleged the aircraft was violating its sovereignty by conducting a reconnaissance mission over China's exclusive economic zone. EMBASSY OF THE P.R.C. IN THE U.S., U.S. SERIOUSLY VIOLATES INTERNATIONAL LAW (Apr. 15, 2001), http://www.china-embassy.org/eng/zt/zjsj/t36383.htm (last visited Aug. 27, 2009).

[157] *See supra* notes 120-22 and accompanying text.

[158] Unlike the other domains of land, sea, and air, no state has been compelled to use force to defend its sovereignty or sovereign interests in outer space. Additionally, no state has used force to defend its right to use outer space, nor has a state used force to assert its sovereignty in outer space. However, states have used force against objects (e.g., satellites) other states have placed in outer space. Specifically, China "has secretly fired powerful laser weapons designed to disable American spy satellites by 'blinding' their sensitive surveillance devices." Francis Harris, *Beijing Secretly Fires Lasers to Disable US Satellites*, TELEGRAPH, Sept. 26, 2006, http://www.telegraph.co.uk/news/worldnews/1529864/Beijing-secretly-fires-lasers-to-disable-US-satellites.html (last visited Aug. 27, 2009). This capability is in addition to the anti-satellite capabilities some countries are developing that destroy satellites. Thus, even though outer space is a global commons and state sovereignty does not extend into outer space, states are beginning to appreciate the need to both protect their space assets against force and to use force to respond to attacks against their space assets.

[159] Of course, what constitutes "use of force" in cyberspace is also a contested area. *See* SHARP, *supra* note 22; WINGFIED, *supra* note 22.

states must critically assess their interests in cyberspace, because those interests will eventually trump the desires of those actors who want cyberspace to remain free from state sovereignty. Third, current state practice regarding the concept of sovereignty in cyberspace, as well as how a state responds to violations of its sovereignty in cyberspace, will influence how, and if, an international regime governing sovereignty in cyberspace ultimately develops. Fourth, the capability to identify specific actors in cyberspace will become an important requirement. Finally, a state must be able to exert control of cyberspace and respond to those actors who violate its sovereignty in cyberspace.

IV. ISSUES CONFRONTING STATE SOVEREIGNTY IN CYBERSPACE

Using the insights gained from examining the development and limits of sovereignty in other domains, this chapter examines the practical considerations of attempting to establish state sovereignty in cyberspace. Specifically, states must address four significant issues before they can realize sovereignty in cyberspace.

A. Recognizing Cyberspace as a Sovereign Domain

The most fundamental issue facing the development of sovereignty in cyberspace is persuading states that cyberspace is a domain over which they can assert sovereignty. In 2006, the Secretary of Defense signed the *National Military Strategy for Cyberspace Operations*, which states, in part, that cyberspace is its own domain, along with the other recognized domains of land, sea, air, and space.[160] However, treating cyberspace as a separate domain is not without controversy. In fact, even some within the Department of Defense believe that cyberspace does not constitute a domain.[161] While important, the debate over whether cyberspace is technically a domain should not obscure the more fundamental fact that cyberspace is a human creation, and thus states can assert control over, and shape, cyberspace.

As discussed in Section II, cyberspace requires a physical architecture to exist, cyberspace needs governmental regulation to function effectively, and states are attempting to exert increasing control over cyberspace.[162] More importantly, "there is no intrinsic reason why

---

[160] *See* U.S. DEP'T OF DEF., THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS 3 (2006), *available at* http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf [hereinafter NMS-CO].

[161] *See* David R. Luber & David H. Wilkinson, *Defining Cyberspace for Military Operations*, 93 MARINE CORPS GAZETTE, Feb. 2009, at 40.

[162] *See supra* notes 46-57 and accompanying text.

cyberspace cannot be made more territorial."[163] As a "human creation," cyberspace and its foundational technology are political, "shap[ed] by social actions and institutions."[164] "Global digital networks have the features they do—of placelessness, anonymity, and ubiquity—because of politics, not in spite of them."[165] Therefore, regardless of beliefs about the cyberspace domain, states have the capability to transform it into a domain in which they can exert their sovereignty.

As discussed in the previous section, a state's current practices will influence its future ability to assert any claims of sovereignty in cyberspace. Thus, states must first accept that cyberspace is, or at the very least can be, a domain in which they can exert sovereignty. States must then take additional steps to shape cyberspace to make it easier for them to assert their sovereignty.

B. Wanting Sovereignty in Cyberspace

While recognizing that cyberspace is a domain where states can assert their sovereignty is a fundamental problem, the larger question is whether states even want sovereignty in cyberspace. Developing sovereignty ultimately requires an international regime with specific rules and procedures regulating state activity in that domain, including a requirement to identify and track transnational actors. Certain states, however, may oppose state sovereignty in cyberspace and the international oversight that results. Examining the possible motivations of the United States and China gives insight into this proposition.

An unfettered cyberspace offers the United States an enhanced potential to spread American, or democratic, ideals and virtues. As articulated in the 2006 *National Security Strategy* (NSS),

> The United States has long championed freedom because doing so reflects our values and advances our interests. It reflects our values because we believe the desire for freedom lives in every human heart and the imperative of human dignity transcends all nations and cultures. Championing freedom advances our interests because . . . promoting democracy is the most effective long-term measure for strengthening international stability, reducing regional conflicts, countering

[163] Geoffrey L. Herrera, Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space 12 (prepared for the 47th Ann. Int'l Stud. Ass'n Convention, Mar. 22-25, 2006), *available at* http://www.allacademic.com/meta/p98069_index.html.
[164] *Id*. at 11.
[165] *Id*. at 11-12.

> terrorism and terror-supporting extremism; and extending peace and prosperity.[166]

Considering these objectives, cyberspace generally, and the Internet specifically, provide the ideal medium for the United States to both spread democracy and engage in the battle of ideas. Because the United States believes that every human yearns to be free, securing a forum for the free expression and exchange of ideas to take place is a key means of spreading freedom. Thus, the United States can meet its objectives indirectly by advancing a free and open Internet.

While this is an idealistic view, evidence increasingly demonstrates that the Internet's impact furthers the interests of the United States. For example, the Internet has changed the interaction between the Chinese state and society by undermining the communist regime's monopoly of information and allowing for the formation of a "digitally mediated civic society;" providing a public space for civilians to engage in politics; and fostering public distrust of public institutions.[167] Despite these positive outcomes, China's political liberalization is not the same as political democratization, but it is still an important step towards political democratization, and one that the United States would find in line with its national security strategy.[168]

Iran is another country where the United States would consider cyberspace a positive influence. As of 2005, nearly 100,000 blogs had sprung up in Iran, and Iranians were increasingly relying on the Internet for news and opinion.[169] Moreover, after Iranian bloggers and online journalists were confined and tortured, public protests resulted in the release of many those arrested.[170] More recently, the Internet played a significant role in both organizing protests after the controversial Iranian

---

[166] GEORGE W. BUSH, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES 3 (2006), *available at* http://www.strategicstudiesinstitute.army.mil/pdffiles/nss.pdf. The NSS continues, "From the beginning, the War on Terror has been both a battle of arms and a battle of ideas—a fight against the terrorists and against their murderous ideology. . . . In the long run, winning the war on terror means winning the battle of ideas, for it is ideas that can turn the disenchanted into murderers willing to kill innocent victims." *Id.* at 9.

[167] YONGNIAN ZHENG, TECHNOLOGICAL EMPOWERMENT: THE INTERNET, STATE, AND SOCIETY IN CHINA 103-34 (Stan. Univ. Press 2008). Zheng concluded that the Internet "has played an important role in facilitating political liberalization [through collective action] in different aspects such as political openness, transparency, and accountability." *Id*. at 11.

[168] *Id.* at 186.

[169] Omid Memarian, *Internet Yearns to Be Free in Iran*, SAN FRANCISCO CHRON., Dec. 9, 2005, http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2005/12/09/EDG7VG4KK31.dtl (last visited Aug. 27, 2009).

[170] *Id.*

presidential election in June 2009 and showing the rest of the world the brutality with which the Iranian regime responded.[171]

While a free and open Internet greatly facilitates U.S. goals to spread democracy and freedom, a strong international regime regulating sovereignty in cyberspace, might provide states a greater opportunity and capability to control speech and the spread of information by allowing them to monitor cyberspace content and individual actors more closely. Moreover, the United States might also oppose state sovereignty in cyberspace because it views itself as the dominant cyber power that would benefit the most from a cyberspace free from state sovereignty.[172] While the media often reports about cyberattacks against the United States, news outlets seldom mention U.S. actions in cyberspace. However, the lack of news regarding U.S. activity in cyberspace does not mean the activity does not exist. For example, an article on the leak of an Osama Bin Laden video reported that a "commercial intelligence firm that specializes in intercepting al-Qaeda's Internet communications, often by clandestine means," uncovered "a security gap in the terrorist group's internal communications network" and learned of an upcoming Osama Bin Laden video.[173] While a commercial company was behind the leak, this example highlights how organizations within the United States are conducting cyberattacks against other computer networks, presumably in other countries.

China may also prefer to preclude state sovereignty in cyberspace because cyberspace offers China possible asymmetric advantages when confronting the United States. American experts note that cyberattacks "even the playing field" because the U.S. infrastructure relies so heavily on Internet and online technologies.[174] China apparently agrees with this assessment, believing that U.S. dependency

---

[171] *See e.g.*, Patrick Quirk, *Iran's Twitter Revolution*, FOREIGN POL'Y IN FOCUS, June 17, 2009 (discussing the influence of technology in the aftermath of the 2009 Iranian presidential election), http://www.fpif.org/fpiftxt/6199 (last visited Sept. 10, 2009).

[172] Moreover, the United States is open about its belief that it has advantages in cyberspace and promoted this belief in the *National Military Strategy to Secure Cyberspace* (NMS-CO) when it stated, "the United States currently enjoys technological advantages in cyberspace."[172] Although the NMS-CO went on to state that "these advantages are eroding," the fact remains that the United States believes it has the advantage. NMS-CO, *supra* note 160, at 9.

[173] Joby Warrick, *U.S. Intelligence Officials Will Probe Leak of Bin Laden Video*, WASH. POST, Oct. 10, 2007, at A13, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/10/09/AR2007100902055.html.

[174] William Matthews, *Security Experts: Cyberattacks Will Increase*, A.F. TIMES, Nov. 4, 2008 (quoting Howard Schmidt, a former cybersecurity adviser to the White House), http://www.airforcetimes.com/news/2008/11/airforce_cyberattacks_110408/ (last visited Aug. 27, 2009).

on information technology "constitutes an exploitable weakness."[175] Four main reasons motivate the Chinese: the comparatively low costs of cyber operations, the difficulty of tracing a cyberattack's source, the chaos such attacks can create, and the "underdeveloped legal framework to guide responses."[176] Thus, establishing state sovereignty in cyberspace could restrict Chinese freedom of action in this militarily relevant domain.

Furthermore, state sovereignty in cyberspace might also force a degree of openness that China does not want. Examining the development of sovereignty in sea, air, and outer space shows that the respective regimes acknowledged some form of innocent passage or made allowances for the transborder movement of other states.[177] Transferring this concept to cyberspace, developing sovereignty might require agreed-on rules and procedures for when and what type of content or information can pass through cyberspace, across borders, and directly to the citizens of each state. As Article 19 of the Universal Declaration of Human Rights states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[178] Thus, any international regime regarding cyberspace might incorporate these values; something that China might oppose.

Finally, both the United States and China may now prefer cyberspace without sovereignty because cyberspace capabilities

---

[175] U.S.-CHINA ECON. AND SECURITY REV. COMM'N, 2008 ANNUAL REPORT TO CONGRESS 166 (2008), *available at* http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf.
[176] *Id*. at 167.

> China is likely to take advantage of the U.S. dependence on cyber space for four significant reasons. First, the costs of cyber operations are low in comparison with traditional espionage or military activities. Second, determining the origin of cyber operations and attributing them to the Chinese government or any other operator is difficult. Therefore, the United States would be hindered in responding conventionally to such an attack. Third, cyber attacks can confuse the enemy. Fourth, there is an underdeveloped legal framework to guide responses.

Id.
[177] Specifically, as discussed earlier, states are sovereign in their territorial waters, but ships from other states have a right of innocent passage in those territorial waters. *See supra* note 96 and accompanying text. Moreover, states have sovereignty in the air above their territory, but the regime also provides rules and procedures governing how airplanes from one state can enter and traverse the airspace of another state. *See supra* note 118 and accompanying text.
[178] Universal Declaration of Human Rights, G.A. Res. 217A, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc. A/810 (Dec. 12, 1948).

continue to grow and neither state wants to prematurely limit future operations. With the continual expansion of cyberspace's potential and capability, states might want to wait to enter agreements that define acceptable and prohibited activity until they obtain a better understanding of cyberspace's strategic potential. While states can withdraw from international agreements, such actions are not without some costs.

In sum, the United States and China may have valid reasons for not wanting sovereignty in cyberspace to exist, reasons that other states may share. Although no one can predict the conditions under which an international consensus towards sovereignty in cyberspace might evolve or how long that development might take, the process will begin only after more and more states realize that cyberspace is a domain where they can exert sovereignty and that it is in their interests to do so.

C. Civilian Expectations

Another challenge to state sovereignty in cyberspace comes from global views regarding the ability to access the Internet freely and anonymously. For example, a French measure to cut off Internet connections to individuals who persisted in illegally downloading movies and music recently passed only after early defeats and vocal opposition.[179] Additionally, a European Union directive that would "require all Internet service providers to retain information on email traffic, visits to websites and telephone calls made over the Internet, for 12 months" prompted outraged response from various privacy groups over its gestapo-like intrusions.[180] If states were to impose sovereignty in cyberspace, they would require greater identification of cyberspace actors. That in turn would likely result in a large outcry from individuals who presume that anonymous activity in cyberspace is both

[179] Many members of the National Assembly skipped the initial vote on the measure, which had always been unpopular with ordinary voters, and it was initially defeated in what some characterized as a "victory for the citizens and the civil liberties over the corporate interests." Eric Pfanner, *France Rejects Plan to Curb Internet Piracy*, N.Y. TIMES.COM, Apr. 9, 2009, http://www.nytimes.com/2009/04/10/technology/internet/10net.html (last visited Aug. 27, 2009). Ultimately, the National Assembly, which Sarkozy's party controls, passed the measure in a later vote, though lawsuits are expected. AFP, *French Parliament Adopts Tough Internet Piracy Bill*, May 12, 2009, http://www.google.com/hostednews/afp/article/ALeqM5i1XOUmbCAIkSpiwtCgSncSr2mtkw (last visited Aug. 27, 2009).

[180] David Barrett, *Internet Records to be Stored for a Year*, TELEGRAPH, Apr. 5, 2009, http://www.telegraph.co.uk/scienceandtechnology/technology/technologynews/5105519/Internet-records-to-be-stored-for-a-year.html (last visited Aug. 27, 2009). Various privacy groups were outraged, with one group even stating, "[t]his is the kind of technology that the Stasi [the secret police of East Germany] would have dreamed of." *Id.*

a current reality and a right. Despite a state's interests in establishing sovereignty in cyberspace, individuals also have valid privacy interests that must be accounted for, and protected, by any international regime.

D. Technical Issues Regarding Sovereignty

Finally, states face numerous technical challenges in attempting to impose sovereignty in cyberspace. While the detail of these technical challenges is outside the scope of this article, they do exist, but so do solutions. This section briefly addresses two issues and provides possible solutions. First, creating a system that can specifically identify actors in cyberspace is a daunting task. One possible solution is something akin to the DOD's common access card (CAC), which members use to log into DOD computer systems and also allows tracking in cyberspace.[181] Similarly, the state, or some other designated organization, could issue a specific CAC that the individual must use to gain access to an ISP that can access information from other states. Alternatively, users wanting to access the Internet globally could be required to use a biometric scanner before continuing. In either situation, states—or a designated international body established as part of an international cyberspace regime—could then trace back the illegal movements of specific actors in cyberspace.

The second issue is that states must also be able to establish a cyberspace border that a state can both monitor and control. Without the capability to perform this function, the concept of sovereignty in cyberspace is meaningless. One approach is to establish Internet border inspections similar to the physical border crossings that exist today.[182] This approach relies on the limited number of entry and exit points that route Internet traffic in and out of the United States. Thus, the United States could perform basic searches looking for specific IP header information such as IP addresses.[183]

While these solutions are far more complex than discussed here, still, "there is no intrinsic reason why cyberspace cannot be made more territorial."[184] States have the power to shape cyberspace in a manner that makes both actor identification and border control easier. While overcoming these technical issues is daunting in terms of technical

[181] *See* DoD Common Access Card, Welcome to the Next Step in Homeland Security, http://www.cac.mil/ (last visited Sept. 12, 2009).
[182] Captain Oren K. Upton, Asserting National Sovereignty in Cyberspace: The Case for Internet Border Inspection (June 2003) (unpublished M.A. thesis, Naval Postgraduate School), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA417582&Location=U2&doc=GetTRDoc.pdf.
[183] *Id*. at 45-55.
[184] Herrera, *supra* note 163.

ability and cost, the costs of not having sovereignty in cyberspace is daunting as well. For example, the cost of defending the DOD against cyberattack in a recent six-month period was more than $100 million.[185] More importantly, the cost to the United States of a successful cyberattack against its critical infrastructure could be in the billions or more. Thus, overcoming these technical issues is worth the investment.

States must overcome a number of problems to make sovereignty in cyberspace a reality. This chapter addressed four problems, although there are numerous more—both known and unknown. The technical problems highlighted here are probably the least problematic of the four; if states want sovereignty to exist in cyberspace, then they will find a way to overcome the technical difficulties. Moreover, influencing states to recognize cyberspace as a domain and persuading individuals to accept greater control in cyberspace may also be challenging. However, perhaps the greatest obstacle facing sovereignty in cyberspace is from states that do not want state sovereignty in cyberspace and the international regime governing cyberspace that would need to emerge.

V. CONCLUSION

Without question, cyberspace offers staggering possibilities to mankind. Individuals and states have correctly seized upon these possibilities and flung themselves into cyberspace, looking to take advantage of its opportunities and leverage its capabilities. Unfortunately, this rush into cyberspace created significant vulnerabilities—military, economic, and social—that individuals, organizations, and states alike continue to exploit. As with other technologies, individual states and the international community as a whole must catch up to cyberspace in terms of creating laws and institutions that can regulate, protect, and punish activity in cyberspace. The fundamental step that states need to take is recognizing and establishing state sovereignty, the foundational principle of the current international order, in cyberspace.

While examining the possibilities for sovereignty in cyberspace, states must realize that cyberspace neither is immune from state sovereignty nor can it be considered a global commons. Moreover, the development of state sovereignty in the sea, air, and outer space domains offers insights as to how state sovereignty might develop in cyberspace. A major insight is that an international regime is needed to

[185] Jim Garamone, *Cyber Defense Cost Pentagon $100 Million in Six Months, Officials Say*, AM. FORCES PRESS SERVICE, Apr. 8, 2009, *available at* http://www.defenselink.mil/news/newsarticle.aspx?id=53852.

successfully extend state sovereignty beyond a state's territorial area to these other domains. While a number of issues confront the development of state sovereignty, the main obstacle is the states' belief that sovereignty in cyberspace and an international regime governing cyberspace might be contrary to their best interests.

The key question thus becomes what the United States should do with regard to establishing state sovereignty in cyberspace. While the United States might have much to gain from operations in cyberspace, it may also have the most to lose. Specifically, cyberspace provides states and non-state actors the opportunity to negate the United States' conventional military advantage, circumvent its natural boundaries, and directly attack critical infrastructure inside the United States. Yet, problematically, when the United States views cyberspace, it sees a domain in which it needs to conduct military operations instead of a domain that it could shape, either on its own or collectively within the international community.

The United States could take several practical steps to develop the concept of sovereignty in cyberspace unilaterally, multilaterally, and internationally. Unilaterally, the United States could unequivocally declare that it considers its cyberspace to be part of its sovereign territory. To support this declaration, the United States can assert control over its cyberspace borders by creating a means to block traffic from ISPs or countries from which cyberattacks originate. More importantly, the United States can send a clear message to the world about cyberattacks as it has with terrorist attacks. The United States stated that it makes "no distinction between those who commit acts of terror and those who support and harbor them."[186] It could do the same by stating that it will not distinguish between those who commit cyberattacks and those who support and harbor them.

Multilaterally, the United States could reach agreements with other countries to recognize state sovereignty in cyberspace, to assist each other in tracing cyberattacks to their original sources, to identify the specific actors responsible for those cyberattacks, and to either prosecute or extradite those individuals responsible for the cyberattacks. Internationally, the United States could work within such organizations as the United Nations to establish common cyberspace principles and norms to form building blocks for a cyberspace regime. The key to these efforts—both multilaterally and internationally—is not only focusing on state actors in cyberspace, but on non-state actors as well. As expressed by Michael Chertoff, former Secretary of Homeland Security, "The modern international legal order must be predicated on a new principle, under which individual states assume reciprocal

[186] BUSH, *supra* note 166, at 12.

obligations to contain transnational threats emerging from within their borders so as to prevent them from infringing on the peace and safety of fellow states around the world."[187]

The United States can choose to take the lead in recognizing and establishing state sovereignty in cyberspace. By establishing state sovereignty in cyberspace, the United States, as well as every other state, will develop the framework to consider other cyberspace issues. Any resulting cyberspace regime will set forth acceptable activity in cyberspace, help identify and track harmful threats, and establish appropriate forums to address cyberspace issues. Alternatively, the United States can choose to continue its *ad hoc* responses to developments in cyberspace, hoping to maintain its advantage, and hoping that no other state or non-state actor will be able to attack the United States via cyberspace successfully and devastatingly. Of course, hope is not a strategy.

[187] Michael Chertoff, *The Responsibility to Contain: Protecting Sovereignty Under International Law*, vol. 88, no. 1 FOREIGN AFF., Jan./Feb. 2009, at 130, 131.

NON-INTERVENTION AND NEUTRALITY IN CYBERSPACE: AN EMERGING PRINCIPLE IN THE NATIONAL PRACTICE OF INTERNATIONAL LAW

LIEUTENANT COLONEL JOSHUA E. KASTENBERG

Lieutenant Colonel Joshua E. Kastenberg (B.A., University of California, Los Angeles (1990); J.D., Marquette University (1996); LL.M., Georgetown University (2003)) is the Staff Judge Advocate, 332d Air Expeditionary Wing, Balad Air Base, Iraq. Prior to his current assignment, he served as Staff Judge Advocate, Joint Task Force-Global Network Operations, a standing joint task force under the command of United States Strategic Command. Under the Unified Command Plan, it is the sole cyber-defense operational command for the Department of Defense. He is a member of the Wisconsin Bar.

I. INTRODUCTION[1]

Of all the recent legal literature examining the role of nations and corporations in cyberspace, very little has been devoted to the relationship between state-sponsored information operations—the roles and uses of cyberspace in interstate conflict—and neutrality. Most of the legal scholarship has been devoted to applying the laws of war to cyberspace operations. Issues such as proportionality, lawful targeting, and when an action constitutes a hostile act, appear to have taken preeminence over other matters. This article departs from that construct and addresses a related and equally important issue: the enforcement of neutrality in cyberspace. The United States will not always be a party to a conflict, and the executive branch's official stated policy may be to adhere to a position of non-intervention or even strict neutrality.

Admittedly, unlike in mid-twentieth century conflicts, it has become increasingly difficult for a state to regulate commerce, particularly electronic commerce, because of the internationalization of global business and the worldwide transit of electronic information across cyberspace. At present, roughly eighty percent of the Internet traffic traverses through the United States, chiefly through servers owned by private enterprise.[2] As a result, transactions which occur between London and Tokyo will still likely travel through the United States. Electronic information which flows through cyberspace is unlike any other type of physical transaction. Physical mails and shipped goods may leave London and reach Tokyo without ever traversing the geographic territory of a third state. Even an undersea telephone wire cable theoretically enables a predictable flow between two points, without transiting a third state.

Historically, national governments tried to remain neutral in third-party conflicts because conflict eroded commerce and the addition of interested states into a conflict tended to lengthen wars, thereby increasing the loss of lives. Neutrality, as discussed below, was recognized as a set of behavioral norms that limited the damage of warfare to warring states, notwithstanding commercial losses attendant with warfare. The United States, since its existence, has both recognized the importance of neutrality principles and demanded that other states act similarly. But, while it is well-understood that the behavioral requirements of neutral states are usually enforceable in the

---

[1] This issue was first addressed by Colonel Steven Korns and (then) Major Joshua Kastenberg in *Georgia's Cyber Left Hook*, PARAMETERS, 2008, at 60. The author thanks Colonel Korns for his insight and assistance in developing the concepts of cyber neutrality further. Sections of this law review article incorporate themes from the article in Parameters. However, the intended audience here is practitioners of operations law.

[2] *See, e.g.*, GABRIEL WEIMANN, TERROR ON THE INTERNET: THE NEW ARENA, THE NEW CHALLENGE 183-87 (2005).

physical realm, the advent of cyberspace makes this more difficult, particularly in the realm of information and electronic warfare.

The executive branch of the United States, with legislative checks, is the arm of government charged with determining and enforcing foreign policy. The executive branch may conclude that it is not in the best interests of the nation to remain fully neutral. Certainly, the enforcement of neutrality in cyberspace has not yet occurred, and there appears to be no policy for enforcement. This article suggests a rubric using existing laws for exerting executive authority.

Section I of this article discusses the emergence of conflict in cyberspace. Importantly, this article does not address either criminal enforcement or a state's duty in that realm but instead focuses on the executive branch's authority to enforce neutrality in cyberspace. Section II provides a basic rubric of neutrality rules as applied to conflict in cyberspace. Section III analyzes the most recent cyber-conflict, the Georgian-Russian War of 2008, and the potential consequences the United States risked because it lacked a cyber neutral position. Finally, the article concludes with an assessment of the need for a greater exertion of authority from the executive branch to police cyberspace. Importantly, this article does not advocate that the United States must take a wholly neutral position in conflicts which do not involve it. However, the executive branch should make clear that it has the authority to enforce cyber neutrality when it is determined by that branch to be necessary to national policy.

II. EMERGENCE OF CYBER WARFARE

Although the concept of cyber warfare is not new, since 2005 there has been an escalation of proxy conflict within cyberspace, particularly in two notable instances. In 2007, the Estonian government suffered cyber attacks on its infrastructure.[3] The attack degraded enough critical media and communications systems that it rendered the government impotent to conduct its essential functions of monitoring the country's economy and command and control over military forces.[4] The Estonia "911" emergency equivalent was off-line for an extended period. The natural inclination of several observers was to suspect the Russian government of orchestrating the attack.[5] No public evidence

[3] Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV 1427, 1428-29 (2008) (citing *Newly Nasty*, ECONOMIST, May 26, 2007, at 63); Korns & Kastenberg, *supra* note 1, at 63.
[4] Kelsey, *supra* note 3, at 1429.
[5] Korns & Kastenberg, *supra* note 1, at 65.

has emerged to sustain this suspicion.[6] In response to the attacks, Estonia appealed to the United States and the North Atlantic Treaty Organization for assistance.[7]

On July 19, 2008, an Internet cyber security firm reported on a distributed denial of service (DDoS) cyber attack against the country of Georgia.[8] Three weeks later, on August 8, security experts observed a second round of DDoS attacks against Georgia, this time more substantial, with multiple command and control (C2) servers concentrated against Georgian governmental and commercial websites. Analysts noted that this second round of DDoS attacks appeared to coincide with the movement of Russian troops into South Ossetia in response to Georgian military operations a day earlier in this region.[9] By August 10, DDoS attacks rendered most Georgian governmental websites inoperable.[10]

As a result of the DDoS attacks, the Georgian government found itself cyber-locked, barely able to communicate on the Internet.[11] In response to the situation, the Georgian government took an unorthodox step and sought "cyber refuge" in the United States.[12] Without first seeking U.S. government approval, Georgia relocated its

---

[6] *Id.*; *see also*, Scott Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L., 192, 193 (2009).

[7] Korns & Kastenberg, *supra* note 1, at 63; Shackelford, *supra* note 5.

[8] Korns & Kastenberg, *supra* note 1, at 64-65; Steven Adair, *The Website for the President of Georgia Under Attack – Politically Motivated?*, SHADOWSERVER FOUNDATION, July 20, 2008, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080720 (last visited Sept. 2, 2009). Shadowserver specifically reported:

> For over 24 hours, the website of President Mikhail Saakashvili of Georgia has been rendered unavailable due to a multi-pronged distributed denial of service (DDoS) attack. The site began coming under attack very early Saturday morning. Shadowserver has observed at least one web-based command and control (C2) server taking aim at the website hitting it with a variety of simultaneous attacks. The C2 server has instructed its bots to attack the website with TCP, ICMP, and HTTP floods . . . the C2 server involved in these attacks is on IP address 207.10.234.244, which is subsequently located in the United States.

[9] Adair, *supra* note 8; Korns & Kastenberg, *supra* note 1, at 65.

[10] Steven Adair, *Georgian Websites Under Attack - DDoS and Defacement*, SHADOWSERVER FOUNDATION, Aug. 11, 2008, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080811 (last visited Sept. 2, 2009); Shaun Waterman, *Georgia Hackers Strike Apart From Russian Military*, WASH. TIMES, Aug. 19, 2008, http://www.washtimes.com/news/2008/aug/19/georgia-hackers-strike-apart-from-russian-military (last visited Sept. 7, 2009); Karl Zimmerman, Webhosting Report, Steadfast Networks, comment posted July 20, 2008, http://www.webhostingtalk.com/showpost.php?p=5220780&postcount=41 (last visited Sept. 11, 2009).

[11] Korns & Kastenberg, *supra* note 1, at 66.

[12] *Id*.

Presidential website to a U.S. web hosting company and moved its Ministry of Foreign Affairs (MFA) press dispatches to Google's Blogspot.[13] The MFA also mirrored its Internet services at a site in Estonia and on the website of Poland's president, Lech Kaczynski.[14]

Georgian-Russian hostilities in South Ossetia generated a substantial amount of analysis and speculation regarding the underlying cyber conflict.[15] Most of the focus has centered on who conducted the cyber attacks, and why. However, the Georgian-Russian conflict provides an opportunity to examine a more subtle, intriguing, and perhaps overlooked aspect of cyber conflict—the concept of cyber neutrality. The Georgian case raises two fundamental questions: can the United States remain neutral (or cyber neutral) during a cyber conflict, and how did the actions of the Georgian government and private U.S. information technology (IT) companies impact U.S. status as a cyber neutral?

The implications of these two questions should concern U.S. policy makers and military strategists. Even if the United States is not a belligerent in a cyber conflict, incursions on the U.S. Internet infrastructure will likely occur. Private industry owns and operates the Internet. The unregulated action of these third party actors during a cyber conflict could unintentionally impact U.S. cyber neutrality. There is little, if any, modern legal precedence which resolves this question. Nonetheless, the fact that U.S. IT companies provided cyber assistance to the Georgian government, without any apparent U.S. government involvement, exemplifies a significant cyber policy issue. Although nations still bear ultimate responsibility for the acts of their citizens or surrogates, translating this protocol to fit the modern realities of cyber conflict is a complex challenge. By relocating its cyber assets to the

---

[13] Adair, *supra* note 10; *see also* MINISTRY OF FOREIGN AFFAIRS OF GEORGIA, http://georgiamfa.blogspot.com (last visited Sept. 7, 2009); Noah Shachtman, *Estonia, Google Help "Cyberlocked" Georgia*, WIRED: DANGER ROOM, Aug. 11, 2008, http://blog.wired.com/defense/2008/08/civilge-the-geo.html (last visited Sept. 7, 2009); Peter Svensson, *Georgian President's Web Site Moves to Atlanta*, USATODAY.COM, Aug. 11, 2008, http://www.usatoday.com/tech/products/ (last visited Sept. 7, 2009); Tulip Systems Incorporated, http://www.tshost.com (last visited Sept. 11, 2009).

[14] John Markoff, *Georgia Takes a Beating in the Cyberwar With Russia*, N.Y. TIMES: BITS BLOG, Aug. 11, 2008, http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia (last visited Sept. 7, 2009); *see also Information About The Latest Developments In Georgia*, MINISTRY OF FOREIGN AFFAIRS OF GEORGIA, http://www.president.pl/x.node?id=20043119 (accessed on the web site of the President of Poland) (last visited Sept. 7, 2009); Shachtman, *supra* note 13.

[15] Korns & Kastenberg, *supra* note 1, at 67-68; Markoff, *supra* note 13; *see also* Kim Hart, *Longtime Battle Lines Are Recast In Russia And Georgia's Cyberwar*, WASH. POST, Aug. 14, 2008, at D1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html (last visited Sept. 7, 2009); Noah Shachtman, *Georgia Under Online Assault*, WIRED: DANGER ROOM, Aug. 10, 2008, http://blog.wired.com/defense/2008/08/georgia-under-o.html (last visited Sept. 7, 2009).

United States, Georgia's unconventional response to the July and August 2008 DDoS attacks, supported by U.S. industry, adds a new element of complication that strategists need to consider in planning for future cyber operations.

This is not to argue that the United States failed to plan for the eventuality of a cyber conflict, and it is important to note that defense capabilities may be used to enforce cyber neutrality if the need to do so arises. The Executive Branch of the U.S. Government has prepared for the eventuality of a cyberwar. In 1997, President William J. "Bill" Clinton established the President's Commission on Critical Infrastructure Protection. The Commission predicted that by 2002, 19 million people would have the ability to launch cyber attacks. It also noted that since little in the way of specialized equipment is needed to conduct such attacks, governments could expect an exponential growth in increasingly sophisticated malicious cyber activity.[16]

On May 22, 1998, President Clinton issued Presidential Decision Directive/NSC-63.[17] In it, the President noted, "The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems."[18] In 2002, President George W. Bush issued National Security Presidential Directive (NSPD) 16, which directed the government to review offensive capabilities against enemy computer networks.[19] In 2004, President Bush issued NSPD-38, *National Strategy to Secure Cyberspace*.[20] The two strategy documents are related in the same manner in which offense and defense are related in a military operational construct. Both documents are not releasable to the general public due to classification considerations.

In 2008, President Bush promulgated NSPD 54/Homeland Security Presidential Directive (HSPD) 23, *Cyber Security and Monitoring*. While NSPD 54/HSPD 23 remains classified, its definition of cyberspace is: "'Cyberspace' means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded

---

[16] COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, WHITE PAPER, THE CLINTON ADMINISTRATION'S POLICY ON CRITICAL INFRASTRUCTURE POLICY: PRESIDENTIAL DECISION DIRECTIVE 63 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/paper598.htm.

[17] *See generally* Presidential Decision Directive NSC-63, Critical Infrastructure Protection (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[18] *Id.*

[19] *See* Bradley Graham, *Bush Orders Guidelines for Cyber Warfare*, WASH. POST, Feb. 7, 2003, at A1.

[20] National Security Presidential Directive 38, National Strategy to Secure Cyberspace (2004) (quotation is unclassified portion of a classified document).

processors and controllers in critical industries."[21] Later, Deputy Secretary of Defense Gordon England, issued a memorandum that defined 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."[22]

Presently there are two proposed bills pending in the United States Senate that will enable the executive branch to exert greater control over cyberspace during emergencies. Senator Jay Rockefeller (D - West Virginia) introduced Senate Bill 773 titled the Cybersecurity Act of 2009.[23] Section 18 of the proposed act enables the President to declare an emergency and order the limitation or shutdown of a Federal Government or United States critical information infrastructure system or network.[24] While the pending bill is designed to place the Director of National Intelligence and the Secretary of Commerce as the primary agencies for ensuring cyber-security, the Department of Defense will have an advisory role.[25] Senator Thomas Carper (D - Delaware) introduced the second bill, the United States Information and Communications Enhancement Act of 2009.[26] This bill would establish a National Office for Cyberspace in the White House, charged with overseeing the execution of cybersecurity policies and procedures in the federal government.[27] Neither act expressly touches on the subject of cyber neutrality, but both would give to the executive branch a leverage of control over the internet to enforce neutrality during national emergencies.

The U.S. Department of Defense (DOD) has prepared for the eventuality of cyber operations in a wartime context as evidenced in directives, instructions, and doctrine. The Joint Functional Component Command for Network Warfare is the sole agency for network attack. However, with the pending creation of the sub-unified command, the authority to conduct network warfare will fall to the commander of the

[21] National Security Presidential Directive 38/ Homeland Security Presidential Directive 23, Security and Monitoring (2008) (quotation is unclassified portion of a classified document).
[22] Both definitions are contained in the Memorandum from the Deputy Secretary of Defense Memo to the Military Departments et al., subject: "The Definition of Cyberspace" (12 May 2008), and its accompanying staff papers (on file with author).
[23] S. 773, 111th Cong. (2009); *see also* R. Michael Senkowski & Mimi W. Dawson, *Cybersecurity: A Briefing - Part II*, METRO. CORP. COUNS., Aug. 2009, at 34.
[24] S. 773, 111th Cong. (2009), § 18.
[25] *Id*. § 3.
[26] S. 921, 111th Cong. (2009).
[27] *Id*. § 3552.

new command. This command is slated to be fully operational in October 2009. [28]

DOD Directive (DODD) O-3600.3, *Technical Assurance Standard for Computer Network Attack (CNA) Capabilities*, was promulgated on May 13, 2005. This directive is classified "Top Secret," except for the name. Presumably, it contains, as the name implies, capabilities requirements for conducting CNA. Because CNA is defined as "[o]perations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves," in DODD 3600.01, *Information Operations*, dated August 14, 2006, it can also be assumed that the classified document approaches network attack in a like manner. Likewise, DODD O-8530.1, *Computer Network Defense*, dated January 8, 2001, is classified.

The DOD's doctrinal view of cyberspace is found in Joint Publication (JP) 6-0, *Joint Communications System*, dated March 20, 2006. It states:

> The GIG [global information grid] operates as a globally interconnected, end-to-end, interoperable network-of-networks, which spans traditional boundaries of authority. Given the inherent global reach of the GIG, many NETOPS [network operations] activities are not under the command authority of a using CCDR [combatant commander]. Therefore, a great deal of coordination and collaboration (unity of effort) is essential to fully enable NETOPS capabilities.[29]

JP 5-0, *Joint Operation Planning*, dated December 26, 2006, notifies commanders of combatant commands and service commanders to plan for asymmetrical threats. In terms of computer operations, the doctrine states, "one example of a persistent, asymmetric threat that is inherently global and poses risk cross-AOR [area of responsibility] boundaries is adversary exploitation and attack of DOD computer networks on the global information grid."[30] But in none of these rules is there a consideration for policing cyber neutrality.

---

[28] Siobahn Gorman, *Gates to Nominate NSA Chief to Head New Cyber Command*, WALL STREET J., Apr. 24, 2009, http://online.wsj.com (last visited Sept. 11, 2009).

[29] JOINT CHIEFS OF STAFF, JOINT PUB. 6-0, JOINT COMMUNICATIONS SYSTEM, at 71 (20 Mar. 2006), *available at* http://www.dtic.mil [hereinafter JP 6-0].

[30] JOINT CHIEFS OF STAFF, JOINT PUB. 5-0, JOINT OPERATION PLANNING, at I-22 (26 Dec. 2006), *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp5_0.pdf [hereinafter JP 5-0].

III. CYBER NEUTRALITY, A BASIC RUBRIC

Neutrality, in the United States, is primarily the executive branch's province, as a matter of its constitutional authority over foreign policy.[31] In 1908, Woodrow Wilson, then president of Princeton University, articulated, "One of the greatest of the President's powers I have not yet spoken of at all: his control, which is very absolute, of the foreign relations of the nation. The initiative in foreign affairs, which the President possesses without any restriction whatever, is virtually the power to control them absolutely."[32] Yet, at the beginning of World War I, U.S. President Wilson declared the United States a neutral nation, but American banks continued providing loans to Britain and France, and American industry sold armaments almost exclusively to Britain, France and their allies.[33] The German government responded by waging unrestricted submarine warfare, maritime commerce raiding, and espionage activities within the continental United States.[34]

Wilson's neutrality stance was more emotional than actual, in that he did not exercise executive authority to halt U.S. loans and arms shipments to belligerents.[35] Over a half century later, Supreme Court Justice William O. Douglas penned sentiments similar to Wilson's in writing, "my view of foreign affairs is that Congress has the power to declare war, and that all diplomacy short of that is under the guidance of the President."[36] Even as Douglas harshly criticized the Nixon administration's policies in Vietnam and concluded the conflict was "unlawful," Douglas held fast to the principle of executive authority in foreign policy.[37]

It must be noted that although the executive branch is preeminent in foreign policy, as a matter of checks and balances, Congress does retain the authority to regulate foreign commerce and no treaty can obligate the United States without the Senate's advice and consent.[38] In 1920, the Supreme Court determined that individual states, of the United States, do not possess the authority to act contrary

---

[31] U.S. CONST. art. II, § 2; Korns & Kastenberg, *supra* note 1, at 61-62.
[32] WOODROW WILSON, CONSTITUTIONAL GOVERNMENT IN THE UNITED STATES 77 (1908); Korns & Kastenberg, *supra* note 1, at 61-62.
[33] JENNIFER KEENE, WORLD WAR I: DAILY LIFE THROUGH HISTORY 5 (2006); RONALD STEELE, WALTER LIPPMAN AND THE AMERICAN CENTURY 89 (1999).
[34] WILLIAM MCNEILL, THE PURSUIT OF POWER 341-42 (1982); THEODORE ROPP, WAR IN THE MODERN WORLD 257-58 (1959).
[35] ANNE RICE PIERCE, WOODROW WILSON AND HARRY TRUMAN: MISSION AND POLICY IN AMERICAN FOREIGN POLICY 22 (2003).
[36] WILLIAM O. DOUGLAS, THE COURT YEARS: 1939-1957, AN AUTOBIOGRAPHY 270 (1980).
[37] *Id*.
[38] U.S. CONST. art. II, § 2.

to a treaty.[39] More importantly, this finding also extends to individual corporations, which may not conduct trade with a foreign government against the executive branch's prohibition of such trade. Indeed, where a corporation violates this prohibition, it may be subject to criminal sanctions. If the U.S. government establishes a strict position of neutrality, corporations based in the United States may not provide material support to a belligerent state, except where the government permits.[40] Corporations may, however, engage in non-military trade or provide humanitarian support.[41]

For the purpose of this article, cyber neutrality does not depart from the traditional international law of neutrality. This rubric of laws requires combatant states to recognize the rights of neutrals. In addition, neutral states must refrain from assisting either side in a conflict, other than to effectuate peace.[42] Neutrality laws as codified in the 1907 Hague V Conventions give states certain legal rights when not participating in a conflict, especially the right to remain neutral and maintain relations with all belligerents.[43] States that declare themselves to be neutral, and act accordingly, are entitled to immunity from attack.[44] Neutrality does not require neutral states to shut off all commerce with combatant states, although such commerce must not expressly provide military aid to a combatant state during conflict.[45] The Conventions also dictate that the territory of a neutral state is inviolable; belligerents may not move troops, weapons, or other materials of war across the territory of a neutral state.[46] Belligerent states may not conduct hostilities from the territory or waters of a neutral state, and a belligerent's aircraft may not penetrate neutral airspace.[47] The Conventions require that neutral states prevent belligerents from engaging in these violations.[48] A neutral state that

---

[39] *See* U.S. CONST. art. I, § 8, cl. 3; Missouri v. Holland, 252 U.S. 416 (1920); U.S. v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936).

[40] When the United States is in conflict with another nation, the President's power to suppress trade with belligerent nations is almost absolute. *See* Trading with the Enemy Act, 50 U.S.C. app. § 5(b) (2006).

[41] *Id.* The U.S. State Department list of state sponsors of terrorism is at http://www.state.gov/s/ct/c14151.htm (last visited Sept. 12, 2009).

[42] Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, arts. 1–3, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague Convention V]; *see also* Convention Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415, 1 Bevans 723 [hereinafter Hague Convention XIII]; STEPHEN C. NEFF, THE RIGHTS AND DUTIES OF NEUTRALS 1 (2000).

[43] Hague Convention XIII, *supra* note 42, art. 1.

[44] *Id*.

[45] Hague Convention V, *supra* note 42, art. 7.

[46] *Id*. art. 5.

[47] *See* Detlev Vagts, *The Role of Switzerland: Neutrality Law in World War II*, 20 CARDOZO L. REV. 459, 465-67 (1998).

[48] Hague Convention V, *supra* note 42, art. 9.

takes no action jeopardizes its neutrality status. In 1917, the Supreme Court cemented this framework into American jurisprudence.[49]

As an emerging form of warfare, cyber war is not explicitly addressed under current international law, thus neither is cyber neutrality. However, overarching principles apply to both.[50] Cyber warfare implicates the principle of neutrality because a belligerent may launch attacks using the international structure of the Internet. The core issue is the routing of these cyber attacks through neutral countries, which is likely given the Internet's architecture. Cyber attacks routed across the Internet nodes of neutral states would appear to violate conventional neutrality law, despite the lack of physical intrusion.[51] The same would apply to cyber attacks launched from a neutral state, even if the neutral state did not control the attack. International law would appear to require a belligerent state (or third party neutral) to stop its citizens from engaging in such acts.

International law is not definitive on whether cyber techniques such as DDoS are legally considered "attacks" or "weapons,"[52] and whether cyber attacks can be considered legitimate acts of "armed conflict."[53] Malicious software, or malware, is not an "arm" of war, yet

---

[49] *See* The Steamship Appam, 243 U.S. 124 (1917). The *Appam* involved a British vessel which had been seized on the high seas by the German Navy, but brought into an American port for fuel. The Court found the seizure lawful under international law, but once the German Navy brought the vessel into neutral American jurisdiction, the British ship owners possessed standing to sue for recovery of the vessel because the Germans had violated neutrality by bringing a war prize through neutral territory. Of importance, the Court held: "The violation of American neutrality is the basis of jurisdiction, and the admiralty courts may order restitution for a violation of such neutrality. In each case the jurisdiction and order rests upon the authority of the courts of the United States to make restitution to private owners for violations of neutrality where offending vessels are within our jurisdiction, thus vindicating our rights and obligations as a neutral people." *Id*. at 128.

[50] Knut Dörmann, *Computer Network Attack and International Humanitarian Law*, INT'L COMM. OF THE RED CROSS, May 19, 2001, *available at* http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/5p2alj; *see also* Robert G. Hanseman, *The Realities and Legalities of Information Warfare*, 42 A.F. L. REV. 187 (1997); Bruce Smith, *An Eye for an Eye, a Byte for a Byte*, FED. L., Oct. 1995, at 12; George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079 (2000).

[51] Lawrence T. Greenberg et al., *Information Warfare and International Law* 10 (1998), *available at* http://permanent.access.gpo.gov/lps1804/iwilindex.htm.

[52] Kelsey, *supra* note 3, at 1443; *see also* Steven M. Barney, *Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace*, *in* THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF STRATEGY ESSAY COMPETITION 1 (Nat'l Def. Univ. Press, 2001), *available at* http://www.ndu.edu/inss/books/Books_2001/essays2001/Essays01.pdf; Davis Brown, *A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179 (2006); Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007).

[53] Kelsey, *supra* note 3, at 1443; *see also* Greenberg et al., *supra* note 51, at 30–33; Hanseman, *supra* note 50, at 183; Gregory F. Intoccia & Joe W. Moore,

the effects of cyber attacks can equal that of kinetic attacks. Arguably, a cyber attack that causes physical destruction could constitute an "armed attack" under the United Nations (UN) Charter.[54] The Charter appears to define an "armed attack" as a crossing of geographic domains by the use of armed force.[55]

Some advocates articulate that beyond transmitting a mere communication signal, cyber attacks effectively move a weapon across the Internet.[56] For example, in issuing National Security Directive 16, President George W. Bush ordered the development of guidelines to regulate the use of "cyber weapons in war."[57] The Estonian Defense Minister initially characterized the April 2007 Estonian cyber event as an "extensive cyber attack."[58] He contemplated invoking NATO Article V, which considers an "armed attack" against any NATO country to be an attack against all.[59] A 2008 Defense Science Board report stated that terrorists are using the Internet as an "asymmetric weapon."[60] A past assistant to the President for cyber security indicated that "[a]ttacks on the Internet itself . . . could cause widespread problems."[61]

On the other hand, some skeptics stress that no international legal precedents clearly define cyber weapons, and point to the Law of Armed Conflict (LOAC) as being unsettled with respect to cyber attacks.[62] Admittedly, there is a rationale for this view. The Council of Europe Convention on Cybercrime (COE Convention), to which the

---

Communications Technology, Warfare, and the Law: Is the Network A Weapon System?, 28 HOUS. J. INT'L L. 469 (2006).

[54] U.N. Charter art. 51.

[55] *Id*.

[56] *See* Brown, *supra* note 52.

[57] Bradley Graham, *Bush Orders Guidelines for Cyber-Warfare: Rules for Attacking Enemy Computers Prepared as U.S. Weighs Iraq Options*, WASH. POST, Feb. 7, 2003, at A1; Korns & Kastenberg, *supra* note 1, at 63.

[58] Kevin Poulsen, *Cyberwar and Estonia's Panic Attack*, WIRED: THREAT LEVEL, Aug. 22, 2007, http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html (last visited Sept. 7, 2009); *see also* Jeremy Kirk, *Estonia Recovers from Massive DDoS Attack*, COMPUTERWORLD.COM, May 17, 2007, http://www.computerworld.com (last visited Sept. 7, 2009).

[59] North Atlantic Treaty art. 5, Apr. 4 1949, 63 Stat. 2241, 34 U.N.T.S. 243, *available at* http://www.nato.int/docu/basictxt/treaty.htm ("The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations . . . ").

[60] DEFENSE SCIENCE BOARD, FINAL REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON STRATEGIC COMMUNICATION 27 (2008).

[61] John Schwartz, *When Computers Attack*, N.Y. TIMES.COM, June 24, 2007, http://www.nytimes.com (last visited Sept. 7, 2009) (quoting Paul Kurtz' statement that "[a]ttacks on the Internet itself, say, through what are known as root-name servers, which play a role in connecting Internet users with Web sites, could cause widespread problems").

[62] Intoccia & Moore, *supra* note 44, at 484.

United States is a party, does not contain any reference to cyber attacks, and instead considers as criminal acts all offenses against "the confidentiality, integrity or availability of computer systems."[63] The Center for Strategic and International Studies points out that DDoS attacks are more commonly used for illicit activities like fraud than for cyber war.[64] NATO defense ministers declined to define the Estonia cyber event as an attack requiring military action.[65] The Estonian Justice Minister ultimately conceded that independent civilians, rather than the Russian government, conducted cyber attacks against his country. The Estonian government now classifies the incident as an act of terrorism rather than cyber war.[66]

In 2005, the U.S. Air Force Operations and International Law division published a memorandum stating "the network is not a weapon system."[67] An Internet security expert recently observed "there are good reasons to reject the idea that timeout errors (DDoS) are an act of war."[68] Until the obfuscation surrounding cyber attacks is better clarified, many in the legal and technical communities will continue to see DDoS events as acts for the criminal justice system—not the national defense system—to resolve.

Although the debate over cyber conflict remains unsettled, the international law community does appear to be coalescing around the general principle that use of the Internet to conduct cross-border cyber attacks violates the principle of neutrality. As one legal scholar has noted, "[w]hen an information packet containing malicious code travels

---

[63] *United States Joins Council of Europe Convention on Cybercrime*, DEP'T OF STATE, Sept. 29, 2006, http://www.america.gov/st/washfile-english/ (last visited Sept. 7, 2009); *see also* Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167 [hereinafter COE Convention], *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[64] Schwartz, *supra* note 52 (quoting James Andrew Lewis' statement that "[t]hese 'bot-nets' are more commonly used for illicit activities like committing online fraud and sending spam").

[65] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN, May 17, 2007, http://www.s.co.uk/world/2007/may/17/topstories3.russia (last visited Sept. 7, 2009).

[66] *EU Should Class Cyber Attacks as Terrorism: Estonia*, BRISBANE TIMES.COM, June 8, 2007, http://news.brisbanetimes.com.au/technology/eu-should-class-cyber-attacks-as-terrorism-estonia-20070608-h9r.html (last visited Sept. 7, 2009); *see also* Joel Hruska, *Student Behind DoS Attack that Rekindled Bad Soviet Memories*, ARS TECHNICA, Jan. 24, 2008, http://arstechnica.com/news.ars/post/20080124-student-behind-dos-attack-that-rekindled-bad-soviet-memories.html (last visited Sept. 7, 2009); Jeremy Kirk, *Student Fined for Attack Against Estonian Web Site*, INFOWORLD (Internet edition), Jan. 24, 2008, http://www.infoworld.com/article/08/01/24/Student-fined-for-attack-against-Estonian-Web-site_1.html (last visited Sept. 7, 2009).

[67] Memorandum from U.S. Air Force Operations and Int'l L. Div., to Staff Judge Advocate, U.S. Air Force Comm. Agency, subject: Legal Issues Related to "Network as a Weapon System" (13 May 2005) (on file with author).

[68] Poulsen, *supra* note 58.

through computer systems under the jurisdiction of a neutral state, a strict construction of the law of neutrality would result in that state's neutrality being violated."[69] This evolution in thought should concern the United States, because as cyber conflict increases it is likely that the United States will see increased incursions on or across its Internet assets.

A surrender of neutrality or acquiescence to belligerent activity may draw a neutral state into the conflict.[70] Under this rule, if a neutral state cannot or does not take action to halt a cyber attack, a belligerent may choose to counter by physically attacking the neutral state's communications infrastructure. Thus, even without the physical violation of a neutral state's territory, a cyber attack may force a neutral state to become unwillingly involved. This loss of non-belligerent status is precisely what the Hague laws of neutrality seek to avoid. In short, although there is a growing body of legal thought, the concept of cyber neutrality remains ill-defined under current U.S. and international law. U.S. planners will likely see an increase in the number of situations where U.S. cyber neutrality is brought into question. The challenge for U.S. strategists is how to plan for cyber neutrality with little precedence.

Neutrality law also defines a limited telecommunications exception. Under Article VIII of the 1907 Hague Convention V, "[a] neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus," so long as the neutral state impartially permits the use of those structures by all belligerents.[71] The United States interprets this article as applying to modern communications.[72] Article VII implies that as long as a neutral party allows all belligerents equal passage on its communications infrastructure, neutrality is not violated. However, legal experts question whether the Article VIII exception applies to modern IT systems which can generate and transmit malicious data packets from, or across, a neutral party's Internet infrastructure to attack another belligerent's computer systems.[73]

Cyber neutrality may be defined as the right of any state to maintain relations with all parties in a cyber conflict, and the right not to

---

[69] William J. Bayles, *The Ethics of Computer Network Attack*, PARAMETERS, Spring 2001, at 44, 44-45, *available at* http://www.carlisle.army.mil/usawc/Parameters/01spring/bayles.htm.
[70] Hague Convention V, *supra* note 33, art. 8.
[71] *Id.*
[72] DEP'T OF DEF. OFFICE OF GEN. COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (1999), *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf (last visited Sept. 7, 2009); *see also* Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL L. REV. 57, 62 (1998).
[73] Kelsey, *supra* note 3, at 1442.

support or take sides with any cyber belligerent. Under a traditional international law rubric, to remain neutral in a cyber conflict, a cyber neutral state must not originate a cyber attack, and it must also, within its capabilities, take action to prevent a cyber attack from transiting its Internet nodes.[74] A neutral state also has the obligation to police its peoples from independently taking action. Admittedly, this may be difficult in states which emphasize the almost unlimited right of free speech, but, if a neutral state takes no action, it risks losing its cyber neutral status. The U.S. Constitutional framework is more than adequate to allow for appropriate action.

IV. CASE STUDY: THE CYBER ATTACK ON GEORGIA CONSEQUENCES FOR U.S. CYBER NEUTRALITY

On July 19, 2008, unknown persons used a computer located at a U.S. ".com" Internet protocol address[75] to command and control (C2) a DDoS attack against the website of Georgia's president, Mikheil Saakashvili.[76] The DDoS attack rendered the Georgian website inoperable for over 24 hours. Some security analysts speculate that this DDoS attack may have been a dress rehearsal for larger cyber operations against Georgia that ensued later in August 2008.[77] Analysts were unable to pinpoint the party who controlled the U.S. computer. However, cyber security experts identified the C2 server as a MachBot DDoS controller written in Russian and frequently used by Russian hackers. Therefore, analysts speculated on ties to Russia.[78]

---

[74] *Id*. at 1443.

[75] A computer with a ".com" Internet address implies a commercial entity; a ".gov" Internet address is reserved for U.S. Government use. Use of a ".com" computer in this specific DDoS attack implies the computer was not under direct U.S. government control.

[76] Adair, *supra* note 7; *see also* Dancho Danchev, *Georgia President's Web Site Under DDoS Attack From Russian Hackers*, ZDNET, July 22, 2008, http://blogs.zdnet.com/security/?p=1533 (last visited Sept. 7, 2009); John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1, *available at* http://www.nytimes.com.

[77] Markoff, *supra* note 13.

[78] Adair, *supra* note 8. Adair writes,

> [Although] DDoS attacks against various other neighbors of Russia to include Estonia have been quite popular in the last few years . . . we do not have any solid proof that the people behind this C&C [C2] server are Russian. However, the HTTP-based botnet C2 server is a MachBot controller, which is a tool that is frequently used by Russian bot-herders. On top of that, the domain involved with this C2 server . . . does tie back to Russia . . . . This server recently came online in the past few weeks and has not issued any other attacks . . . all attacks we have observed have been directed right at www.president.gov.ge.

Id.

The COE Convention characterizes the July 2008 DDoS attack against Georgia as cyber crime, not cyber war.[79] Within the COE Convention construct, the United States should have taken action under Article II (illegal access) and Article IV (system interference) to prevent the DDoS attack, a crime against Georgia.[80] Apparently, the attack stopped only after a private company took action on its own and blocked access to the U.S computer that controlled that DDoS attack.[81] The implication is that the international community prefers viewing DDoS attacks as criminal in nature. The result has been a growing body of cybercrime law, yielding additional clarity and cooperation. In fact, the U.S. Department of Justice successfully prosecuted several cases over the past two years involving DDoS attacks.[82] From the COE Convention's perspective, Interpol, rather than NATO, would have been the proper response to the Estonian (April 2007) and Georgian (July 2008) DDoS attacks. This same level of clarity is lacking when the nature of a cyber event changes from criminal to war between nation states.

On August 8, 2008, cyber security experts observed a second wave of DDoS attacks against Georgian websites.[83] This time, analysts speculate that the attacks coincided with Russia's movement of military forces into South Ossetia. Some have even characterized this incident as the first time a known cyber attack coincided with a "ground war."[84] The DDoS attack spread to computers throughout the Georgian government.[85] The Georgian Foreign Ministry blamed Russia for the

---

[79] *United States Joins Convention on Cybercrime*, *supra* note 63; *see also* COE Convention, *supra* note 63.

[80] Korns & Kastenberg, *supra* note 1, at 63.

[81] Adair, *supra* note 8.

[82] *See, e.g.*, *Botherder Dealt Record Prison Sentence for Selling and Spreading Malicious Computer Code*, U.S. DEP'T OF JUSTICE, May 8, 2006, http://www.cybercrime.gov/anchetaSent.htm (last visited Sept. 7, 2009) ("Concluding the first prosecution of its kind in the United States, [U.S. v. Ancheta], a well known member of the 'botmaster underground' was sentenced this afternoon to nearly five years in prison for profiting from his use of botnets--armies of compromised computers--that he used to launch destructive attacks . . . [the defendant] was sentenced to 57 months in federal prison . . . the longest known sentence for a defendant who spread computer viruses.); *see also Operator of a 'Bot-net' Network of Thousands of Virus-Infected Computers Sentenced to 12 Months in Federal Prison*, U.S. DEP'T OF JUSTICE, Oct. 23, 2007, http://www.cybercrime.gov/downeySent.pdf (last visited Sept. 7, 2009); *Indictment and Arrest for Computer Hacking*, U.S. DEP'T OF JUSTICE, Oct. 1, 2007, http://www.cybercrime.gov/kingIndict.pdf (last visited Sept. 7, 2009).

[83] Korns & Kastenberg, *supra* note 1, at 65.

[84] Markoff, *supra* note 13; *see also* Brandon Griggs, *U.S. at Risk of Cyberattacks, Experts Say*, CNN.COM, Aug. 18, 2008, http://www.cnn.com (last visited Sept. 7, 2009).

[85] Adair, *supra* note 8; *see also Russian Business Network (RBN) Now Nationalized, Invades Georgia Cyber Space*, RUSSIAN BUS. NETWORK, Aug. 9, 2008, http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html (last visited Sept. 7, 2009); Waterman, *supra* note 10.

attacks.[86] Others pointed to the Russian Business Network (RBN), a criminal syndicate suspected of being under Russian government influence.[87] Conversely, an Internet journalist visited a website where he downloaded pre-packaged software that enabled him within minutes—had he chosen to do so—to join in the DDoS attacks against Georgia. His assessment:

> In less than an hour, I had become an Internet soldier. I didn't receive any calls from Kremlin operatives; nor did I have to buy a Web server or modify my computer in any significant way . . . [m]y experiment also might shed some light on why the recent cyberwar has been so hard to pin down . . . . Paranoid that the Kremlin's hand is everywhere, we risk underestimating the great patriotic rage of many ordinary Russians, who . . . are convinced they need to crash Georgian Web sites. Many Russians undoubtedly went online to learn how to make mischief, as I did. Within an hour, they, too, could become cyber-warriors.[88]

Some cyber security analysts have concluded that the August 2008 DDoS attack against Georgia was a mix of government incentivized, organized cyber crime syndicates such as RBN, as well as ordinary cyber-citizen protestors.[89] Gadi Evron, former head of cyber security for the Israeli government, stated "this is not warfare, but just some unaffiliated attacks by Russian hackers."[90] Arbor Networks, a security firm, "found no evidence . . . of state-sponsored cyber-warfare"

---

[86] *Cyber Attacks Disable Georgian Websites*, MINISTRY OF FOREIGN AFF. OF GEORGIA, Aug. 11, 2008, http://georgiamfa.blogspot.com/2008_08_01_archive.html (last visited Sept. 7, 2009).

[87] *RBN Now Nationalized*, RUSSIAN BUS. NETWORK, Aug. 9, 2008, http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html (last visited Sept. 7, 2009).

[88] Evgeny Morozov, *An Army of Ones and Zeroes - How I Became a Soldier in the Georgia-Russia Cyberwar*, SLATE, Aug. 14, 2008, http://www.slate.com/id/2197514 (last visited Sept. 7, 2009); *see also* Evgeny Morozov, http://evgenymorozov.com/blog/?p=416 (last visited Sept. 7, 2009).

[89] Waterman, *supra* note 10; *see also* Dancho Danchev, *Coordinated Russia vs Georgia Cyber Attack In Progress*, ZDNET, Aug. 11, 2008, http://blogs.zdnet.com/security/?p=1670 (last visited Sept. 7, 2009); Joel Hruska, *Russians May Not be Responsible for Cyberattacks on Georgia*, ARS TECHNICA, Aug. 13, 2008, http://arstechnica.com (last visited Sept. 7, 2009).

[90] Gadi Evron, *Internet Attacks Against Georgian Websites*, CIRCLEID, Aug. 11, 2008, http://www.circleid.com/posts/88116_Internet_attacks_georgia (last visited Sept. 7, 2009).

and characterized the attackers as most likely "non-state actors."[91] Experts at cyber security firm Shadowserver indicated "it would appear that these cyber attacks have certainly moved into the hands of the average computer using citizen."[92]

While receiving less attention than analysis of the DDoS attacks against Georgia, perhaps of greater importance to U.S. policy makers is the Georgian government's novel reaction. If the responsibilities of states during cyber conflict are somewhat unclear, they are even more ambiguous when a belligerent seeks cyber refuge in a neutral state's territory.

Tulip Systems (TSHost) is a private web hosting company in Atlanta, Georgia. On August 8, while in the country of Georgia, the owner of TSHost apparently contacted Georgian government officials directly and offered assistance.[93] That the owner of TSHost is a U.S. resident of Georgian birth cannot be overlooked.[94] On August 9, the Georgian government transferred critical governmental Internet services to TSHost servers in the United States, including the Georgian President's website. In an admission, the TSHost Chief Executive Officer (CEO) stated that the company had volunteered its servers to "protect" the nation of Georgia's Internet sites from malicious traffic.[95] TSHost further revealed that after it relocated Georgian websites to the United States, DDoS attacks, traced to Moscow and St. Petersburg, ensued against TSHost's servers.[96] The TSHost CEO confirmed the company reported the attacks to the FBI, but he did not claim to obtain government sanction for his activities.

This important fact is not widely publicized: a U.S. company with no clear authority and no apparent U.S. government approval

---

[91] Kelly Jackson Higgins, *Botnets Behind Georgian Attacks Offer Clues*, DARK READING, Sept. 9, 2008, http://www.darkreading.com/document.asp?doc_id=163342 (last visited Sept. 7, 2009).

[92] Adair, *supra* note 8 ("Since August 8, 2008, a large number of Georgian websites, both government and non-government alike, have come under attack…one of the Georgian government websites was being attacked by dozens of Russian computers from several different ISPs throughout the country… lots of ICMP traffic and Russian hosts sounds a lot more like users firing off the 'ping' command…much like in the attacks against Estonia, several Russian blogs, forums, and websites are spreading a Microsoft Windows batch script that is designed to attack Georgian websites…it would appear that these cyber attacks have certainly moved into the hands of the average computer using citizen."); Korns & Kastenberg, *supra* note 1, at 66. A redacted version of the actual software script used in the DDoS attacks is also available at the site hosting Adair's article.

[93] Peter Svensson, *Russian Hackers Continue Attacks on Georgian Sites*, AP NEWS, Aug. 12, 2008, http://www.usatoday.com/tech/products/2008-08-12-2416394828_x.htm (last visited Sept. 7, 2009); s*ee also* Griggs, *supra* note 84; Korns & Kastenberg, *supra* note 1, at 63; Svensson, *supra* note 13.

[94] Korns & Kastenberg, *supra* note 1, at 63.

[95] Griggs, *supra* note 84.

[96] Svensson, *supra* note 13.

directly contacted the Georgian government and arranged to protect its Internet assets by moving them to U.S. territory.[97] Undeterred, cyber attackers followed and turned their DDoS attacks against the U.S. site. As a result of TSHost actions, the U.S. effectively experienced cyber collateral damage.[98]

On August 8, the Georgian government sought additional protection within the United States by transferring its official MFA and government news sites to Google's Blogspot.[99] While Georgia's combat troops were retreating to Tbilisi to defend the capital, Georgia's cyber forces were turning to the United States to defend the country's Internet capabilities. Google effectively became the cyber refugee camp for Georgia's cyber property.[100] The Georgian government used equipment located in U.S. territory—specifically Google's Internet servers in California—to protect its Internet capabilities and ensure continued war-time communications with its citizens and forces. Georgia's creative cyber strategy relied on relocation to the United States because the Georgian government did not believe DDoS attackers could take down Google's servers, given the company's vast infrastructure and ability to defend it.[101] It does not appear that the Georgian government coordinated this strategy with the U.S. prior to execution. There were also accusations, later refuted, that Google removed details of Georgian maps from its on-line mapping service.[102]

In the Georgian-Russian cyber conflict, the actions of the Georgian government and a well-intentioned, patriotic CEO could have imperiled U.S. cyber neutrality. Apparently, neither Google's nor TSHost's actions had U.S. government involvement or approval.[103]

As noted above, Article III of Hague Convention V forbids belligerents from erecting on the territory of a neutral Power a wireless

---

[97] Korns & Kastenberg, *supra* note 1, at 67.
[98] *Id*.
[99] Jon Swaine, *Georgia: Russia Conducting Cyber War*, TELEGRAPH, Aug. 11, 2008, http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/-Georgia-Russia-conducting-cyber-war.html (last visited Sept. 7, 2008); *see also* Larry Dignan, *Georgia Turns to Google's Blogger to Counter Alleged Cyber Attack*, SEEKING ALPHA, Aug. 11, 2008, http://seekingalpha.com (last visited Sept. 7, 2009); Pete Swabey, *Google Embroiled in Georgian Conflict*, INFO. AGE, Aug. 12, 2008, http://www.information-age.com (last visited Sept. 7, 2009).
[100] Korns & Kastenberg, *supra* note 1, at 67.
[101] *Id*.
[102] *Id*.; *see also* Dave Barth, *Where is Georgia on Google Maps?*, GOOGLE LAT LONG BLOG, Aug. 12, 2008, http://google-latlong.blogspot.com/2008/08/where-is-georgia-on-google-maps.html (last visited Sept. 7, 2009); *see also* Miguel Helft, *Google: We Did Not Erase Maps of Georgia*, N.Y. TIMES BITS BLOG, Aug. 12, 2008, http://bits.blogs.nytimes.com/2008/08/12/google-we-did-not-erase-maps-of-georgia (last visited Sept. 7, 2009); Katie Hunter, *Tuesday Map: Georgia's Google Vanishing Act*, FOREIGN POL'Y: PASSPORT, Aug. 12, 2008, http://blog.foreignpolicy.com/node/9515 (last visited Sept. 7, 2009).
[103] Korns & Kastenberg, *supra* note 1, at 68.

telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea.[104] One could argue that the Georgian government, as a cyber belligerent, violated this law when it established websites on U.S. cyber neutral territory, and then used the websites as "other apparatus" to communicate with its forces back in the territory of Georgia. The United States took no action to halt these operations. Further, it did not direct TSHost or Google to terminate support for Georgia. By allowing U.S. private companies to protect the Georgian government's Internet assets, one could make the case that the U.S. government jeopardized, or even relinquished, its cyber neutrality, and subjected the U.S. cyber infrastructure to potential attack.

Added to this issue, cyber corps or cyber warriors are terms often used in reference to U.S. government civilian and military personnel who conduct cyber operations.[105] This military nomenclature may be problematic. Given that the U.S. private industry operates the majority of the Internet, there is concern as to whether the category of cyber combatant could be extended to include private civilians operating the Internet.[106] When speaking about the success of her company in blocking DDoS attacks against Georgia's website, the TSHost CEO stated, "our people aren't getting any sleep."[107] Article IV of Hague V prohibits neutrals from forming "corps of combatants" to assist belligerents. Although unlikely, TSHost and Google actions could be interpreted as a violation of Hague V in that they formed a quasi-corps of cyber combatants on behalf of the U.S. government to protect Georgia's Internet assets.

Hague V Articles VIII and IX provide that a neutral state is not required to restrict a belligerent's use of the neutral's telecommunications systems, as long as these services are provided impartially to all belligerents.[108] The U.S. government could have required TSHost and Google to terminate Internet services for the Georgian government. By its silence, the U.S. government may have unknowingly established an unwanted precedence. Conceivably, future cyber belligerents, taking note of U.S. inaction in the Georgian case, could under the Hague V impartiality clause (Article IX) demand similar cyber refuge, or use of U.S. Internet infrastructure. The potential implications are disturbing.

---

[104] Hague Convention V, *supra* note 42, art. 3.

[105] *Fact Sheet: Protecting America's Critical Infrastructure – Cyber Security*, DEP'T OF HOMELAND SEC., Feb. 15, 2005, http://www.dhs.gov/xnews/releases/ (last visited Sept. 7, 2009); DEP'T OF DEF. CHIEF INFORMATION OFFICER, ANNUAL INFORMATION ASSURANCE REPORT ES-1 (2000), *available at* http://stinet.dtic.mil/cgi-bin/ ("The new warfighter is the cyber-warrior with technical and non-traditional skills").

[106] Intoccia & Moore, *supra* note 13, at 1.

[107] Svensson, *supra* note 13.

[108] Hague Convention V, *supra* note 42, art. 3.

Clearly, the Georgian and Russian governments were conventional belligerents in the Ossetian theater of conflict. It is unclear, however, if they were cyber belligerents. When bombs and bullets fly, identification is relatively easy; not so for cyber weapons. Both governments claim they did not participate in the DDoS attacks.[109] Expert analysis appears to substantiate, to a degree, that technically the governments themselves did not directly participate in cyber conflict.[110] The July and August DDoS attacks could be characterized as cyber conflict by proxy. Instead of states, it appears that cyber criminals as well as hundreds of loosely self-organized, non-combatant citizens and self-styled cyber-militias inflicted the attacks. This leads to uncertainty as to which attackers were officially cyber belligerents, and which ones were cyber neutrals.

Existing international laws of war focus primarily on conflicts between nation states, and are fundamentally weak in addressing non-state actor participation in cyber conflict. The 2007 Estonian cyber event serves as a superb case study. Although it was originally called cyber war, this changed in the post conflict retrospective analysis. Governments and experts concluded that unknown, non-state actors conducting DDoS attacks against a Baltic nation-state is not cyber war; at best, according to Estonian officials, it is terrorism.[111] The DDoS attacks against Georgia were strikingly similar to the Estonian case, and therefore place in doubt whether an actual state of cyber conflict existed between the governments of Georgia and Russia. This interpretation certainly raises questions regarding the legal status of U.S. cyber neutrality. The Georgian case stands as the latest example of the untidy nature of cyber conflict. Clearly, the Estonian and Georgian cyber events have established new precedents and subtexts for cyber war and neutrality.

The terms "cyberspace" and "global electronic village" imply that the Internet is a stateless and borderless entity used by all and owned by none.[112] Some in the legal community have used these notions to define cyberspace as a "separate place," governed by its own legal framework, where international treaties don't apply and governments have yielded sovereignty to "netizens" and self-regulatory initiatives.[113] These symbolic notions do not stand up to reality. The

---

[109] Korns & Kastenberg, *supra* note 1, at 70.
[110] *Id*.
[111] *See, e.g., EU Should Class Cyber Attacks as Terrorism*, *supra* note 66; Hruska, *supra* note 66; Kirk, *supra* note 66.
[112] *See, e.g.*, David Howes, *e-legislation: Law-Making in the Digital Age*, 47 MCGILL L.J. 39, 41-44 (2001).
[113] *See, e.g.*, John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND., Feb. 8, 1996, http://www.eff.org/~barlow/Declaration-Final.html (last visited Sept. 7, 2009); Michael Geist, *Cyberlaw 2.0*, 44 BOSTON

Internet in fact does have borders. Internet equipment is government or corporate owned. Internet assets are located in facilities within the territories of recognized nation states. Internet equipment is connected to national electric grids.[114]

When the government of Georgia relocated its Internet capabilities to TSHost and Google servers, it did not move its cyber assets to "space"; rather, it moved actual government data and information capabilities to equipment located in the states of Georgia and California, within U.S. territory. Under traditional Hague V Conventions, this act could be interpreted as a violation of U.S. neutrality. Nonetheless, there remains a lack of international agreement on how "border-centric" laws relate to the notion of a "borderless" Internet. This impinges on the cyber neutrality concept, which is built upon the traditional notion of absolute, recognizable borders.

V. CONCLUSION

As noted in the introduction, this article does not advocate that the United States must enforce neutrality in cyberspace in conflicts to which it is not a party. It does argue, however, that based on the current and future nature of interstate conflict, the executive branch should consider whether it is in the national interest to assert its authority to enforce neutrality in cyberspace. This is important because belligerent governments may consider U.S. corporations assisting their opponent states as a legitimate target for a cyber counter-strike (or perhaps a kinetic strike). Whether the executive branch determines that cyber neutrality is important to advocate for as an international law principle is outside the scope of this article as well. However, it is clear that the executive branch should be prepared to assert its Constitutional authority to enforce cyber neutrality before two belligerent states enter into conflict. And, commensurate with this authority, the federal government can organize and train to preserve this neutrality should the need arise.

COLLEGE L. REV. 323 (2003); David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

[114] *See, e.g.*, Dan Jerker B. Svantesson, *Borders on, Border Around – The Future of the Internet*, 16 ALB. L.J. SCI. & TECH. 433, 434-35 (2006).

ARMED ATTACK IN CYBERSPACE: DETERRING ASYMMETRIC WARFARE WITH AN ASYMMETRIC DEFINITION

MAJOR GRAHAM H. TODD

Major Graham H. Todd (B.S., U.S. Air Force Academy (1993); M.A., University of Kansas (1994); J.D., Florida State University (2001)) is currently the Chief of Operations Law at Eighth Air Force, Barksdale Air Force Base, Louisiana. He is a member of the Florida Bar.

China is likely to take advantage of the U.S. dependence on cyberspace for four significant reasons. . . . Fourth, there is an underdeveloped legal framework to guide response.[1]

There is currently no international, legally binding instrument that would address cyberspace attacks as threats to national security.[2]

I. INTRODUCTION

Change has come and gone. While academics have been discussing methods to define the use of force in cyberspace, governments and policy makers may have missed an opportunity to shape the law of war. Just like a child "pinching" a peppermint from the candy store while the owner was not looking, someone may have successfully launched two cyberspace attacks, and no one called either one an unlawful use of force or armed attack. Did a state actor set a precedent that could become part of customary international law?

Every day there are new stories and developments about the increasing connectivity of people around the world spurred by the continued fast pace of technological developments in the computer and communications industries. Military applications of cyberspace are also rapidly evolving, moving the domain of cyberspace to the front lines of conflicts. But, the legal frameworks that regulate war or armed conflict are lagging far behind the technological changes that have already occurred. Today, cyberspace is seamless and transcends international boundaries at the speed of light. Unfortunately, law, especially international law, failed to keep pace with the new applications of existing technologies.[3] On the criminal front, law enforcement agencies are swamped with allegations ranging from identity theft to theft of corporate data, while armed with only a marginally effective process to investigate, extradite, and prosecute international cyberspace criminals. However, the conduct of military operations in and through cyberspace, with potentially greater global implications, is bypassing the currently inadequate mire of international law. What if international law could provide a framework capable of enabling deterrence in cyberspace?

---

[1] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, 2008 ANNUAL REPORT TO CONGRESS 9 (2008), *available at* http://www.uscc.gov.

[2] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, CYBER ATTACKS AGAINST GEORGIA: LEGAL LESSONS IDENTIFIED 22 (Nov. 2008), *available at* http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

[3] By 1977, sales of computers such as Apple II, TRS 80, and Commodore PET would eventually lead to the personal computer impacting lives of ordinary people around the world. Meanwhile, commercial internet service providers began offering services in the late 1980's. Today, according to Wikipedia, there are more than 1 billion personal computers in use and more than 1 billion users of the internet. Wikipedia, Personal Computer, http://en.wikipedia.org/wiki/Personal_computer (last visited Mar. 15, 2009).

Scholars have written many articles regarding cyberspace attacks in the international regime and what constitutes a use of force or act of war in cyberspace.[4] Yet, there is no consensus regarding how to define attacks in cyberspace under international law. The unique qualities of operations in cyberspace will make this the most difficult domain in which to resolve international disputes and conflict. In this article, I intend to offer a new methodology for determining armed attacks in cyberspace by using existing criminal law legal tools. Specifically, this methodology will borrow from the criminal law's definitions of cyberspace crimes, in order to craft a definition of a cyberspace weapon. More importantly, by defining cyberspace weapon, this methodology will enable the international community to define what constitutes a cyberspace attack. Providing the legal framework for a definition of cyberspace attack, such as the new methodology outlined in this article, will serve to reduce the potential for conflict in cyberspace.

The article will first examine cyberspace and how current approaches have attempted to apply international law to armed attacks in cyberspace. Looking through the lens of current international laws will highlight how the unique attributes of cyberspace could increase the likelihood of international conflict. The article will identify how the failure of international law to define armed attacks and weapons further exacerbates this problem. The article will then transition from current international laws to examine whether current criminal law definitions and methodologies can fill the gap and provide realistic definitions of weapons and armed attacks in cyberspace. Lastly, the article will put these proposed definitions to the test against the most challenging aspects of cyberspace: attribution and espionage.

---

[4] *See, e.g.*, Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. OF TRANSNAT'L LAW 885 (1999) [hereinafter Schmitt, *Computer Network Attack*]; WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (1999); THOMAS C. WINGFIELD, WHEN IS A CYBER ATTACK AN "ARMED ATTACK?": LEGAL THRESHOLDS FOR DISTINGUISHING MILITARY ACTIVITIES IN CYBERSPACE (Cyber Conflict Studies Association Feb. 1, 2006), *available at* http://www.docstoc.com/docs/445063/when-is-a-cyberconflict-an-armed-conflict; Michael N. Schmitt, *Wired warfare: Computer network attack and jus in bello*, 84 (No. 846) INT'L REV. OF THE RED CROSS 365, 399 (2002); THOMAS C. WINGFIELD & JAMES B. MICHAEL, AN INTRODUCTION TO LEGAL ASPECTS OF OPERATIONS IN CYBERSPACE (Apr. 28, 2004) (unpublished report prepared for Naval Postgraduate School Homeland Security Development Program), *available at* http://bosun.nps.edu/Archimages/5948.pdf; MICHAEL N. SCHMITT, HEATHER A. HARRISON DINNISS & THOMAS C. WINGFIELD, COMPUTERS AND WAR: THE LEGAL BATTLESPACE (June 25-27, 2004) (background paper for Meeting on Current Challenges to International Humanitarian Law, Harvard Univ.), *available at* http://www.ihlresearch.org/ihl/pdfs/schmittetal.pdf; Thomas C. Wingfield, *Legal Aspects of Information Operations in Space*, 9 USAF ACAD. J. OF LEGAL STUD. 121 (1998/1999).

II. APPLYING CURRENT INTERNATIONAL LAW TO CYBERSPACE ATTACKS: FALLING SHORT WITHOUT DEFINITIONS

A. What is Cyberspace?

For the purposes of this article, I define cyberspace as *an evolving man-made domain for the organization and transfer of data using various wavelengths of the electromagnetic spectrum. The domain is a combination of private and public property governed by technical rule sets designed primarily to facilitate the flow of information*.[5] The key feature of cyberspace is that it is a man-made domain designed to transfer data and information.

Information is the reason cyberspace exists, and this feature makes current discussions involving the international law of conflict management, *jus ad bellum*, so different from traditional *jus ad bellum* discussions. Simply put, information is fundamentally different than the traditional tools of war; bits and bytes bear no physical resemblance to bullets and bombs. Michael Schmitt noted that cyberspace threats differ in four ways from traditional threats: (1) computer networks are a new target category, with computer network attacks capable of providing the same results as striking the traditional target with a kinetic weapon; (2) an attack does not have to use kinetic force and can solely involve a command from one computer to the target system; (3) the intended results are often not kinetic and could simply involve the manipulation of data or disruption of a service; and (4) cyberspace threats are not constrained by political boundaries or geography.[6]

I would add four more distinguishing factors between cyberspace threats and traditional or kinetic uses of force: (1) cyberspace attacks can be completed literally at the speed of light; (2) the results of some cyberspace attacks, whether intended or not, can be similar to those involving weapons of mass destruction;[7] (3) the cost of acquiring the equipment and expertise to conduct operations in

---

[5] This definition was developed jointly with my cyberspace law cohort, Major Noah Bledstein at 8 AF/JA. Major Bledstein has been working on cyberspace law issues since 2003. His assistance in discussing and developing the ideas and definitions in this paper was invaluable. It does not specifically address the issue of whether some part or all of cyberspace should be considered a global commons.

[6] Schmitt, *Computer Network Attack*, *supra* note 4, at 888.

[7] Because the infrastructure of modern societies relies on the technology and data which can be easily targeted during a cyberspace operation, the disabling of such infrastructure or manipulation of data could cause substantial damage and harm to a society. For example: disabling air traffic control systems or the systems which control the water flowing from a large dam, manipulating the data relied upon by banks or the International Monetary Fund, or manipulating the DNA coding for the subsequent year's flu vaccine.

cyberspace is *de minimis* in comparison to fielding conventional forces; and (4) attributing the attack to the responsible party and determining whether the attack was intentional or accidental is extremely difficult.[8]

The attribution problem, which this article discusses throughout, is indeed the elusive factor that most severely complicates the application of international law. In fact, the attribution problem makes cyberspace so different from other mediums or domains that it requires an entirely new international law approach. The unique nature of the cyber domain impacts not only national level decisions but also the development of law in this area, as evidenced by the current state of law regarding cyberspace and conflict management, which is discussed below.

B. Current Legal Approaches to Cyberspace Attacks

The majority of scholars considering attacks in cyberspace have used an ambiguous, effects-based analytical approach relying on international law to determine what constitutes a "use of force" under Article 2(4) of the U.N. Charter or whether an "armed attack" occurred under Article 51 of the U.N. Charter.[9] The discussions and articles have also looked to other treaties that comprise international law and the law of war, such as the Hague Conventions and the Geneva Conventions. On first impression, an effects-based approach to the issue that relies on

[8] A nuance of limited attribution is that much of the public is unaware of what is going on in cyberspace. In the other domains where military operations are conducted, the activities are much more visible. However, in cyberspace, we can't easily spot electrons and data packets whisking by us or through a phone line.

[9] *See supra* note 4. A brief description of two of the leading approaches follows: First, Gary Sharp's approach recognizes that a use of force in cyberspace may rise to the threshold of an armed attack, depending on its "scope, duration, and intensity," which are factors previously relied upon by the United States (*See infra* note 28). Mr Sharp suggests relying upon an analysis of how states have responded in previous cases to help analyze whether an unlawful use of force or armed attack have occurred, essentially relying on a normative analysis. Mr Sharp summarizes his test by stating: "What constitutes a use of force of a scope, duration, and intensity that constitutes an armed attack and triggers the law of armed conflict is a question of fact that must be subjectively analyzed in each and every case in the context of all relevant law and circumstances." SHARP, *supra* note 4, at 69. Michael Schmitt's analytical approach involves six factors which are used to "delimit" economic/political coercion from determining what is a use of armed force: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy. Mr Schmitt's premise for using an effects based approach primarily rests with his assessment that the U.N. Charter was not directly focused on outlawing "force" but rather the "deleterious consequences" of state actions, and outlawing uses of force under Article 2 was a "prescriptive short-hand to achieve their goals." Schmitt, *Computer Network Attack*, *supra* note 4, at 911. I would recommend that all practitioners in this area read both works. Mr Sharp's book is especially invaluable as a thorough review of international law that applies to cyberspace operations.

international law seems to make sense, since it is electromagnetic data that moves through cyberspace and then creates an electromagnetic effect at the terminating point. The actors certainly focus on what effects they can achieve in and through cyberspace. These effects-based approaches add considerable value to the discussion of the issue, but they are unnecessarily constrained by relying primarily on legal documents and customary international norms developed before the advent of mass-produced computers.

The only substantial international legal document developed to address issues related to cyberspace is the European Union's Convention on Cybercrime[10] (Cybercrime Convention). While the Cybercrime Convention does not address cyberspace attacks as possible acts of war and instead focuses on criminal acts, it does help establish a framework for a new methodology of analyzing cyberspace attacks. Instead of focusing on the end result of a cyberspace event, the effects, and trying to determine whether such an act is a use of force or armed attack under international law, a criminal law methodology places increased emphasis on the genesis of a cyberspace event. The criminal law approach thus focuses on defining the beginning of a cyberspace event and not the effects, and those definitions can then be applied to international law and military operations in cyberspace.

Before discussing the benefits of the criminal law approach, however, one must first understand how most commentators are currently applying international law to actions in cyberspace. A review of current scholarship on this issue will show the difficulty in applying decades old terms and norms to actions in cyberspace. As a starting point, Article 2(4) of the U.N. Charter provides that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."[11]

However, without international sanctions there is little incentive for a party to comply with Article 2(4)'s peaceful objectives.[12] The

---

[10] Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[11] U.N. Charter art. 2, para. 4

[12] *Id.* Art. 1 of the Charter states the purpose of the Charter. Subparagraph 1 specifically states:

> To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.

historical reality is that most state actors have not conducted themselves as though they feared some form of international punishment for their actions. By itself, Article 2(4) seems, therefore, to create very little deterrent effect in conflict management.

However, in contrast to Article 2(4), Article 51 permits parties to act in self-defense in response to an "armed attack."[13] Pragmatically, this right of self-defense can have the quickest success at reducing illegal uses of force constituting breaches of the peace, thereby increasing the deterrent effect of international law.[14] While it is important to analyze whether a state action is a threat or use of force, the more critical question is whether the action is an armed attack, authorizing the recipient to respond in self-defense? The right of self-defense puts other states on notice that their offensive actions could be met with military force.

The right of self-defense has historically been limited by the reality that smaller nation states would respond against bigger and more powerful states with conventional force only if an attack truly jeopardized its national survival.[15] This could be called the "bully dilemma" of international law.[16] The "bully dilemma" pragmatically disenfranchises smaller and weaker states from the protection of Article 51. If a "bully" state engages in a small-scale breach of the peace against a significantly smaller state that smaller state will likely

---

[13] Mr. Sharp reasons "a state never loses its right to use force in self-defense in response to a use of force within the meaning of Article 2(4), however, the right of self-defense under customary international law may not always justify an armed response." Mr. Sharp recognizes that his position may not be held by all and that any right of self-defense is limited by the principles of proportionality and necessity. SHARP, *supra* note 4, at 48-49.

[14] When there is a threat or use of force under Article 2, the United Nations can impose sanctions, to include armed intervention under Chapter 7. However, building the consensus for such actions often takes considerable time and debate, while the victims of such use of force wait for relief. Even the liberation of Kuwait took more than six months before U.N. authorized forces began significant operations to remove Iraqi forces.

[15] For example, when the United States launched cruise missiles against Sudan and Afghanistan in August 1998, neither country responded with conventional force. The codename for the operation was "Infinite Reach." What if Sudan had then possessed a capability to respond in cyberspace? How could Sudan respond in cyberspace, and would the U.S. have countered, if attribution could be obtained?

[16] Mr Sharp, on page 52 of CYBERSPACE AND THE USE OF FORCE, *supra* note 4, concluded the third chapter of his book by stating "[t]here is no black and white, mechanical rule in the law of conflict management that clearly defines what a use of force is under all circumstances." He then followed that statement by using the opposite of the "bully dilemma" to demonstrate his conclusion that a use of force is a question of fact which must be subjectively analyzed: "For example, a state's activity that is lawful against another state of equal size may nevertheless be significant enough against a smaller state to cross Article 2(4)'s 'political independence' threshold." A subjective "size matters" approach to law provides no clarity and leaves smaller states wondering whether they can seek international assistance or defend themselves.

acquiesce to the aggression. The smaller state will likely determine that it is better to suffer outright defeat than to attempt to stop the aggression and fail. Meanwhile, as noted above, sanctions under the U.N. Charter are rarely invoked against the "bully" state, especially when the "bully" state is a permanent member of the U.N. Security Council and therefore holds a veto.

However, in contrast to the historical "bully dilemma," as depicted above, the asymmetric nature of operations in cyberspace now allows any party to possess the capability to swiftly act in self-defense with incredible lethality. The "bully" could soon be extinct and a new era of conflict could unfold, where the appearance of parity could inspire more breaches of the peace.[17] This is why the development of law in this area must move forward.

C. Looking to Jus in Bello to Define Armed Attack

The potential lethality of cyberspace responses and unique attributes of cyberspace should compel international lawyers to consider the right of self-defense against cyberspace attacks in light of both the *jus in bello* and *jus ad bellum*. Beginning with *jus in bello*, the focus of the examination is whether the current laws and definitions provide sufficient clarity to help nation states resolve what is an armed attack in cyberspace. Unfortunately, international law fails to define "armed attack". The Geneva Conventions and additional documents relating to the Law of Armed Conflict (LOAC), *jus in bello*, do provide definitions of related terms that can clarify what international law would likely consider an armed attack. The Geneva Conventions and Additional Protocols are "not a separate paradigm of conflict management," but are focused on *jus in bello* issues.[18]

Article 49 of Additional Protocol I to the Geneva Conventions (Protocol I) defines "attack" as "acts of violence against the

[17] To use a college football analogy, the spread of the "West Coast Offense" to many universities has resulted in non-traditional powerhouse programs rising up and defeating Goliaths of the gridiron. Boise State University's BCS victory over the University of Oklahoma highlights how smaller teams with allegedly lower quality recruits can use a new method of attack to level the playing field. In cyberspace operations, what is to stop a small nation state from responding with a non-attributable cyberspace operation in response to perceived threats or incursions by a "bullying" superpower? Even if the smaller state is questioned, it could respond that it is acting in self-defense to what it considered an armed attack with necessary actions to protect it from further harm. Such an asymmetric shift in warfare could result in an increasing number of "cyberspace conflicts" much like the low intensity conflicts of the 1980s. However, the capacity for "cyberspace conflicts" to rapidly escalate in lethality, due to self-defense actions, could be an incentive for nation states to instead look for a model that promotes deterrence.

[18] SHARP, *supra* note 4, at 77.

adversary."[19] The official commentary for Protocol I further adds that the definition "refers simply to the use of armed force to carry out a military operation."[20] Note that because this definition requires the use of armed force, non-military personnel hacking into the New York Stock Exchange and causing substantial economic harm would not be an attack.[21] Such an application identifies practical limitations with the current definition in Article 49.

Common Article 2 of the four Geneva Conventions states that the Conventions shall apply during "any other armed conflict," yet that term is not well defined in the conventions.[22] The official commentary to Common Article 2 helps in understanding what is an armed conflict and states that "de facto hostilities" are sufficient. The commentary then makes clear the Conventions' intention for a low threshold and broad application of the term "armed conflict":

> The substitution of this much more general expression for the word "war" was deliberate. One may argue almost endlessly about the legal definition of "war." A

---

[19] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, *available at* http://www.icrc.org/ihl.nsf/FULL/470?OpenDocument. The United States has not ratified Protocol I, but it is accepted as customary international law. It is interesting to note that Article 49 further states:

> [The] provisions of this section apply to any land, air or sea warfare which may affect the civilian population, individual civilians or civilian objects on land. They further apply to all attacks from the sea or from the air against objectives on land but do not otherwise affect the rules of international law applicable in armed conflict at sea or in the air.

Id. International law recognizes distinctions with regard to conducting hostilities in the domains of air and sea, yet there is no strong movement for international recognition of the distinctive qualities of the domain of cyberspace.

[20] Commentary for Protocol I, art. 49, para. 1882, *available at* http://www.icrc.org/ihl.nsf/WebList?ReadForm&id=470&t=com.

[21] Even in 1977, international law failed to grasp the importance of economic battles that could bring a country to its knees.

[22] The four Geneva Conventions were signed on 12 August 1949. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287. The Conventions and their commentaries are available on the International Committee of the Red Cross (ICRC) web page at: http://www.icrc.org/ihl.nsf/CONVPRES?OpenView. The Geneva Conventions represent customary international law with regard to the conduct of armed hostilities or *jus in bello*.

> State can always pretend, when it commits a hostile act against another State, that it is not making war, but merely engaging in a police action, or acting in legitimate self-defence. The expression "armed conflict" makes such arguments less easy. Any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place.[23]

In addition to the above statement, each of the four commentaries to the Geneva Conventions provides slightly different amplifying language for Article 2. This is, no doubt, due to the specific context of each of the four Geneva Conventions. For example, with respect to the First Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, the Commentary adds:

> The respect due to human personality is not measured by the number of victims. Nor, incidentally, does the application of the Convention necessarily involve the intervention of cumbrous machinery. It all depends on circumstances. If there is only a single wounded person as a result of the conflict, the Convention will have been applied as soon as he has been collected and tended. . . .[24]

---

[23] Commentary to Article 2 of the four Geneva Conventions. The quoted language is repeated in paragraph 1 of the commentary for Article 2 of each of the four Geneva Conventions. Commentary for Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, art. 2, para. 1, *available at* http://www.icrc.org/ihl.nsf/COM/365-570005?OpenDocument; Commentary for Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, art. 2, para. 1, *available at* http://www.icrc.org/ihl.nsf/COM/370-580005?OpenDocument; Commentary to Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, art. 2, para. 1, *available at* http://www.icrc.org/ihl.nsf/COM/375-590005?OpenDocument; Commentary to Geneva Convention relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, art. 2, para. 1, *available at* http://www.icrc.org/ihl.nsf/COM/380-600005?OpenDocument.

[24] *Id.* Paragraph 1 of the commentary for Article 2 of the Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12 1949, provides almost identical language, with a minor distinction regarding shipwrecked persons: "If there is only a single shipwrecked person as a result of the conflict, the Convention will have been applied as soon as he has been collected and tended. . . ." Paragraph 1 of the commentary for Article 2 of the

Thus, what is clear from the Commentaries regarding when an "armed conflict" has occurred is not the number or persons involved or whether the parties are using "cumbrous machinery", such as tanks, rockets, planes, etc., or "even if there has been no fighting," but simply whether there is "[a]ny difference arising between two States and leading to the intervention of armed forces." Further, a consistent theme is that "armed conflict" usually involves some sort of negative impact on at least one person, even if it is a civilian victim. The Commentary language begs the question—a question not answered—what is "intervention of the armed forces?"

In sum, this discussion of the Geneva Conventions as they relate to *jus in bello* reveals that "armed conflict" is an activity that involves acts of violence between armed forces, which affect at least one person, regardless of the amount of damage or suffering inflicted. Overall, the threshold is quite low and certainly does not require significant damage or loss of life. The policy concern to protect people from the harsh effects of conflict most likely inspired such a low, almost bright-line approach. While the definitions and Official Commentaries of the Conventions help explore the issue, the U.N. Charter remains the principal document for analyzing *jus ad bellum* issues relevant to the armed attack determination.

D. Armed Attack and Jus ad Bellum

Unfortunately, the U.N. Charter itself provides very little by way of definition when it comes to the term, "armed attack." Moreover, no official commentary addresses the issue. However, one place scholars have turned for clarification is the U.N. General Assembly's 1974 resolution defining aggression, Resolution Number 3314. In that resolution, the General Assembly defined aggression as the "use of armed force by a State against the sovereignty, territorial integrity, or

---

Convention (III) Relative to the Treatment of Prisoners of War, Aug. 12 1949, provides the following minor distinction:

> It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces; it suffices for the armed forces of one Power to have captured adversaries falling within the scope of Article 4. Even if there has been no fighting, the fact that persons covered by the Convention are detained is sufficient for its application. The number of persons captured in such circumstances is, of course, immaterial.

Paragraph 1 of the commentary for Article 2 of the Convention (IV) Relative to the Protection of Civilian Persons in Time of War simply clarifies with regard to civilians that the "respect due to the human person as such is not measured by the number of victims."

political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."[25] More importantly, the resolution provides a number of specific acts that constitute aggression, including, but not limited to:

> Invasion, attack or military occupation; bombardment or the use of any weapons against a State; blockade; an attack on the land, sea, or air forces or the marine and air fleets of a State; and the sending of armed bands, groups, irregulars or mercenaries to complete any of the previous acts.[26]

The resolution states that it may limit a finding of aggression in light of relevant circumstances, such as when the act is not of "sufficient gravity." The pragmatic tone of this qualifying language is more consistent with how nation states subjectively conclude whether an armed attack occurred.[27] The term "sufficient gravity" may be an unintended endorsement of the "bully dilemma." Thus, the "bully" state again avoids accountability when the international community determines its small-scale aggression is not of "sufficient gravity," i.e. the international community is not sufficiently concerned about their own safety and security. Unfortunately, subjective conclusions do not add much clarity to resolving what acts would be considered an armed attack in cyberspace. As noted above, such definitional clarity is essential to aiding all states in understanding which acts in cyberspace can result in self-defense actions. If there was a legal framework, which created a clearer understanding of one's accountability in cyberspace, there would be a greater likelihood of deterring states from acting

---

[25] G. A. Res. 3314, U.N. GAOR, 29th Sess., art. 1 (Dec. 14, 1974) *available at* http://www.un.org/documents/ga/res/29/ares29.htm. This language is almost identical to the language found in Article 2(4) of the UN Charter.

[26] *Id*. art. 3.

[27] Mr Sharp accurately notes that the United States uses the factors of scope, duration and intensity to determine whether de facto hostilities exist, but notes that the application has been inconsistent. When a Navy A-6 crew was shot down over Syria in 1983 and one of the crew members was captured, the U.S. claimed POW status for Lt Goodman and stated that "'armed conflict' includes any situation in which there is hostile action between the armed forces of two parties, regardless of the duration, intensity **or** scope of the fighting." (emphasis added by this author) This is contrasted with the later U.S. position regarding the status of Chief Warrant Officer 3 Michael Durant as an unlawful detainee, since the U.N. operations in Somalia "did not rise to the level of de facto international armed conflict." SHARP, *supra* note 4, at 61-62. Essentially, Mr Sharp's position is that the U.S. position has evolved and now relies on the conjunctive "and" when applying the three factors of scope, duration, and intensity, versus the disjunctive "or."

aggressively in cyberspace, because they would know which acts could result in a cyberspace self-defense action.[28]

Whether one looks to the "Schmitt analysis" using six factors or Sharp's approach of "heuristic analysis" to develop a profile of how states apply the factors of scope, duration, and intensity to the U.N. Charter and Common Article 2 framework, there appears to be no clear answer in contemporary international law. Mr Sharp, quoting Ian Brownlie, attempted to illustrate how international law can be applied during an international incident: "the minor nature of an attack" helps to prove the "intention to attack, of honest mistake, or simply the limited objectives of an attack."[29] Brownlie's observation made sense in the days of conventional weapons and minor border skirmishes or incursions. One or two shots fired by a border guard versus dropping two 1,000 pound bombs can circumstantially help determine intent. Generally, with such kinetic attacks, the first or second order effects are readily discernable. However, warfare has changed and a new domain has evolved.

In cyberspace, what may appear as a "minor attack" could evolve into something much more destructive to a nation state, taking days or months to cause observable, significant harm. Weapons of mass destruction, terrorist attacks, and cyberspace attacks are quite different from the traditional methods of massing forces and building up logistics trains and lines of communication. States can much more easily identify preparation for a kinetic invasion versus a cyberspace onslaught. Asymmetric warfare may require asymmetric application of the law to provide the clarity and enforceability capable of promoting peace. The development of international law related to activities in cyberspace should not be delayed any longer. [30]

And why is finding a legally clear answer so difficult? In his writing, Sharp recognizes the concerns with a strict interpretation of Common Article 2, since such a "rote" application of the Article 2 threshold "intentionally causes military personnel to become belligerents and lawful targets even though they are conducting a peacetime military operation."[31] Sharp's concern regarding a strict

---

[28] Recall the conclusion of *supra* note 17 regarding how the asymmetric nature of cyberspace warfare could result in an increasing number of conflicts, all with the potential of having substantially greater effects than traditional low intensity conflicts. This asymmetric nature has created a potential deterrence vacuum, which the law must attempt to fill and states must then enforce.

[29] SHARP, *supra* note 4, at 66 (quoting IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES, 366 (1954)).

[30] I refer the reader to the two lead-off quotes at the beginning of this article. The lack of clear, enforceable law will only embolden activities in cyberspace and increase international tension and the likelihood of substantial physical damage in addition to the on-going intellectual carnage.

[31] SHARP, *supra* note 4, at 65-66.

application of Common Article 2 to *jus ad bellum*, conflict management, is certainly justified with regard to the evolution of conventional military activities, such as peacekeeping and peacemaking.

Cyberspace operations, however, do not create the same concerns related to peacekeeping operations. There has been no move to create a U.N. "cyberspace peacekeeping force" to engage in online actions to enforce U.N. resolutions or sanctions, and cyberspace forces are not conducting humanitarian missions. In addition, neither Common Article 2, the U.N. Charter, nor the U.N. definition of aggression are contemporary enough to be strictly applied to activities in cyberspace, since they lack definitions applicable to the unique methods used in cyberspace operations. Nevertheless, the policy objective and low threshold of Common Article 2 provide hope that international law is capable of applying a stricter, definition-based approach to cyberspace attacks. The need for a legally clear answer should help shift the focus from an ambiguous, effects-based approach that relies solely on international law to the development of a definition-based approach capable of consistent application to cyberspace operations that affect other states.

E. Weapons are the Key

The U.N. General Assembly's defined aggression to include the use of "any weapons" against another state. The use of such a clearly broad term as "any" logically implies that the use of even minor weapons against a state could be considered an act of aggression, if the circumstances are of "sufficient gravity." Leaving aside the inevitably ambiguous discussion of events that may be of "sufficient gravity" in the eyes of the U.N. General Assembly, the General Assembly's inclusion of the use of weapons in its definition of aggression brings the discussion regarding armed attacks in cyberspace back to the initial proposal of analyzing cyberspace attacks using the criminal law model.

The criminal law model's reliance on clear definitions requires us to focus on the causative event, versus emphasizing the effects. For example, a crime is committed when a person fires a gun toward another, regardless of whether the other person is actually struck by a bullet. The minimum crime is some type of assault, likely an aggravated one, in the absence of a legal defense. If the person is struck by the bullet (effect of attack) or other circumstances are developed to indicate a more serious intent, then the chargeable crimes range from aggravated assault to murder. As this example demonstrates, under a criminal law approach, a crime (attack) occurred under all of the factual variations. The increase in harm (effect) only increases the level of punishment the offender may face from society and does not influence whether a crime of some sort occurred.

Regardless of the severity of the crime (attack), societies have long recognized the policy interest in taking measures to respond to and deter crimes. This deterrence objective is a philosophical difference between a criminal law approach and an effects-based approach relying on international law. International law, relying upon an effects-based threshold, is implicated only when an incident's consequences rise above a certain threshold. Whereas the criminal law model reacts even if there is just an attempt to commit a prohibited act. Thus, a criminal law approach focuses on the actual act and the method used, whether accessing a computer without proper authorization or robbing a bank with a gun. Relying on the criminal law approach allows one to examine the genesis of an attack at an even deeper level. The criminal law approach strives to provide clarity and consistency, allowing all members of a society to know what conduct is prohibited, which also serves the additional objective of deterrence. In the case of defining cyberspace attacks, a consideration of cyberspace weapons is the key to providing such clarity.

The use of a weapon of some kind is the true genesis of an attack. In fact, the types of weapons available to a state determine the possible attack methodologies.[32] Thus, studying weapons is also important to understanding the strategy of potential adversaries. However, for the purpose of providing clarity to the issue of armed attacks in cyberspace, the definition of what is a weapon in cyberspace becomes the foundational question to developing a new approach to international law affecting cyberspace operations.

While the U.N. General Assembly used the term "any weapon" and provided no further definition of what constitutes a weapon, one can turn to the law of armed conflict (LOAC) for assistance. Based on the LOAC's specific guidance regarding conventional tools of war, conventional militaries tend to have a practical understanding of what are lawful and unlawful weapons. For example, exploding bullets and poisonous gas are unlawful weapons.[33] The LOAC focuses, however, almost completely on kinetic weapons.

Despite its narrow focus on kinetic weapons, the LOAC has nevertheless struggled to define a "weapon," and there is currently no

[32] For example, possessing and being able to field deep strike kinetic weapons such as low observable bombers opens up a range of options for a state actor. Likewise, possessing and being willing to use suicide bombers or biological weapons creates a tactical (asymmetric) advantage over adversaries. Thus, being able to conduct operations in cyberspace creates a new line of attack methods.

[33] Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land, Oct. 18, 1907, art. 23, *available at* http://www.icrc.org/ihl.nsf/FULL/195?OpenDocument [hereinafter Hague Regulation (IV)]. Article 23 outlaws weapons that cause unnecessary suffering. *See also* Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, Geneva, June 17, 1925.

accepted definition under international law. Instead, Article 36 of Protocol I requires a review of any "new weapon, means or method of warfare" to ensure its use would comply with international law.[34] Although the United States has not ratified Protocol I, customary international law requires the review of weapons .[35]

The International Committee of the Red Cross (ICRC) has noted that each state tends to have its own definition of "weapon."[36] Even within the U.S. Department of Defense (DoD) there is no standard definition of "weapon."[37] Thus, each service developed its own definition of weapon, which it uses to determine whether a means or method of warfare requires a legal review in accordance with Article 36 of Protocol I. In the Air Force, paragraph 1 of Air Force Instruction 51-402, Weapons Review, 13 May 1994, defines weapons as "devices designed to kill, injure, or disable people, or to damage or destroy property." The definition specifically excludes "electronic warfare devices." The definition also differentiates between effects on people and effects on property, failing to include devices that "disable" property. Meanwhile, the United States Army and Navy each provide a definition of weapon that specifically includes devices that "disable" property.[38] Thus, the Army and Navy definitions appear to be more

---

[34] Throughout the remainder of the discussion, the term "weapon" will be used in lieu of the broader term, "weapon, means or method of warfare."

[35] INT'L & OPERATIONS LAW DIV., OFFICE OF THE JUDGE ADVOCATE GENERAL, DEP'T OF THE AIR FORCE, AIR FORCE OPERATIONS & THE LAW 25, 48 (1st ed. 2002). Pages 25 and 48 provide a list of which Articles of Protocol I the United States does not accept as customary international law. Those articles are: 1(4), 35(3), 39(2), 44, 47, 55, and 56. For a detailed discussion on the U.S. position regarding these provisions, *see* Michael J. Matheson, *The United States Position on the Relation of Customary International law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 Am. U. J. Int'l L. & Pol'y 419, 420 (1987).

[36] INT'L COMM. OF THE RED CROSS, A GUIDE TO THE LEGAL REVIEW OF NEW WEAPONS, MEANS AND METHODS OF WARFARE, MEASURES TO IMPLEMENT ARTICLE 36 OF ADDITIONAL PROTOCOL I OF 1977 9 (2006) [Hereinafter ICRC GUIDE ON NEW WEAPONS].

[37] Apparently, U.S. DEP'T OF DEF., INSTR. 5500.15, REVIEW OF LEGALITY OF WEAPONS UNDER INTERNATIONAL LAW (16 Oct. 1974) is no longer a current publication and the author was not able to locate a successor instruction. However, according to page 9 of the ICRC GUIDE ON NEW WEAPONS, *supra* note 36, the DOD Law of War Working Group proposed a definition which included "all arms, munitions, materiel, instruments, mechanisms, or devices that have an intended effect of injuring, damaging, destroying or disabling personnel or property."

[38] U.S. DEP'T OF ARMY, REG. 27-53, REVIEW OF LEGALITY OF WEAPONS UNDER INTERNATIONAL LAW, para. 3.a. (1 Jan. 1979), defines a weapon as: "Chemical weapons and all conventional arms, munitions, materiel, instruments, mechanisms, or devices which have an intended effect of injuring, destroying, or disabling enemy personnel, materiel, or property." U.S. DEP'T OF NAVY, SEC'Y OF THE NAVY INSTR. 5000.2C, IMPLEMENTATION AND OPERATION OF THE DEFENSE ACQUISITION SYSTEM AND THE JOINT CAPABILITIES INTEGRATION AND DEVELOPMENT SYSTEM, para. 2.6.2 (19 Nov. 2004) defines a weapon as: "all arms, munitions, materiel, instruments, mechanisms, devices,

closely aligned with the foreseeable type of military operations that could occur in cyberspace, i.e. operations that disable or destroy systems by manipulating or corrupting the data relied upon by the system.

III. The Key to this Puzzle: Cyberspace Weapons and the Criminal Law Definition-Based Model

A. Defining Cyberspace Weapons

The criminal law approach and methodology help resolve the issues of ambiguity, enforceability, and attribution for two reasons. First, it provides strong definitions that can withstand judicial scrutiny and allow for fair application to a variety of fact patterns. A nuance of this first strength is that criminal law definitions must also clearly put everyone on notice as to prohibited activities. The second strength is that the criminal law methodology requires the definition of a prohibited act to have some degree of intent, also known as the scienter element. Relying on these strengths, the criminal law approach creates a definition of a cyberspace crime that is clear, flexible, and requires a minimum level of intent. The criminal law methodology will then enable us to reverse engineer the definition of a cyberspace crime in order to establish the definition of a cyberspace weapon.

As noted earlier, the European Union's Convention on Cybercrime is an international treaty intended to create consistency in criminal laws related to internet activities. Unfortunately, the Cybercrime Convention does not offer a definition of malicious logic or cyberspace weapon. Instead, the Cybercrime Convention identifies specific activities states should criminalize. Logically, the reason to prohibit certain activities is to avoid unwanted effects. The criminal law methodology is able to transform unwanted effects into specific definitions and prohibitions, whereas the current approach under international humanitarian law relies on an ambiguous analysis of facts using undefined prohibitions.

The intent of the Cybercrime Convention was to set up a basic framework whereby the parties agreed to create their own state criminal codes to address broadly defined prohibited activities. Because the Convention defines prohibited activities broadly, it does not provide the detailed definitions of actual effects in cyberspace necessary to specifically define a cyberspace weapon. Nevertheless, the Convention's aspirational criminal law definitions of unlawful activity in cyberspace can help identify the international community's thoughts

---

and those components required for their operation, that are intended to have an effect of injuring, damaging, destroying, or disabling personnel or property, to include non-lethal weapons."

regarding unlawful cyberspace effects and thus the weapons that cause those effects. By looking at what types of activities the Cybercrime Convention intends to criminalize, it is possible to reverse engineer the definition of a cyberspace weapon.

Specifically, the Cybercrime Convention provides that the parties will adopt laws that criminalize cyberspace crimes such as: unlawful access, unlawful interception, interfering with data or systems, and computer fraud or forgery.[39] Looking at the broad definitions for these offenses under the Cybercrime Convention, terms such as "obtaining," "damaging," "deleting," "deteriorating," "altering" or "suppressing" data represent a common theme of what happens to electromagnetic data when a cyberspace crime occurs.[40]

This criminal law framework parallels the scenarios discussed by many others with regard to armed attacks in cyberspace. For example, the U.S. Department of Defense defines Computer Network Attack as: "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[41] Whether a cyberspace crime or a cyberspace attack, the goal is to affect someone else's data, or use data to affect property.

The domain of cyberspace is obviously not as physically transparent as the domains of air and space. If one were to try and "fire" one million volts at a cyberspace target, there are too many information nodes, such as routers and switches, along the internet pathway that would become the unintended recipient of the "electromagnetic missile." The one million volt "electromagnetic missile" would cause

---

[39] *See* Convention on Cybercrime, *supra* note 10, at arts. 2-8.

[40] *Id.* arts. 4, 5. Article 4 provides:

> Data interference: 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 provides:

> System interference: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

[41] JOINT CHIEFS OF STAFF, JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS 113 (17 Mar. 2009) [hereinafter JP 1-02].

collateral damage to those nodes and would be worn down long before it reached its intended target. Cyberspace attacks, just like criminal hacks, are designed to affect electromagnetic data in various ways, which then impact the adversary's cyberspace to create an operational advantage for the attacker. Thus, the basic legal framework of the Cybercrime Convention is beneficial in the context of military operations in cyberspace.

Although the Cybercrime Convention does not provide definitions of key terms such as "damaging" or "altering," the Cybercrime Convention points us to the criminal codes of party states, such as the United States, to specifically define the *actus reus*. The criminal code of the United States is considered for several reasons: the United States invented the internet; the United States is arguably the largest user of cyberspace; the United States is a leading prosecutor of cyberspace crimes; and many nations work with the United States to solve cyberspace crimes.

Section 1030 of Title 18 of the U.S. Code criminalizes intentionally causing damage to a protected computer.[42] Section 1030 is often used by U.S. Attorneys to prosecute persons who steal or corrupt data located on computer systems and persons who engage in denial of service attacks. Section 1030 defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." This definition of "damage" recognizes the reality of what happens during a criminal hack or a cyberspace attack: "damage" in cyberspace does not require smashing, burning, or blowing things up. The U.S. Code provides a clear, judicially accepted and internationally recognized definition of damage in the cyberspace realm. By borrowing from this definition, it is possible to logically develop a definition of a cyberspace weapon, the key to the puzzle.[43]

From the above, we see that in its most simple terms, the definition of a weapon is "something that causes damage." Applying the definition of damage from Section 1030, I propose the following definition of a cyberspace weapon: *Any capability, device, or combination of capabilities and techniques, which if used for its intended purpose, is likely to impair the integrity or availability of data, a program, or information located on a computer or information processing system.*[44] Although the proposed definition uses the term

[42] The definition of a "protected computer" includes computers used exclusively by the U.S. Government or financial institutions. *See* 18 U.S.C. § 1030(e)(2) (2006).

[43] It is important to note again that the U.S. Code sections addressing crimes occurring in cyberspace are generally accepted by foreign law enforcement partners. Therefore, relying on the Title 18 definition of "damage" in cyberspace is a definition that many international partners are already somewhat familiar with.

[44] I again must humbly thank Major Noah Bledstein at 8 AF/JA for his help in developing this definition.

"impair" versus the DOD favored term "disable," the terms are somewhat similar in meaning. The term "disable" requires that a weapon must cause a complete loss of function, while the term "impair" recognizes that malicious software code need only reduce an information system's capability, i.e. degrade.[45]

B. Applying the Definition of a Cyberspace Weapon

Now that we have defined cyberspace weapon, the remaining challenge is to determine whether the proposed definition works within the context of cyberspace operations and within the current limits of international law. While the first instances of negative code may not have been written with the intent of harming a computer, today the story is quite different. Today, the development of computer code that negatively impacts an information system has evolved and spread like an advanced, persistent plague. The tools of the modern hacker, whether criminal, military, terrorist, geek, or spy, are broadly referred to as malicious logic. While malicious logic can take many forms, the key question for our purposes is: "At what point does malicious logic become a cyberspace weapon, the use of which constitutes an armed attack under international law?" The first part of the question focuses not on the end result but on the "tool" used in cyberspace and whether that tool is a "weapon." The second part of the question will focus on the weapon's use in cyberspace.

First, one must consider whether particular cyberspace "tools" constitute weapons under international law. The ICRC Commentary on Article 35 of Additional Protocol I states: "The words 'methods and means' include weapons in the widest sense, as well as the way in which they are used."[46] Furthermore, the ICRC Guide on New Weapons expounds on the above commentary provision by noting that the legal

---

[45] Again, recall that while the services' definitions of weapon all used the term "disable," JP 1-02, *supra* note 41, uses the term "degrade" when describing Computer Network Attack.

[46] Commentary for Additional Protocol I, *supra* note 20, para. 1402 (for art. 35). Article 35 provides overarching guidance regarding the means and methods of warfare and reads:

> Basic rules - 1. In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited. 2. It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering. 3. It is prohibited to employ methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment.

Protocol I, *supra* note 19, at art. 35.

review requirements of Article 36 apply even to non-lethal weapons based on "the ways in which these weapons are to be used pursuant to military doctrine, tactics, rules of engagement, operating procedures and countermeasures" and also applies to all acquired weapons, whether procured based on military specifications or "off-the shelf."[47] Both the Commentary and the ICRC guide conclude that the analysis regarding whether a weapon is lawful or unlawful should be focused on the weapon's "normal or expected use."[48]

Next, one must analyze how the proposed definition of a cyberspace weapon can be applied in the real-world context of two recent "cyberspace attacks" in Estonia and Georgia. Considering the realities of these two events, does the proposed definition provide sufficient clarity for use in international law?

The cyberspace event in April and May of 2007 in Estonia involved a number of distributed denial-of-service (DDoS) actions against the networks for the two largest banks, effectively severing all internet communications for two hours and causing partial interruptions thereafter.[49] The event also included acts against an Estonian government internet service provider that "disrupted government communications for at least a short period of time."[50] Lastly, the web page for the Estonian Prime Minister was "defaced," manipulating it to show an alleged apology for moving a Soviet World War II memorial.[51] Clearly, the event in Estonia resulted in reduced availability and impaired the integrity of the information located on computer systems in Estonia. Applying the attacker's methods to the proposed definition, it is clear these methods constituted "cyberspace weapons."

The cyberspace event that occurred in July and August of 2008 in Georgia results in a similar conclusion. Again, a DDoS event targeted the website of the Georgian President, making it unavailable for 24 hours. Attackers also defaced the website with pictures of Adolf Hitler next to the image of the Georgian President, and, using malicious logic, caused websites for other government agencies to lose connectivity.[52] Here again, the methods used by cyberspace attackers in Georgia caused a loss of access and impaired the integrity of the data. Consequently, it is appropriate to label these methods as "cyberspace weapons." The proposed definition of a cyberspace weapon therefore

---

[47] ICRC GUIDE ON NEW WEAPONS, *supra* note 36, at 9–10.
[48] Commentary for Additional Protocol I, *supra* note 20, para. 1469 (for art. 35).
[49] Kenneth Geers, Cyberspace and the Changing Nature of Warfare, Keynote Speech for NATO Cooperative Cyber Defence Centre of Excellence (CDCOE) 9 (Oct. 13, 2008), available *at* http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf (NATO CDCOE can be accessed on the Internet at http://www.ccdcoe.org).
[50] *Id*.
[51] *Id*.
[52] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, *supra* note 2, at 28-33.

provides the degree of clarity to move the discussion forward to defining a cyberspace attack.

C. When is the Use of a Cyberspace Weapon a Cyberspace Attack?

Acknowledging that cyberspace weapons were used in the events in Estonia and Georgia does not answer the ultimate question of whether the acts should be considered armed attacks under international law? Here again, the temptation is to return to an effects-based analysis to answer the question. However, as noted at the beginning of this article, previous attempts to answer the question using such an analysis provide ambiguous answers at best. Instead, by applying a definition-based approach, much like the criminal law does, there is a higher likelihood of reaching a clear answer. Therefore, in order to determine when the use of a cyberspace weapon constitutes an "armed attack" under international law, one must look to how the cyberspace weapon is used rather than its effects.

This question of how a weapon is used is the key transitional point in this analytical approach and borrows substantially from the criminal law. For example, a gun can either be a weapon used to kill people or a weapon used to assist a hunter in gathering food. The intent of the user remains the primary issue under the criminal law. Using this criminal law approach will enable conversion of the above question into a definition applicable to the international law arena.

To prove an offense under the criminal law, almost all crimes require proof of *mens rea*, the idea of a criminal intent or purpose. Specifically, most crimes require proof of either specific or general intent or knowledge. The most difficult *mens rea* to prove is specific intent, whereas knowledge is much more easily inferred from the circumstances. Considering history and the unwillingness of state actors to admit their actual intent, proving the specific or general intent of a state actor is very difficult when relying on circumstantial evidence, and would therefore result in an unenforceable definition beneficial only to academic discussions.

Therefore, because proof of knowledge is easier to prove than either a specific or general *mens rea*, it will lead to a more enforceable standard and place a higher level of responsibility on states. Even though knowledge is a lower threshold than specific or general intent, it is nevertheless a common and accepted *mens rea* requirement under criminal law. Still, the question remains, knowledge of what? As will be discussed further below, state actors have a responsibility, as sovereigns with power and control, to conduct their affairs with due regard for their international legal obligations when they have knowledge of activities within their legal or physical boundaries. Hence, it is appropriate to consider the following definition of a

"cyberspace attack": *A cyberspace attack occurs when a state knowingly uses or knowingly acquiesces to an entity under its legal control or within its territory using a cyberspace weapon against the people or property of another state.*

The proposed definition of cyberspace attack essentially imposes additional responsibility under international law when a state knowingly allows a person or entity to use a cyberspace weapon against the people or property of another state. Under the unique circumstances of cyberspace, such a clear definition establishes the increased degree of responsibility necessary to promote international peace and help deter the myriad of adverse activities in cyberspace. Consider the actions of one rogue group if they were to successfully conduct a cyberspace attack against the critical infrastructure of another state. Regardless of the group's motives, whether nationalistic, ideological, or criminal, causing the death of several hundred people and millions of dollars worth of property damage is a scenario that international law must evolve to address and deter. Still, if the state is completely unaware of a rogue element's activities, then it seems appropriate not to impart responsibility and accountability under international law.

However, what if the state that can legally control the rogue element knew that the element was about to or was currently engaging in a cyberspace attack against persons or property in the victim state? The responsible state could, if necessary, disrupt all communications originating from the rogue element or emanating from the state until it could locate and arrest the attackers for violating their domestic laws. The definition of a cyberspace attack, although similar to the definition of a cyberspace crime, is not intended to hold states responsible for the nefarious efforts of criminals, unless the state is aware of the criminal's efforts and knowingly acquiesces to the use of a cyberspace weapon. The objective is to develop a legal framework that inspires states to cooperate to eliminate the harmful use of cyberspace—to create deterrence.

Without the proposed legal framework, why should a state try to stop an impending cyberspace attack against another state? Under current state practice, if the victim state is an "ally," then the responsible, "host" state will likely feel much more compelled to take positive steps to stop the attack. For example, if a hacker in the United Kingdom was conducting a cyberspace attack against the Hoover Dam in the United States, U.K. security and law enforcement officials would almost certainly act with all diligence to stop the attack and arrest the perpetrators, and would likely allow their extradition to the United States.[53] However, how many cyberspace events against entities in the

[53] For example, the extradition of Scottish national Gary McKinnon is still pending in the United Kingdom. It is alleged that McKinnon completed one of the largest "hacks"

United States has the People's Republic of China informed the United States about, and how many times have they stopped and subsequently arrested the offenders? This question indicates the problem with the current model of international law that relies on state practice, subjective assessments, alliances and the "bully dilemma." International law is currently too vague, as noted by the lead-off quote from the U.S.-China Economic and Security Review Commission.

Some argue that international law may not be inclined to place such a clear responsibility on states for acquiescing to uses of cyberspace weapons, unless they caused effects equivalent to more traditional armed attacks.[54] However, the U.N. has issued resolutions that appear to place a higher burden on states to refrain from acquiescing to certain acts committed from their territory against other states. For example, a General Assembly Resolution in 1970, number 2625, discussed *acquiescence* and said that states have a duty to refrain from acquiescing or tolerating actions from within its territory that cause civil strife in the other state.[55] More recently, the United Nations

---

of U.S. military servers in 2001 and 2002. News.scotsman.com, *Scottish Hacker Gary McKinnon Loses US Extradition Battle*, July 31, 2009, http://news.scotsman.com/latestnews/Scottish-hacker-Gary-McKinnon-loses.5512684.jp (last visited Sept. 3, 2009).

[54] "Mere acquiescence would not constitute an armed attack, but using information infrastructures to help arm or train insurgents would constitute an armed attack." SHARP, *supra* note 4, at 112.

[55] G.A. Res. 2625, U.N. GAOR, 25th Sess. (Oct. 24, 1970). The key excerpts from the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among states in accordance with the Charter of the United Nations are:

> Every State has a duty to refrain from organizing, instigating, assisting, or participating in acts of civil strife or terrorist acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force . . . .
>
> Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State. . . .
>
> States have the duty to co-operate with one another, irrespective of the differences in their political, economic and social systems, in the various spheres of international relations, in order to maintain international peace and security . . . .
>
> All states enjoy sovereign equality. They have equal rights and duties . . . .
>
> The principles of the Charter which are embodied in this Declaration constitute basic principles of international law . . . .

Security Council issued Resolution 1373 on September 28, 2001, which reaffirmed the key principles in Resolution 2625. Resolution 1373 decided under Chapter VII of the United Nations Charter that all states shall take the necessary steps to prevent terrorist acts, to prevent terrorists from using their territories for terrorist purposes, and to provide early warning to other states.[56]

Although not directly on point with all scenarios of cyberspace attack, some cyberspace attacks could fit within the resolutions' already accepted prohibitions related to harboring terrorists, preventing use of territory by terrorists, and acquiescing to those who cause civil strife. The proposed definition of armed attack in cyberspace would really only increase the degree of state responsibility for non-state actors by a small amount. In light of the growing concern related to the impact of non-state actors on international peace, and considering the asymmetric and potentially dangerous attributes of cyberspace, such an increase in state responsibility is not unreasonable.

The strength of the proposed definition of cyberspace attack is that it would place a clear responsibility on all states. All states would know what international law requires and non-state actors would know that their actions could be considered armed attacks. Although clear and strict in comparison to the current approach, the proposed legal threshold is not improperly low. It has a reasonable *mens rea* requirement, to wit: the host state must have knowledge of the impending or ongoing use of a cyberspace weapon. Because the proposed definition requires knowing acquiescence, a state can claim the defense of impossibility. For example, the host state may have no knowledge of an ongoing cyberspace attack because the rogue element first hacked into and gained control of the entire host state's communications infrastructure. Still, once the host state became aware of the intended location of the attack, it would then be responsible to at least communicate that information to the victim state and continue to take reasonable measures to stop or impede the attack and cooperate with the victim state.

The unique attributes of cyberspace, such as its speed and lack of physical borders, are key reasons why host states must be responsible for actions within their territory when they do not take reasonable measures to stop the attack and warn the victim state. One cannot overemphasize the potency of the asymmetric capabilities of cyberspace in comparison to any other war-fighting domain in the world's history, a capability that enables almost any person to engage in actions with

[56] S.C. Res. 1373, U.N. SCOR, 4385th mtg., U.N. Doc. S/RES/1373 (Sept. 28, 2001) condemning the terrorist attacks of 9-11 and stating that "those responsible for aiding, supporting or harboring the perpetrators, organizers and sponsors of such acts will be held accountable."); *see also* G.A. Res. 56/1, U.N. GAOR, 56th Sess., U.N. Doc. A/RES/56/1 (Sept. 12, 2001).

lethal and costly effects. Therefore, another difference between the proposed definition and current requirements under international law is that the proposed definition of a cyberspace attack does not include a requirement that the attack involve the armed forces of the aggressor, as the commentary to Common Article 2 requires and the U.N. definition of aggression implies. However, the U.N. definition of aggression clearly includes mercenaries and irregulars. Once more, considering the asymmetric nature of cyberspace, requiring a cyberspace attack to involve the armed forces or mercenaries of the aggressor would create a legal hole big enough for hundreds of thugs and brigands to "attack" the victim state. In consideration of the incredible amount of physical or information damage that non-state actors can cause in cyberspace, knowing acquiescence to such attacks is the correct standard for imposing state responsibility under international law.

But, is it fair to impose such strict accountability on the use of cyberspace, when some cyberspace attributes, such as ease of access and use, are similar to those of global commons? For example, some may argue that the proposed definition is contrary to Article 8 of the Hague Regulation (V).[57] Article 8 provides that "[a] neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals." It is accepted that many cyberspace communications occur over "telephone cables" and similar telecommunications infrastructure. Thus, the language of Article 8 is applicable to cyberspace operations. Article 8 clearly does not place a duty on a neutral power to forbid or restrict belligerents from using their communications infrastructure. In fact, Article 9 of the Hague Regulation (V) states that any restrictive measures implemented by a neutral power must be equally applied to "both belligerents." Article 8's language, therefore, appears to contradict the proposed definition.

Alternatively, one could argue that the proposed definition of cyberspace attack does not conflict with Article 8, because the proposed definition creates a transitional status for a state. Once a state becomes aware of a cyberspace attack originating from its territory and targeting another state, it is no longer a "neutral power" and now must act to stop the attack or become a de facto "belligerent." The idea of a state transitioning between being a neutral power and a belligerent may be too tenuous for realistic application in international law. In the alternative, states could choose, when adopting the proposed definition

[57] Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, *available at* http://www.icrc.org/ihl.nsf/FULL/200?OpenDocument [hereinafter referred to as Hague Regulation (V)].

of cyberspace attack, to explicitly state that Articles 8 and 9 of the Hague Regulation (V) no longer apply to cyberspace.

Going back to the Estonia and Georgia events, most media attributed the use of cyberspace weapons to Russian internet addresses. Despite early and widespread media attribution to Russia, the attacks continued, strongly implying that Russia was directly responsible for the attacks.[58] Apparently, Russian law enforcement and security services made no effort to stop the cyberspace attacks.[59] Russia was certainly on notice that the world community believed the cyberspace attacks were originating from within its borders. While circumstantial evidence clearly indicated that Russia knowingly acquiesced to these attacks, there was no direct evidence. Reviewing the circumstantial evidence under the proposed definition indicates that Russia violated international law and the victim states had the right of self-defense. However, relying on circumstantial evidence is not something the international community and international law are generally comfortable doing.

This lack of direct evidence is indicative of the attribution problem currently hindering all investigations of actions in cyberspace. Investigators of domestic cyberspace crimes meticulously use forensic tools to identify which specific internet protocol (IP) address is responsible for a cyberspace crime and then interview the suspect to determine their level of knowledge or intent. Unfortunately, overseas investigations can only be accomplished if there is cooperation between the involved states. When a foreign state does not provide equal access to forensic evidence and suspects, the attribution barrier obstructs the inquiry and protects the "attacker." Such actions do not promote peace or resolve conflict.

The effects-based model would likely conclude that the Estonia and Georgia attacks were not severe enough to be considered armed attacks or even an unlawful use of force. There were no burning buildings or smashed tanks or casualties usually associated with a traditional, kinetic armed attack. The cyberspace events did not place either country's stability in jeopardy. Reviewing the international reaction after the fact, there were no declarations by the international

---

[58] Arthur Bright, *Estonia accuses Russia of 'cyberattack,'* CHRISTIAN SCI. MONITOR, May 17, 2007, *available at* http://www.csmonitor.com/2007/0517/p99s01-duts.html; John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 12, 2008, *available at* http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&em; *see also* Wikipedia: The Free Encyclopedia, 2007 Cyberattacks on Estonia, http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia (last visited Sept. 3, 2009); Wikipedia: The Free Encyclopedia, Cyberattacks During the 2008 South Ossetia War, http://en.wikipedia.org/wiki/Cyberattacks_during_the_2008_South_Ossetia_war (last visited Sept. 3, 2009).

[59] *Supra* note 58; *see also* NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, CYBER ATTACKS AGAINST GEORGIA, *supra* note 2, at 28-33; Kenneth Geers, *supra* note 49, at 9.

community that these attacks were armed attacks in violation of Article 2(4) of the U.N. Charter or that they created de facto hostilities under Common Article 2 of the Geneva Conventions. Estonia chose not to consider them armed attacks, while the Georgia situation simultaneously devolved into a kinetic conflict. What option did Estonia really have? If Estonia felt it had sufficient attribution, Estonia could have considered the acts armed attacks, creating a de facto state of hostilities and requested the assistance of the North Atlantic Treaty Organization (NATO) under the NATO Treaty's collective self-defense provision.[60] Estonia could have waited for NATO to risk war with Russia. Estonia could also have responded in self-defense with conventional, kinetic forces, since they did not have any "cyberspace forces." The potential result could have been a strong conventional response from Russia, including occupation of Estonia. Again, the "bully dilemma" reared its head. This prompts the question, is it fair to rely on a 60 year-old conventional model that gives such weight to state practice when the kinetic forces and available cyberspace capabilities are so disproportionate?

Indeed, continued reliance on such a model could lead "minor" states to develop cyberspace forces in an effort to achieve an asymmetric advantage over states with much larger kinetic capabilities, leading to a cyberspace arms race and possibly more conflicts. As the Estonia and Georgia events demonstrate, when a state knowingly chooses to not assist a victim state or hold responsible those who use cyberspace weapons against other states, international law should view that state as a transgressor.

That is what the proposed definition of cyberspace attack intends to do. The proposed definition will have a positive impact on international law and conflict management, because it will clearly place

---

[60] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243. Article 5 states:

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

responsibility on all states to not engage in cyberspace attacks and to police and secure their cyberspace "borders."[61] Essentially, everyone will know a cyberspace attack when they see it, and everyone will know that any state that conducts or permits such an attack could suffer self-defense actions and international sanctions. The end result would hopefully be a dramatic decrease in cyberspace events of foreign origin, which would also reduce the likelihood of a cyberspace "arms race" and cause the de-escalation of low intensity conflicts in cyberspace.

D. Flies in the Ointment: Attribution and Espionage

As referenced above, an effects-based approach magnifies the attribution problem, because it requires attribution of intentional direct participation or support by the state actor, versus knowing acquiescence. The difficulty of attribution in cyberspace prevents the evolution of realistic customary norms.[62] No state actor can realistically consider the full spectrum of actions, because they do not know who acted against them or why. In addition, the difficulty in comprehending the full severity of the "attack," because of the delayed effects of cyberspace weapons, compounds the difficulty in determining an appropriate response.

Unlike the effects-based approach, the proposed definition does not require determining who controlled or supported the activity, the aggressor's intent, or the full magnitude of the attack. Using the

[61] The concept of boundaries and sovereignty in cyberspace is also a topic of discussion amongst academics and practitioners. Although there is no clear definition and enforcement of boundaries in cyberspace, all states should recognize that electronic communications of all types originate in one state and can terminate (and have effects) in another state. Therefore, a state can monitor communications occurring inside its geographic borders. For example, the NSA under the Terrorist Surveillance Program was able to monitor communications where one party was located "outside" the United States. White House Press Briefing, Att'y Gen. Alberto Gonzales & Gen. Michael V. Hayden, Principal Deputy Dir. of Nat'l Intel. (Dec. 19, 2005), *available at* http://www.globalsecurity.org/intell/library/news/2005/intell-051219-dni01.htm. The concept of cyberspace borders has even been expanded to include discussions of a cyberspace Monroe Doctrine with regard to cyberspace infrastructure associated to the United States. *See Reviewing the Federal Cybersecurity Mission: Hearing Before the H. Comm. on Homeland Sec., Sub-Comm. on Emerging Threats, Cybersecurity, & Sci. & Tech.*, 110th Cong. (2009) (statement of Mary Ann Davidson, Oracle Security Officer), *available at* http://homeland.house.gov/SiteDocuments/20090310143850-78976.pdf.

[62] Relying on a heuristic analysis of past actions is somewhat similar to how scientists conduct scientific experiments and then analyze the results. In order for scientific experiments and their results to be reliable, external factors must be eliminated or controlled, and all other factors must be accurately known. The lack of attribution makes it impossible to accurately complete a heuristic analysis, since three of the most important factors, identity, intent, and full severity of attack, will rarely be known without it.

definitional approach, only two questions need to be resolved. First, was a cyberspace weapon used against the property or persons of a state? Second, did a foreign state knowingly allow an entity under its legal control to use the cyberspace weapon against the victim?

Even with the proposed definitions and a two element test, one of the oldest arts, espionage, can still take advantage of the attribution difficulties in cyberspace. Espionage has long been recognized as essential to the success of states and their militaries.[63] While a criminal offense in virtually every nation state, espionage is not a violation of the law of war and was first recognized in the Lieber Code in 1863.[64] It was subsequently codified in the 1907 Hague Regulations and in Protocol I.[65] Acts deemed to be espionage will not trigger a state's right to self-defense, because espionage does not violate international law. Based on the definitions from the various documents considered part of customary international law, the consistent requirement for espionage is that a member of the armed forces gathers or attempts to gather information under false pretenses or while not wearing their uniform.

Such a definition does not perfectly transfer over to espionage in cyberspace. Whether the person at the other computer terminal is wearing his uniform is irrelevant to attributing his identity and intent in cyberspace. Still, a cyberspace spy will intrinsically gain access to the information or data under false pretenses. The average cyberspace intruder does not disclose his identity nor does he come to the main web page and ask the webmaster for permission. Instead, he exploits vulnerabilities in software coding that allow him to gain unauthorized access, which is essentially under false pretenses as discussed in Article

---

[63] Sun Tzu stated: "So, as for enlightened lords or distinguished commanders, the reason they can overcome the adversary when action is taken and achieve unparalleled success is prescience. Prescience cannot be gained from ghost or gods . . . . It must be gained from what is learned by men." SUN TZU, SUN TZU: THE NEW TRANSLATION 112 (J. H. Huang trans. 1993).

[64] FRANCIS LIEBER, INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD, ART. 88 (Apr. 24, 1863), *available at* http://www.icrc.org/ihl.nsf/FULL/110?OpenDocument [hereinafter LIEBER CODE]. Article 88 defines a spy as: "a person who secretly, in disguise or under false pretense, seeks information with the intention of communicating it to the enemy."

[65] Article 29 of Hague Regulation (IV), *supra* note 33, defines a spy thus:

> [A]cting clandestinely or on false pretences, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party. Thus, soldiers not wearing a disguise who have penetrated into the zone of operations of the hostile army, for the purpose of obtaining information, are not considered spies.

Article 46 of Protocol I, *supra* note 19, provides that a member of the armed forces shall not be considered a spy "unless he does so through an act of false pretences or deliberately in a clandestine manner."

29 of Hague Regulation IV. Even when an intruder sends an e-mail directly to an authorized user, asking the user to provide his password information, the e-mail is still sent under false pretenses.[66]

It is certainly possible for cyberspace spies to gain access to information and copy or degrade the data without the use of a cyberspace weapon. However, the tension between lawful espionage and armed attack in cyberspace occurs when a spy uses a cyberspace weapon to access or steal information. If a traditional spy uses a weapon, such as a pistol, the act is viewed as a criminal act, versus an armed attack. Should the same be true of a cyberspace spy who hacks into a system by using a cyberspace weapon? Applying the proposed definition of cyberspace attack, the use of a cyberspace weapon while committing espionage in or through cyberspace could be interpreted as a cyberspace attack and result in self-defense actions.

The only way to resolve the tension between cyberspace espionage and cyberspace attack is to determine whether the cyberspace intruder intends solely to copy and then steal the data or information. Again, this dilemma adds a layer of complexity to the attribution issue by now requiring a determination of the actor's full intent, creating an untenable situation for the victim state. Given that actions happen so fast in cyberspace, a spy or attacker could move "in and out" before a victim state could do any more than determine the foreign internet protocol (IP) address of the intruder. A full damage assessment, identifying what happened to the victim computer system could take hours to weeks. While some cyberspace attacks may be obvious, many will not be, as the beauty of cyberspace warfare is the ability to create second and third order effects, which are difficult to identify in advance.

The attribution issue reaches a pinnacle of complexity when trying to resolve events between espionage and cyberspace attacks. Therefore, today, a victim state is left with three choices: (1) continue to operate in the current international system of subjective analysis and inconsistent past responses while ineffectively trying to gather very detailed attribution information; (2) develop a robust cyberspace force capable of conducting cyberspace attacks, cyberspace espionage, and able to "hack back" to develop reasonably detailed attribution information; (3) or issue an ultimatum to the international community, hoping that others will agree, which informs all other states that any activity in that state's territory that is determined to satisfy the proposed definition of a cyberspace attack will justify self-defense actions by the victim state.

---

[66] Phishing or spear phishing emails target known users on a network and always provide a false reason for the recipient to provide key information or click on a hyperlink that will then redirect the user to another web page where malicious code, read weapon, will be surreptitiously installed on the user's computer.

The difficulty with resolving the espionage issue is that under the first option a state remains vulnerable to many forms of cyberspace attack while attempting to resolve whether the event is an act of espionage or cyberspace attack and waiting for the international community to subjectively analyze the evidence. In addition, the evidence to satisfy the international community would likely include the elusive proof of actual intent to harm the victim state. Adversarial states could choose to take advantage of this slow analysis and decision loop, achieving paralysis by analysis, and methodically weaken a state with what appears to be cyberspace espionage but is in fact a number of cyberspace attacks aimed at creating third order effects. Lastly, it appears that states are not willingly sharing the details of their cyberspace activities with others, which still leaves a void of necessary information to conduct the required heuristic analysis to develop the law under the current framework.

The second option will help the state protect itself from adversarial activities in cyberspace and possibly lead to attributable information. In spite of this benefit, the potential of a cyberspace arms race increases. This development could lead to an increase in low scale cyberspace conflicts and ultimately result in an adversary conducting a second or third order cyberspace attack inflicting massive casualties or property damage.[67] The continued development of cyberspace capabilities appears to be the current direction of the leading states, such as China, Russia, and the United States. States certainly cannot be faulted for taking such an approach, as the current international legal scheme offers them very little protection yet many opportunities to exploit the cyberspace of other states. Therefore, the race for dominance in cyberspace has begun and may soon grow out of control.

The second option also has some parallels to the approach that states took when nuclear tensions were high during the Cold War. The superpowers recognized that conventional methodologies could not be applied to the use of intercontinental ballistic missiles (ICBM). States recognized that Article 51's right of self-defense limited them to proportional actions. However, due to the overwhelming effect and fairly rapid speed of any nuclear attack, states were doctrinally prepared to respond in full at the first indication of even a limited attack, since they recognized that they could not afford to wait and see how many warheads or which locations the adversary's warheads hit and how much damage they caused. Superpowers projected that they were capable, prepared, and willing to respond to even a limited, targeted nuclear first-strike with a full-scale response.

[67] Cyberspace attacks against critical infrastructure, aircraft and air traffic control software, navigation systems (GPS), and pharmaceutical companies to alter the code for medicines and vaccines are just some examples of cyberspace attacks that may not have recognizable first order effects, but catastrophic subsequent effects.

Historically, one can see how nation states adopted their practice in light of the dramatic increase in speed and lethality of nuclear attacks using ICBM's compared to the previous conventional method of warfare, circa World War II. While many decried the age of mutually assured destruction (MAD) and called it "mad," one cannot dispute that during that time period, even though there was a nuclear arms race, no nuclear weapons were used. Mad or not, MAD was an effective method of deterrence. There are a number of parallels between the use of ICBMs and cyberspace operations: cyberspace attacks have the potential for incredible lethality; much greater speed than previous weapons; and the actual severity of the threat, the intent, and the identity of the actor are usually too difficult to determine in sufficient time to respond appropriately before the damage is done.

However, there is one crucial difference between today's option two situation (developing a robust cyberspace force and "hacking back") and the deterrence model of MAD during the Cold War. Currently, it does not appear that a substantial number of states are willing to make a declaration of mutually assured destruction through cyberspace and simultaneously abstain from conducting cyberspace operations. Without such declarations and cessation of the use of cyberspace weapons, the parallels with the Cold War nuclear deterrence model end. Pragmatically, states do not feel the impetus to consider such an approach. There has been no mass disaster or 9-11 type "wake-up call" in cyberspace, and, as noted above, a number of states likely believe they can "win" in cyberspace. Therefore, applying the nuclear deterrence model to cyberspace operations is not practical. Unfortunately, history has shown that society rarely chooses to collectively legislate against harm until after it suffers the consequences.

Still, there is one historical example where society chose to proactively legislate and limit the weaponization of a domain, much like option three. The Outer Space Treaty prohibits the placing of nuclear weapons and weapons of mass destruction in space.[68] The third option can perhaps draw strength from the efforts to limit the militarization of space, recognizing cyberspace as a sort of international commons similar to outer space. Each state, relying on the proposed definitions, would still retain its sovereignty and control of cyberspace infrastructure located within its borders. The implementation of the proposed definitions would recognize that the use of cyberspace is intended for peace-promoting purposes and the use of weapons in cyberspace, even for espionage purposes, will not be accepted. Providing states the right of self-defense using the lower, clear threshold of the proposed

[68] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 6 I.L.M. 386, *available at* http://www.unoosa.org/oosa/SpaceLaw/outerspt.html.

definitions will hopefully inspire states to abstain from cyberspace espionage and attacks and cooperate to protect the peaceful use of cyberspace.

IV. APPLYING THE DEFINITIONS AND EXERCISING SELF-DEFENSE IN CYBERSPACE

In order to further understand how option three's (issuing an ultimatum that the state could respond in self-defense to cyberspace attacks) use of the proposed definitions will promote peace and reduce the improper use of cyberspace, it is helpful to explore how states could act in response to a cyberspace attack. The doctrine of self-defense relies on two principles: necessity and proportionality. Necessity involves whether effective peaceful means of resolution exist; the nature of the aggression, each party's objectives, and the likelihood of effective intervention by the international community.[69] Proportionality requires limiting the magnitude, scope, and duration of the force used in response to that which is reasonably necessary to counter the threat or attack.[70] The timing of a self-defense action is closely related to the factor of necessity and is a debated issue. A delayed response weakens a state's claim of necessity to defend itself. While an early response in anticipation of attack also draws questions as to the certainty of need for the self-defense action.

Looking at necessity and the timing of self-defense actions in cyberspace, the unique qualities of cyberspace again highlight the importance of moving toward a deterrence model. Once a state suffers what it believes to be an armed attack in or through cyberspace, it can arguably satisfy the above requirements of necessity to defend itself. Unfortunately, in cyberspace, there will likely not be sufficient time to consider peaceful resolution of the matter, fully understand the nature of the attack or the intended results, or to mobilize international peacekeeping forces. Thus, the more difficult question related to necessity is how appropriate is anticipatory self-defense in cyberspace?

Anticipatory self-defense "justifies use of force in anticipation of an 'imminent' armed attack."[71] Basically, a state need not wait to receive the aggressor's attack and can instead act in self-defense to "repel" the attack.[72] The doctrine "finds it roots in the 1837 *Caroline* case and subsequent correspondence between then-U.S. Secretary of

---

[69] INT'L & OPERATIONAL LAW DEP'T, THE JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., U.S. ARMY, JA 422, OPERATIONAL LAW HANDBOOK 4 (2007) [hereinafter U.S. ARMY OPERATIONAL LAW HANDBOOK]; *see also* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE (4th ed. 2005).
[70] U.S. ARMY OPERATIONAL LAW HANDBOOK, *supra* note 69.
[71] *Id*. at 6.
[72] *Id*.

State Daniel Webster and his British Foreign Office counterpart Lord Ashburton."[73] Secretary Webster informed Lord Ashburton that a state can act in self-defense when the circumstances are "instantaneous, overwhelming, and leaving no choice of means and no moment for deliberation."[74] The attributes of cyberspace, especially speed and lethality, seem quite similar to Secretary Webster's factors. Essentially, if a state is fortunate enough to develop information about a developing or planned cyberspace attack against it, the attributes of cyberspace may compel a state to act in its best interest and exercise anticipatory self-defense.

The follow-on question involves what a state can do in self-defense, i.e. how is the principle of proportional response applied in and through cyberspace? In cyberspace, there may be a number of ways to technically counter an attack. A state could disconnect itself from cyberspace. However, such a response seems disproportionately burdensome on the victim state and could cause other forms of harm internally. The victim state could quickly counter with anti-virus measures, although such efforts are always a game of "catch-up." The victim state could respond by disconnecting all cyberspace connections with the aggressor state. However, this will only work as long as the aggressor state chooses not to attack through another state. Moreover, such actions require attribution.

Because a state needs to know against which state to exercise self-defense, developing reliable attribution represents another difficulty with applying age-old laws and methods to cyberspace. Given that a cyberspace attack comes from another country and could involve communications "hopping" through several other countries, it is nearly impossible for a state to develop attribution without first violating the cyberspace infrastructure and jurisdiction of other states. Currently, to avoid violating another state's cyberspace, states send requests for assistance to cooperating states. The victim state requests help in developing information about the IP address in question and also requests monitoring of that IP address, allowing the state to "hop back" to the next IP address, and then request more help. This "hopping back" process can be painful and long, leaving the victim state vulnerable. However, the traditional police doctrine of hot pursuit is expanding in international law. Under customary international law, ships and planes can follow offending vessels in hot pursuit up to another state's territorial sea or airspace.[75] However, the European Union has adopted the Schengen Agreement that permits law enforcement officials to cross state borders when pursuing a criminal suspected of certain serious

[73] *Id*.
[74] *Id*.
[75] *Id*. at 541.

offenses[76] The agreement provides that the pursuing officers will cease their pursuit upon request of the other state, however, the pursuing officers can request that the other state arrest the suspect.[77]

Extending the principles of the Schengen Agreement to the domain of cyberspace seems logical, because attacks in cyberspace are analogous to serious criminal offenses. Permitting hot pursuit is consistent with the proposed definition's efforts to deter states from knowingly acquiescing to cyberspace attacks. Witting host states will find it much harder to hide in the shadow of attribution. Providing victim states with a legal "hot pursuit" capability, including proper coordination mechanisms, will be invaluable to promoting cooperation, reducing crime, and deterring attacks in and through cyberspace.

With the ability to more quickly attribute attacks, a state would then have other options to consider under the principle of proportionate response. The victim state could consider firing back in self-defense with a cyberspace weapon at the actual computer(s) used to attack it. This can be reasonably effective if a limited number of computers are involved.[78] However, a victim state will likely remain concerned, due to its limited ability to determine whether more attacks or attacks of increasing severity will follow the initial round of attacks. This challenge may lead a state to consider more serious measures, such as responding with a self-defense attack that involves disrupting a substantial portion of the witting host state's cyberspace. However, the collateral damage from such a self-defense action could be substantial. The questions of necessity and anticipatory self-defense also affect the proportionality decision. Moreover, nothing prohibits states from defending against a cyberspace attack by using kinetic weapons, such as striking a key communication node with a cruise missile or damaging a state's communication satellite(s). The hypotheticals and the potential for conflict abound. Thus, the unique nature of cyberspace and the inability to clearly apply current international laws, norms, and practices make resolution of conflict extremely difficult, and should inspire states to seek a framework of cooperation and deterrence, such as the one I advocate in this article.

---

[76] Convention Implementing the Schnegen Agreement art. 41, June 14, 1985, 1999 O.J. (L 176) 13, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2000/l_239/l_23920000922en00010473.pdf.

[77] *Id*.

[78] Unfortunately, many cyberspace "attacks" involve or will likely involve "botnets" of thousands or more computers under the control of one or more "herders" and capable of "firing" millions of messages or viruses to disrupt or co-opt other systems.

V. LOOKING FORWARD AND CONCLUDING THOUGHTS

The definitions proposed in this article provide a framework for consistency and an opportunity to level the playing field of international law. Today, states can either choose to continue with the status quo, or, recognizing the benefits of the peaceful use of cyberspace, embrace the need for clear definitions of cyberspace weapon and cyberspace attack. Embracing the definitions I propose would, at most, have a moderate impact on how international affairs are conducted today. The Schengen Agreement and the E.U. Convention on Cybercrime serve as models to build a framework of cooperation to promote peace and reduce crime. States would need to establish cyberspace communications centers, whereby each state would agree to pass information to another state as soon as it became aware of a cyberspace attack against a victim state, but is currently unable to halt the attack from affecting the victim state.[79] The centers would also coordinate the hot pursuit issues related to developing attribution.

Those states that choose not to adopt the proposed legal definitions and methods of cooperation would do so knowing that their actions or inaction could be viewed as a cyberspace attack. Each state would still continue to exercise its right of self-defense. Meanwhile, the international community could apply the new legal standard when considering whether to apply sanctions. The end result is that the proposed definition of a cyberspace attack with cooperative application under international law could make a powerful form of asymmetric warfare untenable before it develops into an arms race that leads to increased conflicts and harms people and property.

When our predecessors developed the law of conflict management it is doubtful anyone could foresee the day when a state could attack another state simply by manipulating electronic data. Even the futuristic Buck Rogers and lasers still had visible, kinetic-like effects. Today, one must recognize that the lack of specific definitions for "weapon" and "armed attack" create an untenable vacuum in the evolving domain of cyberspace. So far, only the criminal law has provided thorough definitions in an attempt to keep pace with the development of nefarious tools in cyberspace. The criminal law methodology provides a sufficient degree of flexibility to adapt such definitions to the various uses of prohibited cyberspace tools. The field of international law requires similar flexibility. This article attempted to craft a definition of a cyberspace weapon from the criminal law's efforts to specifically define the acts caused by cyberspace criminals. The

[79] A state could of course provide the information to the potential victim state, even if they were able to halt the attack before it caused harm. This extra level of cooperation would assist all states in developing their capabilities to detect potential cyberspace attacks.

criminal law methodology facilitated the development of a definition of a cyberspace attack. By applying the current international law framework to the proposed definition of an armed attack in cyberspace, this article highlighted how such a definition could lead to parity in cyberspace and thereby promote peace through deterrence.

MILITARY CRIMINAL INVESTIGATIONS AND THE STORED COMMUNICATIONS ACT

LIEUTENANT COLONEL THOMAS DUKES, JR
LIEUTENANT COLONEL ALBERT C. REES, JR.

Lieutenant Colonel Thomas Dukes, Jr. (B.A., University of Maine (1990), J.D., University of Virginia (1994)) and Lieutenant Colonel Albert C. Rees, Jr. (B.A., University of Southwestern Louisiana (1986), J.D., Loyola University School of Law (1992), LL.M., Georgetown University (2002)) are trial attorneys with the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. They also serve in the U.S. Air Force Reserve, where Lt Col Dukes is attached to the Air Force Judiciary as a military judge, and Lt Col Rees is attached to the Air Force Operations and International Law Directorate, Headquarters, U.S. Air Force. Lt Col Dukes is a member of the Virginia Bar, and Lt Col Rees is a member of the Louisiana Bar.

I. INTRODUCTION

In this age of text messaging, Facebook, Flickr, LinkedIn, and Gmail, almost any crime is likely to leave a trail of evidence in the form of electronic communications and their associated records. Most people, criminals included, are putting increasingly large amounts of information in the hands of third parties such as cell phone companies, Internet service providers (ISPs), social networking sites, and other public service providers. Military members are no exception to this societal trend, and the crimes they commit, whether on military installations or in deployed locations, where military criminal investigative organizations (MCIOs)[1] have primary or exclusive jurisdiction to investigate, also likely involve electronic evidence. Military criminal investigators should, therefore, routinely seek electronic evidence as they conduct their investigations; yet, the legal framework for obtaining information from public service providers does not provide effective mechanisms for MCIOs to do their jobs properly.

This article specifically focuses on the practical applications and limitations of the Stored Communications Act [2] (SCA) as it applies to military criminal investigations.[3] We will not analyze other electronic evidence gathering issues, such as real-time interception of communications or Fourth Amendment law as it relates to the search

[1] The primary military criminal investigative organizations are the Air Force Office of Special Investigations (AFOSI), the Naval Criminal Investigative Service (NCIS), the Army Criminal Investigation Command (CID), and the Defense Criminal Investigative Service (DCIS).

[2] 18 U.S.C. §§ 2701-2712 (2006). Practitioners in this area of the law routinely refer to United States Code, Title 18, Chapter 121, which is formally titled "Stored Wire And Electronic Communications And Transactional Records Access" as the Stored Communications Act or the SCA. For example, this usage is found in *Warshak v. United States*, 531 F.3d 521, 522 (6th Cir. 2008); and *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 895 (9th Cir. 2008).

[3] Many prosecutors and investigators do not differentiate between the SCA and the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C. (2006)) [hereinafter ECPA]. The SCA is contained in Title II of ECPA, so strictly speaking the SCA is a subset of ECPA, and, as its title suggests, sets forth the relationships between service providers and government entities for stored communications (i.e., information at rest). ECPA also significantly altered the statutes governing wire taps (i.e., the interception of the content of communications) and pen registers and trap and trace devices (i.e., dialing, routing and addressing information for communications). Wire taps are governed by 18 U.S.C. §§ 2510-2522 (2006), first enacted at Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and generally referred to as "Title III." Pen registers and trap and trace devices are governed by 18 U.S.C. §§ 3121-3127 (2006). For an overview of ECPA, see the U.S. Department of Justice Information Sharing webpage, Federal Statutes Relevant in the Information Sharing Environment, http://www.it.ojp.gov/default.aspx?area=privacy&page=1285 (last visited July 23, 2009).

and seizure of computers and electronic evidence.[4] Our goal is to introduce readers to the SCA, describe how the SCA is a valuable tool for law enforcement, and set forth its limitations for MCIOs. To that end, we will focus on obtaining evidence from "public service providers,"[5] leaving aside the category of "non-public service providers."[6]

In brief, the SCA prohibits public service providers from voluntarily disclosing to government entities information about their customers or their customers' communications, but provides law enforcement organizations with specific procedures to compel disclosure. However, the SCA does not contemplate that the military would have a need to compel disclosure and, particularly in cases investigated under the Uniform Code of Military Justice (UCMJ), does not provide the tools that MCIOs need to routinely obtain valuable information. A comprehensive solution giving military authorities the ability to compel public service providers to disclose the full gamut of information they have relating to their customers will require Congressional action to amend the SCA, as discussed below. As an interim step, however, the Department of Defense (DOD) Inspector General (IG) should expand its administrative subpoena program as much as possible to facilitate MCIOs' general crimes investigations. Further, commanders, the military legal community, and MCIOs should strive to improve cooperative arrangements with the federal and local law enforcement authorities that currently are able to compel disclosure pursuant to the SCA.

---

[4] The Computer Crime and Intellectual Property Section [hereinafter CCIPS] of the U.S. Department of Justice publishes a comprehensive electronic evidence manual, which provides an in-depth discussion of ECPA (including obtaining stored communications and interception of communications) and Fourth Amendment principles governing searches and seizures of computers and electronic evidence. U.S. DEP'T OF JUSTICE, CCIPS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2009), *available at* http://www.cybercrime.gov/s&smanual2009.htm.

[5] This article uses the phrase "public service provider" to describe any entity that provides electronic communications services (as defined at 18 U.S.C. § 2510(15)) or remote computing services (as defined at 18 U.S.C. § 2711(2)) to anyone who "complies with the requisite procedures and pays any requisite fees." U.S. DEP'T OF JUSTICE, CCIPS, *supra* note 4, at Ch. III, § B. These services are available to the general public and may or may not require payment of a fee. Thus, public service providers include companies such as Verizon Wireless, Inc. (provider of cell phone service), Yahoo!, Inc. (provider of free webmail services), Earthlink, Inc. (Internet service provider), and Amazon Web Services (provider of online electronic storage and processing services).

[6] "Non-public service providers" are "providers whose services are open only to those with a special relationship with the provider." U.S. DEP'T OF JUSTICE, CCIPS, *supra* note 4, at Ch. III, § B. For example, non-public service providers include the Department of Defense and other U.S. government departments and agencies (providing services to military and civilian employees and contractors), universities and colleges (providing services to students, faculty and staff), and private companies (providing services to employees).

II. THE STORED COMMUNICATIONS ACT

The SCA provides the rules of engagement governing when and how law enforcement agencies may obtain customer communications or records maintained by providers of electronic communication services and remote computing services.[7] The basic premise of the SCA is that customers of ISPs, cell phone companies, and web-based e-mail providers should receive statutory privacy protections for the account, transactional, and content data that these third-party providers maintain on behalf of the customer.[8]

The easiest way to understand the SCA and how it applies to a typical criminal investigation is to look at the three basic categories of information governed by the SCA and the corresponding types of legal process that law enforcement agencies must use to compel production of each of those categories of information.[9] This overview focuses on criminal investigations seeking evidence from public providers where the law enforcement agency does not wish to alert the subject to their investigation.

The first basic category of information protected by the SCA consists of basic information about the account and the account holder.[10] The information in this category includes the name and address of the account holder; local and long distance telephone connection records; records of session times and duration for Internet service; the start date and length of service; the types of services utilized; any telephone or instrument number or other subscriber numbers or identities associated with the account, including network addresses temporarily assigned to the account; and the means and source of payment for the account,

---

[7] 18 U.S.C. § 2510(15) defines the term "electronic communication service" [hereinafter ECS] as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2711(2) defines the term "remote computing service" [hereinafter RCS] to mean "the provision to the public of computer storage or processing services by means of an electronic communications system." A single provider can be both an ECS and an RCS, depending on the type of services it provides. For the purposes of this article, we will focus on the procedures for obtaining information from "public service providers," without regard to whether they are an ECS or a RCS.

[8] *See* S. REP. NO. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

[9] This article focuses on the legal procedures for compelling disclosure of information covered by the SCA. It does not address the SCA's provisions for voluntary disclosure of customer communications or records to law enforcement agencies, which are contained in 18 U.S.C. § 2702. 18 U.S.C. § 2702(a) contains a general prohibition on voluntary disclosure of covered information by a public service provider to a law enforcement agency. 18 U.S.C. § 2702(b) and (c) contain a variety of exceptions to the general prohibition in 18 U.S.C. § 2702(a), including: with the consent of the customer or subscriber, as necessary to protect the rights or property of the public service provider, or in case of an emergency involving immediate danger of death or serious physical injury to any person.

[10] 18 U.S.C. § 2703(c)(2) (2006).

including any credit card or bank account numbers.[11] A law enforcement agency may compel the production of this type of information with a grand jury, administrative, or trial subpoena.[12]

The second basic category of information protected by the SCA consists of certain transactional records associated with the use of the account.[13] Some examples of the types of information included in this category are account logs that document cell-site data for cell phone calls and e-mail addresses for individuals who corresponded with the account holder. A law enforcement agency may compel the production of this information through the use of a special type of court order authorized by Section 2703(d) of the SCA.[14]

The third basic category of information protected by the SCA consists of the contents of wire and electronic communications and other stored files.[15] The SCA divides this general category into three technical sub-categories, namely: (1) retrieved communications and the content of other stored files; (2) un-retrieved communications that have been in electronic storage for one hundred eighty one days or more; and (3) un-retrieved communications that have been in electronic storage for one hundred eighty days or less.[16] Law enforcement agencies will typically obtain evidence covered by the first two sub-categories by using a special type of search warrant authorized by Section 2703(a) of the SCA.[17] It should be noted that the evidence covered by the first two

---

[11] *Id.*

[12] *Id.* The basic subscriber information listed in 18 U.S.C. § 2703(c)(2) may also be obtained by using an 18 U.S.C. § 2703(d) order or an 18 U.S.C. § 2703(a) search warrant.

[13] 18 U.S.C. § 2703(c)(1) (2006).

[14] A court order authorized by 18 U.S.C. § 2703(d) may be issued by a U.S. District Court or state court when the government "offers specific and articulable facts showing that there are reasonable grounds to believe that [the information sought is] relevant and material to an ongoing criminal investigation." *Id.* The information that may be obtained with an 18 U.S.C. § 2703(d) order may also be obtained by using an 18 U.S.C. § 2703(a) search warrant.

[15] *See* 18 U.S.C. § 2703(a) and (b). 18 U.S.C. § 2703(a) deals with the contents of wire or electronic communications in electronic storage. 18 U.S.C. § 2703(b) deals with the contents of wire or electronic communications in a remote computing service.

[16] *Id.*

[17] A search warrant issued pursuant to 18 U.S.C. § 2703(a) must generally comply with the search warrant procedures contained in the Federal Rules of Criminal Procedure, particularly Rule 41. Pursuant to Rule 41, a federal law enforcement officer or an attorney for the government requests a federal magistrate judge to issue a warrant. An application for a warrant must include an affidavit or sworn testimony describing the location, items sought, and how they are connected to an investigation. If the judge determines that probable cause exists to search for and seize the items sought, then the magistrate judge must issue the warrant. Once issued, the law enforcement officer must execute the warrant and return it to the judge within 10 days. FED. R. CRIM. P. 41. However, there are several significant differences between a search warrant issued under § 2703(a) of the SCA and a traditional search warrant issued pursuant to Rule 41, including that SCA search warrants have nation-wide effect and are served like

sub-categories could also be obtained in some circumstances by using a subpoena or a 2703(d) order and giving prior notice to the account owner.[18] Law enforcement agencies can only obtain the evidence covered by the third sub-category by using a search warrant pursuant to Section 2703(a) of the SCA.[19]

There is no requirement in the SCA, or elsewhere in federal law, for public service providers located in the United States to retain information covered by the SCA for any particular amount of time.[20] As a result, the retention time for information covered by the SCA varies from provider to provider. The SCA does, however, give law enforcement agencies the ability to make public service providers preserve all of the evidence discussed in the preceding paragraphs, by issuing a preservation letter pursuant to Section 2703(f) of the SCA.[21] A provider receiving a 2703(f) preservation letter "shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."[22] Public service providers receiving a preservation request pursuant to 18 U.S.C. § 2703(f) must retain any responsive records for a period of 90 days, which the requesting law enforcement agency can extend for an additional 90 days. Therefore, law enforcement agencies should send a 2703(f) preservation letter each time they identify an account likely to contain relevant information covered by the SCA.

---

subpoenas, with the provider searching their own systems and then turning any responsive information over to the law enforcement agency that served the process.

[18] 18 U.S.C. § 2703(a) and (b) (2006). In *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), the U.S. Court of Appeals for the Ninth Circuit issued a decision that treats all e-mail sought under the SCA as if it were un-retrieved. As a result, law enforcement agencies conducting criminal investigations within the geographic confines of the Ninth Circuit may only obtain e-mails covered by the SCA by using a search warrant. Law enforcement agencies outside the Ninth Circuit still have the option of using a subpoena or a § 2703(d) order with prior notice to obtain information covered by 18 U.S.C. § 2703(b).

[19] 18 U.S.C. § 2703(a) (2006).

[20] In contrast, European Union Member States generally require service providers to retain the types of information covered by the SCA for a period of six months to two years. *See* Council Directive 2006/24, art. 6, 2006 O.J. (L105) 58 (European Parliament and EC).

[21] 18 U.S.C. § 2703(f) (2006).

[22] 18 U.S.C. § 2703(f)(2) (2006).

III. MILITARY CRIMINAL INVESTIGATIVE ORGANIZATION USE OF THE SCA

The investigative tools provided by the SCA are a necessary, and increasingly indispensable, part of any law enforcement agency's arsenal given the proliferation of electronic evidence. It is safe to assume, therefore, that MCIOs will want to obtain evidence governed by the SCA in many, if not most, criminal investigations, including those investigations that involve offenses punishable under the UCMJ. Unfortunately for MCIOs, they cannot readily or directly utilize several of the types of compulsory legal process authorized by the SCA in military criminal investigations.

The easiest way to understand how the SCA applies to military criminal investigations is to revisit each of the three types of compulsory legal process available under the SCA (subpoenas, 18 U.S.C. § 2703(d) orders and 18 U.S.C. § 2703(a) search warrants), and specifically identify whether and how each can be used by MCIOs conducting investigations under the UCMJ. The SCA allows criminal investigators to obtain certain key information by using a subpoena. The SCA specifically authorizes the use of grand jury, administrative and trial subpoenas, whether issued by federal or state authorities.[23] In military criminal investigations, administrative DOD IG subpoenas could be used at the investigative stage to obtain all the information listed in Section 2703(c)(2) of the SCA.[24] In addition, once a convening authority refers a case to trial by court-martial, counsel may issue a trial subpoena to obtain the same info.[25] Essentially, subpoena power under the SCA is freely available to MCIOs, subject only to the limitations imposed by DOD and service regulations.

---

[23] 18 U.S.C. § 2703(c)(2) (2006).

[24] DOD IG's authority to issue administrative subpoenas is derived from the Inspector General Act of 1978, 5 U.S.C. app. 3 § 6(a)(4) (2006), and U.S. DEP'T OF DEFENSE, DIR. 5106.01, INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE, para. 5.6 (13 Apr. 2006) (C1 25 Sept. 2006) [hereinafter DOD DIR. 5106.01]. DOD interprets this authority to extend to subpoenas in support of general criminal investigations. Memorandum, The Inspector General, U.S. Dep't of Defense, to Director, Defense Criminal Investigative Service, *et al.*, subject: Use of DOD IG Subpoenas in Support of Non-Fraud Related Investigations (21 Jan. 2009) [hereinafter DOD IG Memorandum], *available at* www.dodig.mil/Inspections/IPO/Subpoena/SubpoenaIndex.htm. For a description of administrative subpoenas see CHARLES DOYLE, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS NO. RL3332, ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS (Mar. 17, 2006), *available at* http://www.fas.org/sgp/crs/intel/RL33321.pdf.

[25] 18 U.S.C. § 2703(c)(2). The trial counsel's authority to issue subpoenas for the production of civilian witnesses and documents comes from UCMJ art. 46 (2008), and is set forth in MANUAL FOR COURTS-MARTIAL, UNITED STATES, R.C.M. 703(e)(2) (2008). The summary court-martial, president of a court of inquiry, and officer detailed to take a deposition also have such subpoena power. *Id.*

The SCA requires the use of a Section 2703(d) order to obtain certain types of transactional information from providers, and authorizes certain specific state and federal courts to issue the required process.[26] The SCA states that only a "court of competent jurisdiction"[27] may issue a 2703(d) order, and 18 U.S.C. 3127 defines that term to include "any district court of the United States . . . or any United States court of appeals having jurisdiction over the offense being investigated . . . or . . . a court of criminal jurisdiction of a State . . ."[28] This clearly precludes military magistrates or military judges from issuing 2703(d) orders.[29] The SCA requires the use of a search warrant to obtain most content, including unread e-mails and text messages, from service providers.[30] The SCA authorizes federal and state courts to issue search warrants in criminal investigations, subject to specific jurisdictional limitations.[31] In addition, federal search warrants issued pursuant to the SCA must comply with the provisions of Rule 41 of the Federal Rules of Criminal Procedure.[32] As with 2703(d) orders, however, the SCA does not authorize military authorities to issue a search warrant.

Although the SCA does not authorize military authorities to directly issue 2703(d) orders or search warrants in military criminal investigations, MCIOs may still benefit from the SCA's investigative tools when engaged in joint investigations with other federal law enforcement agencies, such as the Federal Bureau of Investigation, the Drug Enforcement Administration, or the Defense Criminal Investigative Service. In joint investigations of offenses such as procurement fraud or controlled substances, MCIOs will frequently be able to obtain information covered by the various provisions of the SCA, because a U.S. District Court and a U.S. Attorney's Office will have jurisdiction over the offenses under investigation.[33] Likewise, in joint investigations involving state or local law enforcement officials, MCIOs can obtain information covered by the SCA through process issued by state and local law enforcement or judicial authorities.

---

[26] 18 U.S.C. § 2703(b)-(d) (2006).
[27] 18 U.S.C. § 2703(d) (2006).
[28] 18 U.S.C. § 3127(2) (2006).
[29] *See* United States v. Khamsouk, 57 M.J. 282, 289 (2002) (commanders' powers are limited to persons and places under military control); *see also* MCM, *supra* note 25, MIL. R. EVID. 315(c).
[30] 18 U.S.C. § 2703(a) (2006).
[31] *Id*.
[32] FED. R. CRIM. P. 41. See explanation of procedure in *supra* note 17.
[33] *See* U.S. DEP'T OF DEFENSE, DIR. 5525.7, IMPLEMENTATION OF THE MEMORANDUM OF UNDERSTANDING BETWEEN THE DEPARTMENT OF JUSTICE AND THE DEPARTMENT OF DEFENSE RELATING TO THE INVESTIGATION AND PROSECUTION OF CERTAIN CRIMES (22 Jan. 1985), included as Appendix 3 to the MCM, *supra* note 25, for the primary rules of engagement governing situations where both the Department of Defense and the Department of Justice have a concurrent interest in the investigation or prosecution of criminal conduct.

In other common scenarios, however, it may not be possible to obtain electronic evidence governed by the SCA due to the nature of the offense or the lack of jurisdiction by any court authorized to issue compulsory process under the SCA. Examples of such scenarios would include: uniquely military offenses, such as desertion, which may only be prosecuted by court-martial; cases where no federal or state court has jurisdiction over the offense being investigated; and cases that are technically within the jurisdiction of a federal or state court, but which fall below prosecutorial thresholds, such as drug cases involving minimal amounts of controlled substances.

IV. SCENARIO

The following scenario describes a hypothetical routine drug case in which public service providers hold important electronic evidence of interest to a MCIO. This scenario, admittedly contrived, applies SCA tools that we have previously discussed. It illustrates the value of stored communications and related information in a typical criminal investigation familiar to military justice practitioners, and the limits placed on military investigators when attempting to gather evidence from public service providers.

Senior Airman (SrA) Sue is stationed at Bertleson AFB, located near Denver, Colorado. She is 22 years old, single, and lives in the dorm on base. On 22 February, a Sunday night, she was randomly selected for a drug urinalysis (UA). On 25 March, the results came back from the lab, showing that she tested positive for cocaine. The Air Force Office of Special Investigations (AFOSI) opened a case and assigned Special Agent (SA) Mack as the lead investigator. Other than the UA results, SA Mack obtained the following information in his initial investigation: When interviewed, SrA Sue's roommate said that on Saturday night, 21 February, she received a text message from SrA Sue. The message stated that SrA Sue was at their favorite late-night diner, studying for her Weighted Airman Promotion System test. The roommate provided SrA Sue's cellphone number, which SA Mack determined to be a Verizon Wireless[34] account. When searching SrA Sue's dorm room, SA Mack found a crumpled, printed copy of an email dated 23 February, from prettys@yahoo.com to joe223322@gmail.com, no subject, with the body stating, "i got picked for a p test! what am i going to do?" SA Mack did not get any other useful information from witnesses or searches.

As soon as SA Mack determines that service providers may have evidence relating to SrA Sue's case, he faxes preservation request

[34] The companies described in this hypothetical scenario are illustrative of the multitude of public service providers.

letters to Verizon Wireless, Inc.,Yahoo!, Inc., and Google, Inc., pursuant to 18 U.S.C. § 2703(f). He directs Verizon Wireless to preserve information relating to SrA Sue's cellphone number, Yahoo! to preserve information relating to prettys@yahoo.com, and Google to preserve information relating to joe223322@gmail.com. The 2703(f) preservation requests prevent the service providers from deleting information related to these accounts for 90 days, giving SA Mack time to seek the appropriate SCA legal process compelling disclosure.[35]

Under the SCA, an investigator's next step in gathering electronic communications evidence is to issue subpoenas to compel the service providers to disclose basic subscriber information pursuant to 18 U.S.C. § 2703(c)(2).[36] However, SA Mack immediately runs into a dead end. The DOD IG, the only DOD entity with subpoena power at this point in the investigation,[37] will not issue subpoenas for him. DOD IG will only consider requests to issue subpoenas in support of investigations of particular crimes; neither possession nor use of controlled substances is one of the crimes.[38] SA Mack's other military option is to wait for the convening authority to refer charges to a court-martial, and ask the trial counsel to issue trial subpoenas after referral.

Yet information obtainable with subpoenas will often produce valuable leads. These can lead to new non-electronic evidence, such as information about individuals who may be associated with the offense, or timelines that clarify when someone was online or using a cellphone. The information disclosed pursuant to a subpoena also sets the stage for additional searches for electronic evidence. Luckily for SA Mack, local police have set a high priority on finding and stopping cocaine dealers in the community. The police are willing to open a joint investigation with AFOSI and asssist SA Mack in his investigation of SrA Sue's case.

The local police, with assistance from the district attorney's office, issue grand jury subpoenas to Verizon, Yahoo!, and Google. The subpoena to Verizon Wireless confirms SrA Sue's cell phone number and the connection records of the calls/texts she sent and received on the weekend of 21-22 February, including the text message she sent to her roommate. But, how could this help SA Mack beyond corroborating the roommate's statement? One useful feature of cellphones is the ability of service providers to determine their location at the time of a

---

[35] *See supra* notes 20-22 and accompanying text for discussion of preservation of evidence.

[36] *See supra* note 12 and accompanying text for discussion of subpoenas.

[37] The military department IGs do not have authority to issue subpoenas. OFFICE OF LEGAL POLICY, U.S. DEP'T OF JUSTICE, REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES app. A1, 57 (2002), *available at* http://www.usdoj.gov/archive/index-olp.html.

[38] DOD IG Memorandum, *supra* note 24, at attachment 2, listing crimes for which DOD IG will issue a subpoena.

transmission.[39] However, cell phone location data is not available using a subpoena. Instead, SA Mack needs a judicial order pursuant to 18 U.S.C. § 2703(d)—an order not available to the military—for "other records" held by a service provider.[40] Again, SA Mack's investigation would end but for the support provided by the civilian police. The district attorney obtains a 2703(d) order from the civilian judge, directing Verizon Wireless to disclose non-content records—including cell phone location records—related to SrA Sue's cell phone calls on 21-22 February. In turn, Verizon provides logs revealing that the text message she sent to her roommate was not sent from the area where the favorite diner is located, but from the far side of the city. This information is certainly helpful in ruling out SrA Sue's alibi and providing further leads.

Subpoenas for subscriber information to Yahoo! and Google provide email account registration information and logs of the originating and destination email and Internet protocol (IP) addresses for the respective email accounts, prettys@yahoo.com and joe223322@gmail.com. The registration information provided by subscribers to free webmail services may be unreliable, because free web-based services such as Yahoo! and Gmail usually have few controls on the information that the subscriber inputs when registering. However, Internet connection logs can be valuable. Among other things, these logs provide clues to the IP address of the computer from which the subscriber logged in to the webmail service at a particular time and date. By using a "whois" [41] online service, SA Mack can determine the owner of the IP addresses—often ISPs—and requests the district attorney to subpoena those owners to provide subscriber information about the person using the IP address at the time in question. In SrA Sue's case, this process reveals that prettys@yahoo.com is SrA Sue and that joe223322@gmail.com is Joe Dealer, a primary suspect in local drug trafficking investigations. Joe resides in the neighborhood from which SrA Sue messaged her friend on 21 February, the Saturday night before she was picked for the drug testing. The records disclosed by the service providers also show that SrA Sue and Joe emailed each other frequently before the weekend of 21-22 February, but that only two

[39] *See*, *e.g.*, In Re Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), No. MDB-07-10192-RGS (D. Mass. Sept. 17, 2007) (memorandum and order on government's motion requesting review), *available at* http://pacer.mad.uscourts.gov/dc/cgi-bin/.

[40] *See supra* note 14 and accompanying text for discussion of 2703(d) orders.

[41] "Such data is commonly referred to as 'WHOIS data,' and includes elements such as the domain registration creation and expiration dates, nameservers, and contact information for the registrant and designated administrative and technical contacts." Internet Corporation for Assigned Names and Numbers [hereinafter ICANN], Glossary, http://www.icann.org/en/general/glossary.htm#W (last visited July 28, 2009). ICANN coordinates the worldwide assigment of domain names on the Internet.

emails were sent after the weekend: one from SrA Sue to Joe, and his reply.

Those emails could provide important evidence, particularly in light of the paper copy of SrA Sue's email seized by the investigators. In some situations, a subpoena can be an appropriate means for obtaining the content of email retrieved (accessed or downloaded) by the recipient or located in electronic storage for more than 180 days. However, a 2703(a) search warrant is necessary to compel service providers to disclose the content of email less than 180 days old and not opened by the recipient.[42] Unless SA Mack knows that all of the stored communications have been opened or are more than 180 days old, it's better to obtain a warrant. In SrA Sue's case, SA Mack does not yet know that the last email sent from Joe was never read by SrA Sue. A subpoena for email content would not reveal either the content of the email or the fact that this email had not been opened, although a thorough analysis of subscriber records might show that the email existed.

The best way to discover what Joe wrote to SrA Sue in that last email is to obtain a 2703(a) search warrant, directing Yahoo! to disclose the contents of the email. Our facts provide ample probable cause. As with the 2703(d) order, SA Mack cannot go to the commander, convening authority, or military judge for a warrant. In the case of SrA Sue, the SA Mack again receives help from the local district attorney, who obtains a 2703(a) warrant from the civilian judge. Yahoo!'s disclosure reveals that Joe's last email to Sue was, "Just because I got the stuff for you don't mean I have to listen to your problem." Maybe not critical to prove SrA Sue's guilt, this evidence could be particularly important in proving Joe's connection to this case.

In this simple example of a routine drug use investigation, electronic evidence stored by service providers enables the case agent investigating SrA Sue to get a more complete picture of what happened. Using SCA procedures, SA Mack shows that it is likely SrA Sue was not where she claimed and that Joe was likely the person who provided her with the cocaine. In addition to the use of this electronic information as evidence, in itself, the data disclosed by service providers creates useful leads for further investigation. Yet, SA Mack is dependent upon a centralized DOD process for subpoenas; when the DOD IG does not assist with subpoenas, he must find a willing civilian law enforcement agency to open a joint investigation. He also must rely on civilian prosecutors to obtain 2703(d) orders and 2703(a) search warrants, making SCA procedures anything but routine. If no civilian law enforcement entity with SCA power will participate in the

[42] See *supra* notes 14-19 and accompanying text for discussion of search warrants.

investigation, then MCIO's investigation may well be over before it really begins.

V. SOLUTIONS

A comprehensive solution giving MCIOs the ability to obtain the full gamut of information held by public service providers would require Congressional action to amend the SCA, UCMJ, or other statutory basis for SCA powers. Even without legislative action, however, there are steps that the DOD IG and the MCIOs could take to leverage their existing authorities and their access to SCA compulsory process. At least two interim options would provide MCIOs with better access to the investigative tools authorized by the SCA, namely (1) for the DOD IG to more readily issue administrative subpoenas, and (2) for the MCIOs to improve cooperative arrangements with federal and local law enforcement authorities.

In the following paragraphs, we discuss and assess the various options for giving MCIOs the tools necessary to fully investigate criminal cases involving evidence governed by the SCA. As with our discussion of the SCA, we do not delve deeply into legal or policy analyses of the possible solutions presented here. These alternatives merely highlight some difficulties in producing an overall fix to the SCA's limits for MCIOs.

A. Expanded Subpoena Authority

Expanding military authority to issue subpoenas would be a significant initial step towards giving MCIOs better access to stored information held by public service providers. The military has two types of subpoena authority that extend beyond military jurisdiction: the administrative subpoena power given to the DOD IG,[43] and the subpoena authority given to a summary court-martial or trial counsel to secure civilian witnesses or evidence for that court-martial.[44] In practice, however, neither of these subpoena options gives MCIOs the ability to easily and routinely obtain SCA covered information from public service providers.

Because it does not appear to require legislation, the easiest way to give MCIOs a more effective and responsive subpoena power would be for the DOD IG to expand its subpoena program to include all general crimes investigated by the MCIOs. This is not a new idea. The DOD IG studied this issue in 2001 and found that MCIOs lacked a "fully effective" means for compelling production of evidence because

[43] 5 U.S.C. app. 3 § 6(a)(4) (2006); DOD DIR. 5106.01, *supra* note 24, para. 5.6.
[44] UCMJ art. 46 (2008); MCM, *supra* note 25, MIL. R. EVID. 703(e)(2).

of the military services' limited authority to issue subpoenas and because the Inspector General does not normally issue subpoenas in general crimes investigations unless the Department of Defense is the "victim."[45] By 2008, the DOD IG changed its policy, and now MCIOs can obtain DOD IG subpoenas for non-fraud criminal investigations, if the investigation has a sufficient DOD nexus and involves one of the offenses the DOD IG determined to warrant its involvement.[46] The list of offenses for which DOD IG will issue a subpoena includes the most serious crimes,[47] and the DOD IG took steps to make it easier for MCIOs to request subpoenas.[48] However, the list does not include many common offenses or any of the purely military offenses such as desertion,[49] absence without leave,[50] and failure to obey order or regulation.[51] If investigating any of these offenses, without also investigating one of the offenses on the DOD IG list, the MCIOs cannot obtain DOD IG subpoenas to compel public service providers to disclose routine—and often important—information related to the case.

As DOD IG policy has evolved from issuing mostly fraud-related subpoenas to regularly issuing subpoenas for serious general crimes, the policy should further expand the DOD IG's subpoena program to include all crimes under the UCMJ. Thus, in any criminal investigation, MCIOs could obtain administrative subpoenas pursuant to the SCA to compel public service providers to disclose a wide variety of information held in relation to subscribers and customers.[52] There

---

[45] DOD IG CRIMINAL INVESTIGATIVE POLICY AND OVERSIGHT, EVALUATION OF SUFFICIENCY OF SUBPOENA AUTHORITY WITHIN THE DEPARTMENT OF DEFENSE IN SUPPORT OF GENERAL CRIMES INVESTIGATIONS, REPORT NO. CIPO2001S004 (May 15, 2001), *available at* http://www.dodig.mil/Inspections/IPO/evalreports.htm. At the time, 95 percent of DOD IG subpoenas supported fraud investigations. *Id.* at 1.

[46] DOD IG Memorandum, *supra* note 24.

[47] *Id*. at attachment 2. The list includes homicides, kidnapping, trafficking in persons, robbery, bomb threats, arson, drug offenses not including possession, felony assaults, serious firearms offenses, sexual assault, terrorism, espionage, and a few other serious crimes.

[48] The DOD IG subpoena program website provides helpful and practical information such as a guide for "Subscriber Data Obtainable by Subpoena from Internet Service Providers Pursuant to 18 USC §2703." U.S. Dep't of Defense Office of Inspector General, Subpoena Documents for Downloading, http://www.dodig.mil/inspections/IPO/Subpoena/SubpoenaIndex.htm (last visited Aug. 4, 2009).

[49] UCMJ art. 85 (2008).

[50] *Id*. art. 86.

[51] *Id*. art. 92.

[52] Although our discussion is focused on the SCA and obtaining evidence from public service providers, such a policy would benefit MCIOs in other situations where an administrative subpoena is necessary to compel a third party to produce records. For example, administrative subpoenas are sometimes necessary to obtain financial information from individuals. *See* Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2006); U.S. DEP'T OF DEFENSE, INSTR. 5400.15, GUIDANCE ON OBTAINING INFORMATION FROM FINANCIAL INSTITUTIONS (Dec. 2, 2004) (C1, Jul. 3, 2007).

appear to be no legal impediments to expand this program; however, it would require the DOD IG to increase staffing and other resources.[53]

In addition to an expanded DOD IG subpoena program, MCIOs could benefit from other sources of enhanced subpoena authority. The trial counsel could be authorized to issue subpoenas at an earlier stage of the military justice process. Investigating Officers appointed to conduct pre-referral investigations under Article 32, UCMJ, might be given subpoena authority similar to that given to officers detailed to conduct depositions.[54] These alternatives would require amendments to existing statutes—the UCMJ or SCA—and executive orders, such as the Rules for Courts-Martial.[55] In any of these situations, the command or installation staff judge advocate could be a major player, working with military investigators from the inception of the case to prepare and submit subpoena requests to the appropriate authority.[56] Making it easier for case agents to obtain SCA subpoenas would make significant amounts of data routinely available during investigations. But, this fails to address the inability of the military to obtain other records and the contents of electronic communications from public service providers.

B. Legislative Remedies to Expand 2703(d) Order and 2703(a) Search Warrant Authority

As discussed earlier, under the SCA an 18 U.S.C. § 2703(d) order for transactional information, or an 18 U.S.C. § 2703(a) search warrant for contents of communications, can only be issued by a "court of competent jurisdiction," which 18 U.S.C. § 3127(2) defines as "any district court of the United States (including a magistrate judge of such a court) or any U.S. court of appeals having jurisdiction over the offense being investigated" or "a court of general criminal jurisdiction of a State

---

[53] The DOD IG has certainly considered whether this function could be further delegated, for example, to the Service IGs. At least one federal court has interpreted the Inspector General Act of 1978 to permit the IG to delegate subpoena authority. United States v. Custodian of Records, Sw. Fertility Ctr., 743 F. Supp. 783, 786 (W.D. Okla. 1990). This delegation extends to individuals that the IG "select[s], appoint[s], and employ[s] . . . to carry out the functions . . . of the Office." *Id.* citing 5 U.S.C. app. 3 § 6(a)(7) (2006). However, the Service IGs are independent of the DOD IG, and the scope of the DOD IG's authority to delegate subpoena power may not extend to the Service IGs.

[54] See, MCM, *supra* note 25, R. C. M. 703(e)(2).

[55] For another view on broadening the military's subpoena power, see Major Joseph B. Topinka, *Expanding Subpoena Power in the Military*, ARMY LAW., Sept. 2003, at 15.

[56] Such coordination would be in keeping with the Air Force's efforts to improve integration of investigations into the military justice process. *See* Memorandum, The Inspector General, The Judge Advocate General, and the AFOSI Commander, U.S. Air Force, to AFOSI Special Agents and U.S. Air Force Judge Advocates, subject: Implementation Plan for Investigation to Action Working Group Recommendations (2 Mar. 2009).

authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device."[57] The definition of a "court of competent jurisdiction" contained in 18 U.S.C. § 3127(2) both prohibits military judges (or magistrates) from issuing SCA process and limits federal and state courts to issuing SCA process only in cases where the court has jurisdiction over the offense under investigation.[58] If the offense under investigation violated the UCMJ and there is no governing federal or state criminal statute, or occurred in a location outside of the geographic jurisdiction of a "court of competent jurisdiction," then there is no legal basis for using the SCA. At least two statutory fixes could remedy this situation and ensure MCIOs are able to fully avail themselves of SCA compulsory process in criminal investigations. A brief analysis of those potential statutory fixes follows.

The first potential statutory fix is for Congress to authorize military judges or military magistrates to directly issue process under the SCA. This approach significantly expands the role that military judges and magistrates have traditionally played in military investigations. It would have the advantage of providing military investigators with ready access to judicial officials empowered to issue compulsory process for evidence in the control of public service providers, thereby speeding up military investigations where electronic evidence is needed. The potential hurdles in pursuing this statutory fix could include concerns related to granting military authorities the power to compel civilian entities to produce evidence in furtherance of military investigations,[59] the need to revise the MCM and various Department of

---

[57] 18 U.S.C. § 3127(2) (2006).

[58] It is worth noting that a strict reading of the definition of a "court of competent jurisdiction," contained in 18 U.S.C. § 3127(2) would appear to empower the U.S. Court of Appeals for the Armed Forces (hereafter CAAF) to issue process under the SCA, because in the context of a UCMJ criminal investigation, CAAF is "[a] United States court of appeals having jurisdiction over the offense being investigated." It is difficult, however, to conceive of a practical, workable procedure for requesting and obtaining SCA process from any U.S. court of appeals, to include CAAF. Moreover, the authors are not aware of any reported instance where a U.S. court of appeals has issued compulsory process pursuant to the SCA. Therefore, we would not advocate this as a realistic solution for MCIOs to obtain SCA process.

[59] The Posse Comitatus Act (PCA), 18 U.S.C. § 1385 (2006), generally prohibits the military from directly enforcing civilian laws, or subjecting civilians to regulatory, compulsory, or prescriptive military power, and any statutory proposal that seeks to expand military authority over civilian entities, e.g., by authorizing military authorities to compel public service providers to produce evidence, seems likely to raise PCA concerns. However, in other instances where Congress has expanded military criminal investigative authority, e.g., by authorizing MCIOs to execute warrants and arrest civilians, PCA concerns have been addressed by, for instance, limiting expansion of MCIO authority only to civilian agents and excluding uniformed military investigators. *See* 10 U.S.C. §§ 4027, 7480, and 9027 (2006) (extending warrant execution and civilian arrest authority to civilian agents of the Army Criminal Investigation Command,

Defense and military service regulations and policies applicable to criminal investigations, and the need for an enforcement mechanism similar to that contained in Rule for Courts-Martial 703. None of these potential concerns appear insurmountable, however.

The second possible statutory fix is for Congress to amend the SCA to explicitly authorize U.S. district court judges and federal magistrate judges to issue SCA process in cases involving investigations of UCMJ criminal offenses. Congress could accomplish this by either amending 18 U.S.C. § 3127(2) to specifically give United States district court judges and federal magistrates jurisdiction over investigations involving the UCMJ's punitive articles,[60] or by adding a separate statutory provision to the SCA that specifically authorized federal (and perhaps even state) courts to issue SCA process in furtherance of military criminal investigations. Taking this approach would ensure that MCIOs had full access to information governed by the SCA, while also ensuring that military requests to issue SCA process were reviewed by the same federal magistrates and U.S. district court judges who handle these requests on a daily basis.

Congress clearly has the authority to make 18 U.S.C. § 2703(d) orders and 18 U.S.C. § 2703(a) search warrants available to MCIOs conducting criminal investigations. The Joint Service Committee on Military Justice (JSC) is charged with reviewing and recommending changes to the MCM and the UCMJ, to ensure they "fulfill their fundamental purpose as a comprehensive body of military criminal law and procedure."[61] A collaborative effort between the JSC, the MCIOs, and the Department of Justice might be an appropriate mechanism to take up this issue and make recommendations regarding the best way to provide MCIOs with the investigative tools they need for electronic evidence controlled by public service providers. We strongly encourage the Department of Defense and the Department of Justice to develop and propose to Congress an appropriate set of statutory fixes at the earliest available opportunity, so that MCIOs can take full advantage of the authorities provided by the SCA when conducting criminal investigations pursuant to the UCMJ.

---

the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations, respectively).

[60] The UCMJ's punitive articles (to include attempt, conspiracy, solicitation, and the general articles) are contained in Articles 80-134. 10 U.S.C. §§ 880-934 (2006).

[61] DEP'T OF DEFENSE, DIR. 5500.17, ROLE AND RESPONSIBILITIES OF THE JOINT SERVICE COMMITTEE (JSC) ON MILITARY JUSTICE, para. 3 (3 May 2003).

VI. CONCLUSION

The Stored Communications Act is an often indispensible workhorse for civilian law enforcement agencies. It provides necessary mechanisms for obtaining evidence that criminal suspects routinely create when they call or send a text message to their accomplices, chat online, or otherwise communicate electronically. City police teamed with their local district attorneys, and federal law enforcement agents working with Assistant U.S. Attorneys, can quickly obtain grand jury subpoenas or judicial orders and warrants for electronic evidence. Unfortunately, these mechanisms are largely unavailable to MCIOs. In general crime investigations, even the versatile administrative subpoena is limited by DOD IG policy to a group of serious crimes. This policy may make sense from a resource allocation perspective, but it limits military investigators in their ability to thoroughly and expeditiously investigate the common crimes that occur on military installations, such as cocaine use by military members, as well as those crimes that fall exclusively within military jurisdiction, such as desertion or dereliction of duty. Further, the trial counsel subpoena is of limited utility in criminal investigations because it is unavailable until a case is referred to a court-martial. Judicial orders and warrants that can compel public service providers to produce relevant evidence are essentially unavailable to MCIOs without civilian law enforcement cooperation.

Congress can fix this problem by enacting statutory amendments that will permit military investigators to take advantage of the tools offered by the SCA. Military criminal investigators and attorneys can work together to advocate for such changes to the law, whether as limited amendments to the SCA, or as more sweeping changes involving the UCMJ. While we wait for this to happen, DOD IG should expand its subpoena program to support requests for administrative subpoenas in all criminal investigations, particularly those involving offenses within exclusive military jurisdiction and prosecutable only under the UCMJ, and MCIOs should continue to take full advantage of the existing DOD IG subpoena program. Finally, the military legal community and MCIOs should strive for the support of their federal and state counterparts to use civilian means for obtaining key evidence via the SCA in criminal investigations that have both a military and a federal or state basis for jurisdiction.

CYBER WARFARE OPERATIONS: DEVELOPMENT AND USE UNDER INTERNATIONAL LAW

MAJOR ARIE J. SCHAAP

Major Arie J. Schaap (B.A., University of North Dakota (1995); J.D., California Western School of Law (1999); LL.M., George Washington University (2008)) is currently assigned to the Directorate of Legal Services, Headquarters Air Command, RAF High Wycombe, United Kingdom. Prior to his current assignment, he served as the Deputy Staff Judge Advocate, 67th Network Warfare Wing, Lackland Air Force Base, Texas. He is a member of the Utah Bar.

We know that if someone shoots missiles at us, they're going to get a certain kind of response. What happens if it comes over the Internet?[1]

I. INTRODUCTION

In 2000, John Serabian, the Information Operations Issue Manager for the Central Intelligence Agency (CIA), noted the CIA was "detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber warfare programs in other countries."[2] He further asserted that the countries developing cyber programs "recognize the value of attacking adversary computer systems, both on the military and domestic front."[3]

As of 2007, there were an estimated 120 countries working on cyber attack commands, and in 10 to 20 years experts believe we could see countries jostling for cyber supremacy.[4] States are no doubt preparing to launch international all-out online attacks and the current political environment includes countries testing the waters to gauge the potential influence, and risks, of such assaults.[5] The assistant director of the FBI's cyber division stated that computer attacks pose the biggest risk "from a national security perspective, other than a weapon of mass destruction or a bomb on one of our major cities."[6] NATO's Chief of Cyber Defense concurs, stating that "cyber terrorism [and] cyber attacks pose as great a threat to national security as a missile attack."[7]

As states begin to focus their energies on developing doctrine and weapons for conducting cyber warfare operations, it is essential that we move beyond just the realization that cyberspace is an important new battleground for conducting warfare operations and recognize the need to come to an understanding of what rules regulate this new battlefield. One commentator noted:

> The rapid advancement of cyber attacks and the emergence of cyber warfare have caught government

---

[1] Randall Mikkelsen, *U.S. Not Ready for Cyber Attack*, REUTERS, Dec. 19, 2008, *available at* http://www.reuters.com/article/technologyNews/idUSTRE4BI00520081219 (quoting Michael Chertoff, Secretary of Homeland Security).

[2] John A. Serabian, Jr., Statement for the Record Before the Joint Economic Committee on Cyber Threats and the US Economy (Feb. 23, 2000) *available at* https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html.

[3] *Id.*

[4] MCAFEE, INC., MCAFEE VIRTUAL CRIMINOLOGY REPORT, CYBERCRIME: THE NEXT WAVE, 13 (2007), *available at* http://www.mcafee.com/us/research/criminology_report/default.html.

[5] *Id.*

[6] Special, *Cyber attacks ranked 3rd danger behind nuclear war*, ARY ONEWORLD, Jan. 8, 2009, *available at* http://www.thearynews.com/english/newsdetail.asp?nid=19868.

[7] Kevin Coleman, *Cyber Weapons and E-Bombs*, DEFENSETECH.ORG., Mar. 13, 2008, *available at* http://www.defensetech.org/archives/cat_cyberwarfare.html.

> and military leaders around the world off guard. Decision making in time requiring defensive measures or military crisis is guided by doctrine and rules of engagement, but in the case of cyber attacks and cyber warfare they do not currently exist.[8]

For over a century, states have developed rules of international law, such as the Geneva Conventions, which seek to avoid war or minimize human suffering when conflicts occur.[9] Additionally, as new technologies emerge, states have drafted new sets of laws, such as treaties restricting biological, chemical and laser weapons.[10] Yet governments have so far resisted calls to craft new rules of international law to govern attacks on or by computers.[11] As a result, current international law does not explicitly address cyber warfare.[12] However, the fact that a particular military activity is not specifically regulated does not mean it can be used without restrictions.[13] While the international community remains unsettled on whether cyber techniques are legally considered weapons and whether cyber attacks can be considered legitimate acts of armed conflict,[14] the denial of service (DoS) attacks against Estonia in 2007 and Georgia in 2008 illustrate that this new form of warfare is operational and also reinforces the need to develop a better understanding of how international law relates to cyber warfare. Without such an understanding, this emerging form of warfare will create uncertainties as to the legality of certain acts; this uncertainty has the potential to then escalate tensions and intensify military operations beyond the cyber domain. For example, more than one senior Russian military official supported the notion that "the use of Information Warfare against Russia or its armed forces will categorically not be considered a non-military phase of a conflict whether there were casualties or not"[15] and that "Russia retains the right

---

[8] Kevin Coleman, *Cyber Attacks & Warfare – Rules of Engagement*, DEFENSETECH.org., Nov 28, 2008, available at http://www.defensetech.org/archives/cat_cyberwarfare.html.

[9] Duncan B. Hollis, *E-war rules of engagement*, L.A. TIMES, Oct 8, 2007, *available at* http://www.latimes.com/news/opinion/la-oe-hollis8oct08,0,5897172.story?coll=la-opinion-rightrail.

[10] *Id.*

[11] *Id.*

[12] Stephen W. Korns and Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS – U.S. ARMY WAR COLLEGE QUARTERLY, Vol. XXXVIII, No. 4 (Winter 2008-2009), at 60, 63, *available at* http://www.carlisle.army.mil/usawc/parameters/08winter/korns.pdf.

[13] Knut Dormann, *Computer Network Attack and International Humanitarian Law*, INTERNATIONAL COMMITTEE OF THE RED CROSS, May 19, 2001, *available at* http://www.icrc.org/Web/Eng/siteeng0.nsf/html/5P2ALJ.

[14] Korns & Kastenberg, *supra* note 12, at 63.

[15] STEVEN A. HILDRETH, CONGRESSIONAL RESEARCH SERVICE REPORT FOR CONGRESS No. RL30735, CYBERWARFARE 11 (June 19, 2001), *available at* http://www.fas.org/

to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor State itself."[16]

This paper is divided into nine parts. Section II reviews the definitions of key terms associated with cyber warfare operations. Section III examines the development of cyber warfare doctrine and organizational structure. Section IV will provide an overview of weapons associated with cyber warfare. Section V will examine cyber warfare operations in relation to espionage under international law. Section VI will examine cyber warfare operations and use of force. Section VII will analyze cyber warfare operations in relation to the law of war. Section VIII will examine other treaties and conventions relating to cyber warfare operations. Section IX will give brief concluding thoughts and recommendations.

II. DEFINING KEY TERMS

To develop a better understanding of how international law relates to cyber warfare operations, one must begin by defining what is cyber warfare. However, in order to understand a definition of cyber warfare, it is necessary to first define cyberspace.

A. Cyberspace

While there is no internationally accepted definition of "cyberspace," numerous definitions exist. 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."[17] Thomas Wingfield, in his book *The Law of Information Conflict: National Security Law in Cyberspace*, gives a more plain language definition. "Cyberspace is not a physical place – it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the

---

irp/crs/RL30735.pdf; *see also* Timothy L. Thomas, *Russian Views on Information Based Warfare*, AIRPOWER J., Special Ed. 1996, at 25.

[16] Thomas, *supra* note 15, at 25 (quoting V.I.Tsymbal, Russian military analyst, Concept of Information Warfare, Address at the Russian-US conference in Moscow: Evolving Post-Cold War National Security Issues (Sept. 12-14, 1995)).

[17] JOINT CHIEFS OF STAFF, JOINT PUBLICATION 1-02, DEP'T OF DEF. DICT. OF MILITARY & ASSOC'D TERMS, at 141 (12 Apr. 2001) [hereinafter JOINT PUB. 1-02], *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

World Wide Web."[18] A 2001 Congressional Research Service (CRS) Report for Congress defined "cyberspace" as the "total inter-connectedness of human beings through computers and tele-communication without regard to physical geography."[19]

These multiple definitions of "cyberspace" illustrate the difficulty in defining the term, which may be one of the difficulties in creating any type of common agreement among states as to how international law should be applied to warfare conducted in cyberspace. I would propose that for the purpose of analyzing military operations in cyberspace, one should start by focusing primarily on computer networks. Therefore, for purposes of this article, I will utilize the definition of cyberspace proposed by the National Military Strategy for Cyberspace Operations: "A domain characterized by the use of [computers and other electronic devices] to store, modify, and exchange data via networked systems and associated physical infrastructures."[20]

B. Cyber Warfare

As with the term "cyberspace," there is no widely accepted definition of "cyber warfare." The Department of Defense defines "cyber operations" as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[21] The Department of Defense defines the phrase "computer network attack" as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[22] Air Force Policy Directive 10-7 uses the term "network warfare operations" to define "the integrated planning and employment of military capabilities to achieve desired effects across the interconnected analog and digital portion of the battlespace."[23] This Policy Directive uses the term "network attack" to define "the employment of network-based capabilities to destroy, disrupt, corrupt,

[18] THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 17 (Aegis Research Corp. 2000).
[19] Hildreth, *supra* note 15 at 1.
[20] Staff Seargant C. Todd Lopez, *Fighting in Cyberspace Means Cyber Dominance*, A.F. PRINT NEWS, Feb 28, 2007, *available at* http://www.af.mil/news/story.asp?id=123042670.
[21] JOINT PUB. 1-02, *supra* note 17 at 141. It further notes that such operations include computer network operations and activities to operate and defend the Global Information Grid.
[22] *Id.* at 113.
[23] U.S. DEP'T OF AIR FORCE POLICY DIR. 10-7, INFORMATION OPERATIONS 19 (6 Sept. 2006) [hereinafter AFPD 10-7], *available at* http://www.fas.org/irp/doddir/usaf/afpd10-7.pdf. It further provides that network operations are conducted in the information domain through dynamic combination of hardware, software, data, and human interactions. *Id.*

or usurp information resident in or transiting through networks."[24] A 2001 CRS Report for Congress, notes that "[c]yberwarfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace, as well as denying an adversary's ability to do the same."[25] A 2006 CRS Report for Congress defined the phrase "computer network attack" as "operations to disrupt or destroy information resident in computers and computer networks."[26] Kevin Coleman, a Senior Fellow and Strategic Management Consultant at the Technolytics Institute, an independent executive think tank, defined "cyber war" as "a conflict that uses hostile, illegal transactions or attacks on computers and networks in an effort to disrupt communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defenses."[27]

These various definitions again illustrate the difficulty in defining what is meant by "cyber warfare." Recognizing that military operations in cyberspace could be viewed as warfare, I propose the phrase "cyber warfare operations" be used in analyzing the wide range of military operations in cyberspace and suggest the following definition: "the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state."

III. DEVELOPMENT OF CYBER WARFARE DOCTRINE AND ORGANIZATIONAL STRUCTURE

This section will examine the development of cyber warfare operations in the United States, in particular, the U.S. Air Force. It will focus on doctrine, organization, and training. It will then provide an overview of the development of cyber warfare operations in other states.

A. Development of Cyber Warfare Operations in the United States

The current state of planning for cyber warfare operations has been likened to the early years following the invention of the atomic

---

[24] *Id.* It further notes that networks include telephone and data services networks and that NetA incorporates Computer Network Attack as defined in joint doctrine. *Id.*

[25] Hildreth, *supra* note 15, at 1.

[26] CLAY WILSON, CONG. RES. SERVICE REP. FOR CONGRESS NO. RL31787, INFORMATION OPERATIONS AND CYBERWAR: CAPABILITIES AND RELATED POLICY ISSUES 5 (Sept. 14, 2006), *available at* http://www.fas.org/irp/crs/RL31787.pdf. This report states that a distinguishing feature of CNA is that it relies on a data stream used as a weapon to execute an attack and provided as an example, the sending a digital signal stream through a network to instruct a controller to shut off the power flow. *Id.*

[27] Kevin Coleman, *The Cyber Arms Race Has Begun*, CSO ONLINE, Jan. 28, 2008, *available at* http://www2.csoonline.com/exclusives/column.html?CID=33496.

bomb a half-century ago, when thinking about how to wage nuclear war lagged behind the ability to launch one.[28] Richard A. Clarke, a former special advisor to the President on cyber security, once stated, "we have capabilities, we have organizations; we do not yet have an elaborated strategy, doctrine, procedures."[29] However, this is starting to change. The first step towards developing a cyber warfare strategy occurred in the summer of 2002, when the President signed National Security Presidential Directive 16, which called for a national policy on the rules of engagement for using cyber warfare as a weapon.[30] This Directive instructed "the government to prepare national-level guidance on U.S. policies for launching cyber attacks against enemies."[31] In February 2003, the White House published *The National Strategy to Secure Cyberspace*, a document that presented cyber security as a subset of Homeland Security and contained, among its many initiatives, a call for the government "to improve coordination for responding to cyber attacks within the U.S. national security community."[32] This document also makes clear that the U.S. government reserves the right to respond "in an appropriate manner" if the United States comes under computer attack and that this response could involve the use of U.S. cyber weapons.[33]

Also in 2003, the Department of Defense published the *Information Operations Roadmap*, in which the Secretary of Defense stated, "[t]he Roadmap stands as another example of the Department's commitment to transform our military capabilities to keep pace with emerging threats and to exploit new opportunities afforded by innovation and rapidly developing information technologies."[34] This publication notes that networks are increasingly the operational center of gravity, and that the Department must be prepared to "fight the net."[35] One of the desired outcomes mentioned in this Roadmap is that forces

---

[28] Bradley Graham, *Bush Orders Guidelines for Cyber-Warfare*, WASH. POST, at A1, Feb. 7, 2003.
[29] *Id*.
[30] Tony Bradley, *Pandora's Box*, ABOUT.COM, at 1, http://netsecurity.about.com/library/weekly/aa031703b.htm (last visited Sept. 14, 2009).
[31] John Lasker, *U.S. Military's Elite Hacker Crew*, WIRED, Apr. 18, 2005, at 1, http://www.wired.com/politics/security/news/2005/04/67223 (last visited Sept. 14, 2009).
[32] Lieutenant Colonel Paul Berg, *Air Force Works to Defend Cyberspace, Too*, A.F. PRINT News, Jun. 30, 2008, *available at* http://www.afcyber.af.mil/news/commentaries/story.asp?id=123104768; NAT'L STRATEGY TO SECURE CYBERSPACE (Feb. 2003), *available at* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.
[33] CLAY WILSON, CONG. RES. SERVICE REP. FOR CONGRESS NO. RL32114, COMPUTER ATTACK AND CYBER TERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 15 (Oct. 17, 2003), *available at* http://www.fas.org/irp/crs/RL32114.pdf.
[34] U.S. DEP'T OF DEF., INFORMATION OPERATIONS ROADMAP 1 (Oct. 30, 2003), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.
[35] *Id*. at 6

will be trained with well-tested and reliable computer network attack weapons that are aligned with appropriate target sets and integrated with other information operations capabilities and weapon systems.[36] Since 2003, there has been a gradual development of incorporating cyber warfare into military doctrine and in creating an organizational structure for managing cyber warfare operations, highlighted most recently by the establishment of the 24th Air Force, a new numbered air force focused on the cyber mission.

1. *Doctrine*

Department of Defense Directive O-3600.1 assigns baseline responsibilities for the conduct of "information operations," a term that includes electronic warfare, computer network operations, psychological operations, military deception, and operations security.[37] This Directive states the Department of Defense policy that information operations "shall be employed to support full spectrum dominance by taking advantage of information technology, maintaining U.S. strategic dominance in network technologies, and capitalizing upon near real-time global dissemination of information, to affect adversary decision cycles with the goal of achieving information superiority for the United States."[38] It also provides that information operations capabilities "shall be developed that can be employed in concert with various core, supporting, related, and intelligence capabilities to provide a fully integrated warfighting capability."[39]

Joint Publication 3-13 provides doctrine for information operations planning, preparation, execution, and assessment in support of joint operations.[40] This publication comments that computer network operations "is one of the latest capabilities developed in support of military operations" and stems from the "increasing use of networked computers and supporting IT infrastructure systems by military and civilian organizations."[41] It also notes that computer network operations, along with electronic warfare, are used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure.[42] This publication further remarks that for the purpose of military operations, computer network operations are divided into three

[36] *Id*. at 49.
[37] U.S. DEP'T OF DEF., DIR. 3600.1, INFORMATION OPERATIONS (14 Aug. 2006), *available at* http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf.
[38] *Id*. at 2.
[39] *Id*.
[40] JOINT CHIEFS OF STAFF, JOINT PUBLICATION 3-13, INFORMATION OPERATIONS, at i (13 Feb. 2006) [hereinafter Joint Pub 3-13], *available at* http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.
[41] *Id*. at II-4
[42] *Id*. at II-4-II-5.

categories: computer network attack, computer network defense, and related computer network exploitation enabling operations. [43]

Finally, Air Force Policy Directive 10-7 provides guidance for planning and conducting Air Force information operations to support the warfighter and achieve national strategy objectives.[44] This Directive states that Air Force information operations consist of the integrated application of electronic warfare operations, network warfare operations, and influence operations.[45] It also notes that network operations are comprised of network attack, network defense, and network warfare support.[46]

2. *Organization*

The U.S. Strategic Command (USSTRATCOM) is one of 10 unified commands under the Department of Defense. Part of USSTRATCOM's mission is to ensure freedom of action in cyberspace and to deliver integrated kinetic and non-kinetic effects, including information operations, in support of Joint Force Commander operations.[47] USSTRATCOM helps plan and coordinate offensive computer operations across military and defense agencies through what it calls the Joint Functional Component Command for Network Warfare (JFCC-NW).[48]

JFCC-NW plans and, when directed, executes operations in and through cyberspace, assuring U.S. and allied forces freedom of action, denying adversaries' freedom of action, and enabling effects beyond the cyber domain.[49] One of the key roles for the JFCC-NW is to foster new lines of communication for network warfare-related activities, bringing together the various organizations within the military that work in this area.[50] Additional key tasks for JFCC-NW are to develop standard procedures and doctrine for network warfare activities[51] and ensure that U.S. forces have the tools they need to wage network warfare today and in the future.[52]

---

[43] *Id*. at II-5.
[44] AFPD 10-7, *supra* note 23, at 1.
[45] *Id.* at 3
[46] *Id.*
[47] U.S. STRATEGIC COMMAND website, http://www.stratcom.mil/default.asp (last visited Aug. 24, 2009) (go to "Organization" tab and then "Missions").
[48] Tim Elfrink, *Offutt, StratCom redefines the front line for the computer age*, OMAHA WORLD-HERALD, Feb 11, 2007, *available at* http://integrator.hanscom.af.mil/2007/February/02152007/02152007-21.htm.
[49] U.S. STRATEGIC COMMAND website, *supra* note 47.
[50] Jeremy Singer, *Defending the Nation's Resources in Cyberspace***,** SPACE NEWS, Jan 26, 2007, *available at* http://www.ndu.edu/inss/Press/jfq_pages/editions/i46/12.pdf.
[51] *Id.*
[52] *Id.*

In March 2005, the National Defense Strategy identified cyberspace as a new theater of operations.[53] Also in 2005, the Air Force mission statement expanded to reflect that cyberspace was now an official Air Force domain: "to fly and fight in air, space, and cyberspace."[54] In 2006, the Secretary of the Air Force announced the 8th Air Force as the lead command for cyberspace.[55] Also in 2006, the Air Force stood up the 67th Network Warfare Wing.[56] "The Air Force established the 67th Network Warfare Wing to have an organization solely focused on ensuring that our networks are able to operate in time of peace and war and to have the capability to deal with potential adversaries who may be trying to exploit our networks."[57] The 67th Network Warfare Wing provides full spectrum network operations from the offensive capabilities of assessment, exploitation, and attack to operating and defending Air Force networks.[58] In 2007, demonstrating another step in the Air Force's move to develop an organizational structure for fighting in cyberspace, the Air Force announced it would be officially standing up a provisional Cyberspace Command. [59] This plan, however, was altered slightly in 2008 when the Air Force announced that, instead of creating a new major command, it would be standing up a component numbered air force that would focus on cyberspace warfighting operations.[60]

3. *Training*

---

[53] Kevin B. Alexander, *Warfighting in Cyberspace*, JOINT FORCES Q., July 31, 2007, at 58, 59, *available at* http://www.military.com/forums/0,15240,143898,00.html.

[54] Staff Sgt. C. Todd Lopez, *Cyber Summit begins at Pentagon Nov. 16*, A.F. PRINT NEWS, Nov. 15, 2006, *available at* http://www.af.mil/news/story.asp?id=123032005.

[55] Air Force News Service, *Air Force secretary announces provisional Cyber Command*, Sept 19, 2007, *available at* http://www.af.mil/news/story.asp?id=123068778.

[56] Staff Sergeant Shad Eidson, *New wing brings Air Force dominance to cyberspace*, A.F. PRINT NEWS, July 7, 2006, *available at* http://www.af.mil/news/story.asp?id=123023007.

[57] *Id.*; s*ee also* Tom Vanden Brook, *Air Force trains warriors to defend cyberspace*, USA TODAY, Jan. 28, 2008, *available at* http://www.usatoday.com/tech/news/computersecurity/2008-01-28-cyber_N.htm.

[58] William J. Allen, *Air Force Cybermission Grows-adds Network Warfare and Ops Squadrons*, 8TH A.F. NEWS, July 31, 2007, *available at* http://www.8af.acc.af.mil/news/story.asp?id=123061908.

[59] Air Force News Service, *supra* note 55. The provisional command, called AFCYBER (P), was located at Barksdale Air Force Base, Louisiana. *Id.*

[60] GlobalSecurity.org: Military, *Air Force Cyber Command AFCYBER (P)*, http://www.globalsecurity.org/military/agency/usaf/afcyber.htm (last visited Sept. 10, 2009); *see also* Air Force News Service, *Officials announce proposed bases for new cyber headquarters*, Jan. 21, 2009, *available at* http://www.af.mil/news/story.asp?id=123132187 (noting that Air Force officials have now announced possible locations for the headquarters of this new numbered Air Force focused on the cyber mission).

The Air Force has also implemented new training in the realm of cyber warfare operations. All Airmen, officer and enlisted, will be taught about cyber warfare in their initial accession training.[61] In addition, approximately 100 students per year will receive more advanced instruction at the Undergraduate Network Warfare Training course, where graduates of the six-month program will be able to operate a computer like a weapon system.[62]

B. Development of Cyber Warfare Operations in other States

A number of states are also incorporating cyber warfare as a new part of their military doctrine. This section will briefly examine cyber warfare operations in China, Russia, and North Korea.

1. *Development in China*

China currently possesses a significant cyber weapons and intelligence infrastructure, and their cyber warfare doctrine is designed to achieve global "electronic dominance" by 2050. This includes the capability of disrupting the information infrastructure of their enemies.[63] In 1999, the *PLA Daily*, the official media outlet for the People's Liberation Army (PLA) of the People's Republic of China, stated, "Internet warfare is of equal significance to land, sea, and air power and requires its own military branch."[64] According to military and intelligence sources, Chinese cyber forces have developed detailed plans for cyber attacks against the United States and others.[65] A 2007 Department of Defense report indicated the PLA had established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks.[66] A CRS Report for Congress noted that China was pursuing the concept of a Net Force, which would consist of a strong reserve force of computer experts trained at a number of universities and training centers.[67] In 2005, the PLA began to

[61] Brook, *supra* note 57.
[62] *Id*.
[63] Kevin Coleman, *China's Cyber Forces*, DEFENSETECH.ORG., May 8, 2008, *available at* http://www.defensetech.org/archives/cat_cyberwarfare.html.
[64] Alexander, *supra* note 53.
[65] Coleman, *supra* note 63.
[66] U.S. DEP'T OF DEF. ANN. REP. TO CONG.: MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA 21 (2007) [hereinafter DOD Annual Report to Congress], *available at* http://www.defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf.
[67] Hildreth, *supra* note 15, at 12.

incorporate offensive computer network operations into its exercises, primarily in first strikes against enemy networks.[68]

2. *Development in Russia*

Russia's armed forces, collaborating with experts in the information technology sector and academia, have developed a robust cyber warfare doctrine,[69] with offensive cyber weapons receiving significant attention.[70] Russia's cyber warfare doctrine is designed to act as a force multiplier, which is a military term that describes a weapon or tactic that, when added to and employed along with other combat forces, significantly increases the combat potential of that force.[71] Like all offensive cyber strategies, Russia's includes the capability to disrupt the information infrastructure of their enemies and includes strategies that would disrupt financial markets and military and civilian communications capabilities as well as other parts of the enemy's critical infrastructure prior to the initiation of traditional military operations.[72]

3. *Development in North Korea*

In 1998, the North Korean military created Unit 121, which focuses solely on cyber warfare and has steadily grown in size and capability since its inception.[73] North Korea possesses the technical capability to construct and deploy an array of cyber weapons and in October 2007 tested its first logic bomb[74]—one of the weapons of cyber warfare operations defined below. This test led to a U.N. Security Council resolution banning sales of mainframe computers and laptop PCs to North Korea. However, the U.N. response failed to deter the North Korean military from continuing their cyber weapons development program.[75]

---

[68] DOD Annual Report to Congress, *supra* note 66, at 21.
[69] Charles Billo & Welton Chang, *Cyber Warfare Analysis of the Means and Motivations of Selected Nation States*, INST. FOR SEC. TECH. STUD., Nov. 2004 (Revised Dec. 2004), at 9, *available at* http://www.ists.dartmouth.edu/docs/execsum.pdf.
[70] Kevin Coleman, *Russia's Cyber Forces*, DEFENSETECH.org., May 27, 2008, *available at* http://www.defensetech.org/archives/cat_cyberwarfare.html; *see also* Billo & Chang, *supra* note 69, at 9, noting that information weaponry, weapons based on programming code, receives paramount attention in official cyber warfare doctrine in Russia.
[71] Coleman, *supra* note 70.
[72] *Id*.
[73] Kevin Coleman, *Inside DPRK's Unit 121*, DEFENSETECH.org., Dec. 24, 2007, *available at* http://www.defensetech.org/archives/cat_cyberwarfare.html.
[74] *Id*.
[75] *Id*.

IV. WEAPONS OF CYBER WARFARE OPERATIONS

In the mid 1990s, a study by the RAND Corporation found the costs of developing the cyber weapons needed for conducting cyber warfare to be extremely modest and within financial reach for nearly every state.[76] It is now estimated that about 140 nations have active operational cyber weapons development programs in place.[77] This section provides an overview of different cyber weapons a state could use to engage in cyber warfare.

A. Denial of Service (DoS) Attack

A DoS attack is "an assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted."[78] It is characterized by an explicit attempt to prevent legitimate users of a service from using that service.[79] One of the advantages of this type of attack is that it can be executed with limited resources against a larger and more sophisticated computer or network. For example, an attacker with an old PC and a slow modem may be able to disable much faster and more sophisticated machines or networks.[80]

A distributed denial of service (DDoS) attack is one in which a mass of infected computers or systems attacks an individual system. When conducting a DDoS attack, an aggresor utilizes thousands of infected computers—known as zombies or bots—to concurrently attack a single system.[81] DDoS attacks are difficult to stop because the data flooding the system originates from multiple computers and multiple locations.[82] In the May 2008 issue of *Armed Forces Journal*, Colonel Charles W. Williamson III wrote:

> America needs a network that can project power by building an af.mil robot network (botnet) that can direct

---

[76] Coleman, *supra* note 27.
[77] *Id*.
[78] TechWeb.Com, Technocyclopedia, Denial of Service Attack, http://www.techweb.com/encyclopedia/defineterm.jhtml?term=denialofserviceattack (last visited Sept. 1, 2009).
[79] CERT Coordination Center, *Denial of Service Attacks*, http://www.cert.org/tech_tips/denial_of_service.html (last visited Sept. 8, 2009).
[80] *Id*.
[81] Nono, *Botnets fight back with Denial of service attacks!!*, PC1NEWS.COM, Sep 12, 2008, http://www.pc1news.com/news/0221/botnets-fight-back-with-denial-of-service-attacks-.html (last visited Sept. 8, 2009).
[82] Kevin Coleman, *Department of Cyber Defense, An organization who's time has come!*, TECHNOLYTICS, Nov. 2007, at 2, *available at* http://www.technolytics.com/Dept_of_Cyber_Defense.pdf.

> such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic. America needs the ability to carpet bomb in cyberspace to create the deterrent we lack.[83]

A Permanent Denial-of-Service (PDoS) attack damages a system so badly that it requires replacement or reinstallation of hardware. Unlike a DDoS attack, which is used to sabotage a service or Website, or as a cover for malware delivery, a PDoS is pure hardware sabotage.[84]

B. Malicious Programs

Malicious programs attack by disrupting normal computer functions, or by opening a back door for a remote attacker to take control of the computer.[85] An attack can either immediately disable a computer or incorporate a time delay, after which a remote command will direct the infected computer to transmit harmful signals that disrupt other computers.[86] The technologically savvy often refer to malicious programs as malware, short for malicious software.[87] Malware may delete files or otherwise make them unusable.[88] Common examples of malware include viruses, worms and trojan horses.[89]

A virus attaches itself to a program or file so it can spread from one computer to another.[90] The virus spreads across disks and networks by making copies of itself.[91] In addition to self-replicating code, a virus normally contains a payload.[92] Cyber attackers can program the payload to have malicious side effects such as data

---

[83] Charles W. Williamson III, *Carpet Bombing in Cyberspace*, ARMED FORCES JOURNAL, May 2008, *available at* http://www.armedforcesjournal.com/2008/05/3375884; *see also*, Robert Vamosi, *Carpet bombing networks*, CNET NEWS, May 15, 2008, http://news.cnet.com/8301-10789_3-9945451-57.html (last visited Sept. 8, 2009).

[84] Kelly Jackson Higgins, *Permanent Denial-of-Service Attack Sabotages Hardware*, DARK READING, May 19, 2008, http://archive.cert.uni-stuttgart.de/isn/2008/05/msg00102.html (last visited Sept. 8, 2009).

[85] Wilson, *supra* note 33, at 29.

[86] *Id*.

[87] Techterms.com, The Tech Terms Computer Dictionary, *Malware*, http://www.techterms.com/definition/malware (last visited Sept. 8, 2009).

[88] *Id.*

[89] Techterms.com, *supra* note 87.

[90] Vangie Beal, Webopedia, *The Difference Between a Virus, Worm and Trojan Horse*, INTERNET.COM, June 30, 2006, http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp (last visited Sept. 8, 2009).

[91] *Introduction to Computer Viruses*, SOPHOS.COM, May 26, 1998, http://www.sophos.com/pressoffice/news/articles/1998/05/va_virusesintro.html (last visited Sept. 8, 2009).

[92] *Id*.

corruption or destruction.[93] Almost all viruses are attached to an executable file, which means the virus may exist on a computer but it cannot infect that computer unless the user runs or opens the malicious program.[94]

A worm operates similarly to a virus in that it spreads from computer to computer. However, unlike a virus, a worm has the capability to travel without any help from a person. It does this by taking advantage of file or information transport features on a system, which allow it to travel unaided.[95] The biggest danger with a worm is its capability to replicate itself on a system. Thus, rather than a computer's sending out a single worm, it could send out hundreds or thousands of copies of itself.[96] Due to the copying nature of a worm and its capability to travel across networks, the end result in most cases is that the worm consumes too much system memory or network bandwidth, causing web servers, network servers, and individual computers to stop responding.[97] Cyber aggresors designed recent worm attacks to tunnel into a computer system and allow malicious users to control the infected computer remotely.[98]

A Trojan horse is "a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage."[99] Those who receive a Trojan horse usually fall prey to opening it because it appears to be legitimate software or files from a legitimate source.[100] Trojan horses can cause serious damage by deleting files and destroying information on a system.[101] Trojan horses can also create a back door on computers that gives malicious users access to the system, possibly allowing the compromise of confidential or personal information.[102] Unlike viruses and worms, Trojan horses do not reproduce by infecting other files nor do they self-replicate.[103]

A blended threat is "a sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one threat."[104] Blended threats use server and internet

---

[93] *Id*.
[94] Beal, *supra* note 90.
[95] *Id*.
[96] *Id*.
[97] *Id*.
[98] *Id*.
[99] SearchSecurity.com, *Trojan Horse*, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213221,00.html (last visited Sept. 10, 2009).
[100] Beal, *supra* note 90.
[101] *Id*.
[102] *Id*.
[103] *Id*.
[104] *Id*.

vulnerabilities to initiate, transmit, and spread an attack, which means they can spread quickly and cause widespread damage.[105]

Polymorphic malware is "malicious software that has the ability to change its signature randomly each time it replicates."[106] This technique is used to avoid detection by anti-spyware programs designed to recognize malware by its signature.[107] With polymorphic malware, only the appearance of the code is altered, not the function.[108]

C. Logic Bomb

A logic bomb is malicious code designed to execute if specific events occur or at a predetermined time.[109] Once triggered, it can take down the computer, delete data, or activate a DoS attack by generating bogus transactions.[110]

D. IP Spoofing

IP spoofing, also known as IP address forgery or a host file hijack, is a hijacking technique in which hijackers masquerade as a trusted host to conceal their identity, spoof a Website, hijack browsers, or gain access to a network.[111] When IP spoofing is used to hijack a browser, a visitor who types in the uniform resource locator (URL) of a legitimate site is taken to a fraudulent web page created by the hijacker. If the user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information or computer or network resources.[112]

E. Digital Manipulation

Digital image manipulation is the alteration of an image using computer program tools and software to produce a contrived image, which often reflects new meaning. This technique involves already existing imagery, such as photographs or videos.[113]

---

[105] *Id*.
[106] *See* InternetSecurityZone.com, Glossary, *Polymorphic Malware*, http://www.internetsecurityzone.com/Glossary/Polymorphic_Malware (last visited Sept. 9, 2009).
[107] *Id*.
[108] *Id*.
[109] Coleman, *supra* note 70.
[110] *Id*.
[111] *See* SearchSecurity.com, Definitions, *IP Spoofing*, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1162868,00.html (last visited 9 Sept., 2009).
[112] *Id*.
[113] *See* M/Cyclopedia of New Media, *Digital Manipulation*, http://wiki.media-culture.org.au/index.php/Digital_Image_Manipulation (last visited Sept. 9, 2009).

Doctoring photographs has been around as long as photography itself.[114] In the intelligence and security communities one of the purposes of photo alteration is to misinform or deceive.[115] As digital photo manipulation software increases in technical sophistication and people become more adept at using the software, the task of detecting manipulated images has become very challenging and digital photographic manipulation is now so sophisticated that it is sometimes impossible to discern whether people or objects in a photograph were actually there when the photo was taken.[116] In 2006, it was uncovered that the media engaged in photo manipulation during the conflict between Israel and the Lebanese Hizbullah group.[117] It is quite conceivable that a state could easily engage in photo manipulation, perhaps even changing images displayed on the internet by other states.

It is now possible to manipulate video in real time. In the fraction of a second between video frames, any person or object moving in the foreground can be edited out, and objects that aren't there can be edited in and made to look real.[118] This fluidity stems from the changeable nature of the pixels that make up modern video.[119] It is now possible to insert sets of pixels into satellite imagery data that interpreters would view as battalions of tanks or war planes.[120] Princeton Video Imaging (PVI) bolstered this point in a demo tape set in a suburban parking lot. The scene appeared ordinary except for amidst the SUVs and minivans are several parked tanks and one armored behemoth rolling incongruously along.[121] Deleting people or objects from live video, or inserting prerecorded people or objects into live scenes, is only the beginning. The video manipulators can make previously recorded speakers say and do things they never actually said or did. In addition, modern technology compresses what used to take an hour into a sixtieth of a second, which permits real-time manipulation as a camera records or broadcasts.[122]

The combination of real-time, virtual insertion with existing and emerging post-production techniques opens up a world of manipulative

---

[114] *See, e.g.*, HANY FARID, PHOTO TAMPERING THROUGHOUT HISTORY, http://www.cs.dartmouth.edu/farid/research/digitaltampering (last visited Sept. 9, 2009).
[115] *See* Espionage Information: Encyclopedia of Espionage, Intelligence, and Security, *Photo Alteration*, http://www.espionageinfo.com/Pa-Po/Photo-Alteration.html (last visited Sept. 9, 2009).
[116] *Id*.
[117] *See* Yaakov Lappin, *Reuters Admits to More Image Manipulation*, YNETNEWS.COM, Aug. 7, 2006, http://www.ynetnews.com/articles/0,7340,L-3287774,00.html (last visited Sept. 9, 2009).
[118] Ivan Amato, *Lying With Pixels, Seeing is No Longer believing*, TECH. REV., July 2000, *available at* http://www.technologyreview.com/Infotech/12115/?a=f.
[119] *Id*.
[120] *Id*.
[121] *Id*.
[122] *Id.*

opportunity.[123] For example, one could insert a world leader into a live broadcast of CNN and have the individual say whatever one wishes. Additionally, states could create completely fabricated real time webcasts showing their adversaries doing whatever they deem appropriate for their purposes. James Currie, a professor of political science at the National Defense University, who also has experience as a staffer with TOP SECRET clearance on the Senate's Intelligence Committee and as a legislative liaison for the Secretary of the Army, is convinced that the military and intelligence communities will, or already do, possess real-time video manipulation capabilities.[124] Pentagon planners started to discuss digital morphing after Iraq's invasion of Kuwait in 1990. Covert operators considered creating a computer-faked videotape of Saddam Hussein crying or getting caught in a sexually compromising situation and then distributing the tapes in Iraq and the Arab world.[125]

Voice morphing enables the cloning of speech patterns and creation of an accurate copy of a person's voice, which can then say anything the operator wishes it to say, appearing to be the voice of someone else.[126] George Papcun of the Los Alamos National Laboratory developed this technology.[127] The Washington Post detailed how Mr. Papcun could, in near real time, clone speech patterns and develop an accurate facsimile by using just a 10-minute digital recording.[128]

V. CYBER WARFARE OPERATIONS IN RELATION TO ESPIONAGE

A large amount of the cyber operations performed by a military will involve the collection of data or intelligence stored on another state's network or analyzing the configuration of the network. These types of actions, provided they do not disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, should not be considered cyber warfare operations. The international community should view such activities as a form of espionage or cyber espionage. Espionage is the act of obtaining, delivering, transmitting,

---

[123] *Id*.
[124] *Id*.
[125] William M. Arkin, *When Seeing and Hearing Isn't Believing*, WASH. POST.COM, Feb. 1, 1999, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin020199.htm (last visited Sept. 9, 2009).
[126] *See* Probert Encyclopedia of Science and Technology, *Voice Morphing*, http://www.probertencyclopaedia.com/G_VOICE_MORPHING.htm (last visited Sept. 1, 2009); *see also* Arkin, *supra* note 125.
[127] *Id*.
[128] Arkin, *supra* note 125.

communicating, or receiving information about the national defense of a "victim" state where the "collecting" state possesses an intent to use the information to injure the victim state, or to give an advantage to any other state.[129] The Department of Defense uses the term "computer network exploitation" to describe "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[130] Another term that fits under this category of cyber espionage is what the Air Force calls "network warfare support," which is defined as "actions tasked by or under direct control of an operational commander to search for, intercept, identify, and locate or localize sources of access and vulnerability for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations."[131] Network warfare support "provides information required for immediate decisions involving network warfare operations" and "can be used to produce intelligence, or provide targeting for electronic or destructive attack."[132]

Article 24 of the Annex to the 1907 Hague Convention IV recognizes the lawfulness of espionage during armed conflict, specifically providing that "ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible."[133] No international convention has ever addressed the legality of peacetime espionage and espionage has been practiced by states for centuries.[134] Additionally, international law does not prohibit espionage as a fundamentally wrongful activity.[135]

Thomas Wingfield, a Research Fellow at the Potomac Institute, concluded that the right to conduct espionage is an essential part of a state's inherent right of self-defense and stated, "the 1961 Vienna Convention on Diplomatic Relations recognizes the well-established right of nations to engage in espionage during peacetime and the practice of states has specifically recognized a right to engage in such clandestine intelligence collection activities as an inherent part of foreign relations and policy."[136] Individual states have, however, enacted laws that severely punish espionage against their own

---

[129] *See* Joint Pub. 1-02, *supra* note 17, at 190.
[130] *Id.* at 113.
[131] AFPD 10-7, *supra* note 23, at 20.
[132] *Id*.
[133] Convention Respecting the Laws and Customs of War on Land, and its annex: Regulation Concerning the Laws and Customs of War on Land, art. 24, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631 [hereinafter Hague Convention IV].
[134] Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. Rev. 217, 218 (1999).
[135] *Id*.
[136] Wingfield, *supra* note 18, at 350.

interests.[137] In general, espionage is treated as lawful under public international law and unlawful under domestic law.[138]

Two examples of activities viewed as cyber espionage are the Moonlight Maze and Titan Rain incidents. These two incidents demonstrate how espionage in the computer age has changed. Nevertheless, at its core, it is still espionage and should be looked at differently then cyber warfare operations when attempting to establish lawful or unlawful activities under international law.

In the Moonlight Maze incident, hackers from Russia penetrated Department of Defense computers for over a year, stealing vast amounts of sensitive information.[139] According to Pentagon and FBI officials, Moonlight Maze was a state-sponsored Russian intelligence campaign to secure U.S. technology, which targeted not just the Department of Defense, but also the Department of Energy, NASA, military contractors and military-linked civilian universities.[140] In this incident, the Department of Defense did not report any damage or destruction of networks.[141] Roberta Gross, the NASA Inspector General, stated, "It's difficult to tell what the damage is . . . . They weren't shutting down systems. They were taking file listings, looking to see what's in people's directories."[142] Richard Clark sees the Moonlight Maze intrusions as "pre-war reconnaissance where half a dozen nations are busy scanning each other's networks to get a good map of where the key things are and what are the key vulnerabilities of those networks."[143]

Titan Rain is the name given to a series of coordinated attacks, believed to be Chinese in origin, on U.S. computer systems since 2003.[144] The precise nature, whether state-sponsored espionage, corporate espionage, or random hacker attacks, is uncertain.[145] The United States traced the attacks to the Chinese province of Guangdong and, according to Alan Paller, director of the SANS Institute, the techniques used make it appear unlikely to come from any other source than the military.[146] The hackers are thought to have stolen U.S. military secrets from the Redstone Arsenal, home to the Army Aviation

---

[137] Scott, *supra* note 134, at 218.
[138] Jennifer J. Rho, *Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute*, 7 CHI. J. INT'L L. 695, 701 n.48 (2007).
[139] Christopher C. Joyner and Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 840 (2001), *available at* http://www.ejil.org/pdfs/12/5/1552.pdf.
[140] *Id*. at 840-841.
[141] *Id*. at 841 n.58.
[142] *Id*.
[143] *Id*. at 841 n.60.
[144] The Language of Computers - Dictionary and Research Guide, *Titan Rain*, http://www.123exp-computing.com/t/03971134833/ (last visited Sept. 1, 2009).
[145] *Id*.
[146] Insecure.org, *Hacker Attacks in US Linked to Chinese Military: Researchers*, Dec. 12, 2005, http://seclists.org/isn/2005/Dec/0059.html (last visited Sept. 8, 2009).

and Missile Command, including aviation specifications and flight-planning software.[147]

VI. CYBER WARFARE OPERATIONS AND USE OF FORCE

The maintenance of international peace and security was the primary reason for creating the United Nations.[148] The U.N. Charter and general international law provide for an absolute prohibition on the use of force by states, except in the case of legitimate self-defense laid down in Article 51 of the Charter.[149] Article 2(3) of the U.N. Charter provides that all Members states "shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered."[150] Article 2(4) of the U.N. Charter provides that all Members "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[151] Article 51 of the U.N. Charter, which provides the sole exception to use of force by individual Members without express Security Council sanction, states:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council . . . .[152]

In *Nicaragua v. United States*, the International Court of Justice confirmed that the prohibition on the use of force was also a principle of customary international law.[153] However, exactly what kinds of action constitute a use of force or armed attack is debatable, as the U.N. Charter does not define either phrase.

A good place to look at what may constitute a use of force or an armed attack is the General Assembly's resolution defining

---

[147] Tom Espiner, *Security experts Lift Lid on Chinese hack attacks*, ZDNET.COM, Nov. 23, 2005, http://news.zdnet.com/2100-1009_22-145763.html (last visited Sept. 9, 2009).
[148] SEAN D. MURPHY, PRINCIPLES OF INTERNATIONAL LAW 439 (2006).
[149] Giuliana Ziccardi Capaldo, *Providing a Right of Self-Defense Against Large Scale Attacks by Irregular Forces: The Israeli-Hezbollah Conflict*, 48 HARV. INT'L L.J. ONLINE 104, http://www.harvardilj.org/online/115 (last visited Sept. 9, 2009).
[150] U.N. Charter art 2(3).
[151] *Id.* art 2(4).
[152] *Id*. art. 51.
[153] Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 188.

aggression.[154] Article 1 of this Resolution uses language similar to that of Article 2(4) of the U.N. Charter; it states, "aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any manner inconsistent with the Charter of the United Nations, as set out in this definition."[155] Article 3 of this Resolution lists seven acts that qualify as acts of aggression and Article 4 notes that these enumerated acts are "not exhaustive."

When analyzing whether cyber warfare operations violate the territorial integrity of another nation, the U–2 incident of 1960 is a good place to start. This involved the downing of an unarmed U.S. reconnaissance plane by a SA-2 surface to air missile (SAM) 1,200 miles inside the Soviet Union.[156] The Soviet Union asserted that U-2 flights over Soviet territory were acts of aggression; however, the U.N. Security Council disagreed, concluding that while the U-2 flight violated Soviet airspace it did not constitute an unlawful use of force in regards to Article 2(4) of the U.N. Charter.[157] If infringement upon the sovereign airspace of another nation does not rise to the level of an unlawful use of force, perhaps infringement upon another nation's networks does not automatically rise to the level of an unlawful use of force. However, it appears self defense actions necessary to stop the intrusion may be permitted. This U-2 incident analysis would be appropriate for most forms of cyber espionage discussed in SectionIV, where the operation consists only of the gathering of data from target or adversary automated information systems or networks, like the Titan Rain and Moonlight Maze examples. While illegal under domestic law, these operations do not constitute an unlawful use of force under international law.[158] However, when more than mere data gathering is involved, the issue becomes less clear. For example, is a DoS attack on one nation by another, which results in the inability of the attacked nation to access web sites and networks, considered an unlawful use of force?

---

[154] Definition of Aggression, G.A. Res. 3314 (XXIX), art. 1, U.N. Doc. A/3314, (Dec. 14, 1974) [hereinafter G.A. Res. 3314].

[155] *Id.* art. 1. Article 3 of this Resolution lists seven acts that qualify as an act of aggression and Article 4 notes that the enumerated acts are "not exhaustive."

[156] *See* U.S. DEPARTMENT OF STATE, 10 FOREIGN RELATIONS OF THE UNITED STATES: 1958-60: E. EUROPE REGION; SOVIET UNION pt. 1 n.147 (1993), *available at* http://dosfan.lib.uic.edu/ERC/frus/frus58-60x1/13soviet7.html.

[157] Wingfield, *supra* note 18, at 352-53.

[158] It should also be noted that the Soviet Union tried the pilot, found him guilty of espionage, and sentenced him to three years imprisonment and seven years of hard labor. Martin Kelly, *Gary Powers and the U-2 Incident*, ABOUT.COM: AM. HIST., http://americanhistory.about.com/od/coldwar/a/gary_powers.htm (last visited Sept. 9, 2009). He only served 1 year 9 months and 9 days before being traded for the Soviet spy Rudolph Abel. *Id.*

In April 2007, important websites in Estonia, including the website of the president, parliament, ministries, political parties, major news outlets, and Estonia's two dominant banks, were hit by a series of DoS attacks.[159] These attacks continued until mid-June.[160] A Defense Ministry spokesman said sites that usually received 1,000 visits a day were buried under as many as 2,000 a second.[161] Officials in Estonia accused Russia of orchestrating the attacks and security officials traced the initial attacks to Russian servers, including domains registered to the government and to the administration of then President Putin.[162] The Kremlin has repeatedly denied government involvement in the attacks, dismissing Estonia's complaints as fabrications.[163] Estonia reported the attacks to the European Union (EU) and the North Atlantic Treaty Organization (NATO).[164]

The NATO Treaty, which Estonia and most EU Member States are a party to, provides that an attack on one of its members shall be considered an attack against all and enables party nations to exercise the right of self-defense recognized by Article 51 of the U.N. Charter.[165] Estonian Defense Minister Jaak Aaviksoo called the attacks a national security situation and compared the situation to the shutdown of sea ports.[166] This comparison is interesting as Article 3(c) of the General Assembly's resolution defining aggression lists "the blockade of the ports or coasts of a State by the armed forces of another State" as an act of aggression.[167] However, it should be noted that Article 41 of the U.N. Charter cites "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication" as a "measure not involving armed force."[168] After discussing the situation with NATO officials, Mr. Aaviksoo stated, "at present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defense, will not automatically be

---

[159] Johnny Ryan, *Growing dangers: Emerging and Developing Security Threats*, NATO REV. (Winter 2007), *available at* http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.
[160] *Id*.
[161] Steven Lee Myers, *'E-stonia' Accuses Russia of Computer Attacks*, N.Y. TIMES.COM, May 18, 2007, http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html?h (last visited Sept. 14, 2009).
[162] *Id*.
[163] *Id*.
[164] Maricelle Ruiz, *Internet Law - Should We Go to War Over a Massive Cyber-Attack?*, INTERNET BUS. L. SERVICES, May 23, 2007, http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1762 (last visited Sept. 9, 2009).
[165] *Id*.
[166] Ryan, *supra* note 148.
[167] G.A. Res. 3314, art. 3(c).
[168] U.N. Charter art. 41.

extended to the attacked country."[169] Shortly after NATO cyber experts went to Estonia the attacks stopped.[170] Some in NATO now believe the attacks were Russia testing the West's preparedness for cyber-warfare in general and of NATO's commitment to its newest, weakest members in particular.[171]

The debate as to whether this type of cyber warfare operation could be considered a use of force was re-energized in August 2008, following accusations that Russia was behind attacks on Georgian government sites shortly before the launching of Russian military action.[172] On August 7, 2008, following separatist provocations, Georgian forces launched a surprise attack against the separatist forces.[173] On August 8, Russia responded to Georgia's act with military operations into Georgian territory, which the Georgian authorities viewed as military aggression against Georgia.[174] The evening of August 7, before the Russian invasion into Georgia commenced, cyber attacks were already being launched against a large number of Georgian governmental websites, making it among the first cases in which a coordinated cyber offensive accompanied, or even preceded, an international political and military conflict.[175] As with the Estonian incident, there is no conclusive proof of who was behind the attacks.[176] However, the level of advance preparation and reconnaissance strongly suggested that officials within the Russian government or military primed Russian hackers for the assault.[177] Scott Borg, director of the U.S. Cyber Consequences Unit, a think tank that advises governments and companies, stated at the time, "we are in a world where governments have not decided yet whether the tools of cyberattacks are

---

[169] Ryan, *supra* note 159.

[170] *Cyber War as the Ultimate Weapon*, STRATEGYWORLD.COM, Jan. 5, 2008, http://www.strategypage.com/htmw/htiw/articles/20080105.aspx (last visited Sept. 9, 2009).

[171] Anne Applebaum, *For Estonia and NATO, A New Kind of War*, WASH. POST, May 22, 2007, at A15.

[172] John Lister, *Are cyber-attacks an act of war?*, TECH.BLORGE.COM, Aug. 16, 2008, http://tech.blorge.com/Structure:%20/2008/08/16/are-cyber-attacks-an-act-of-war/ (last visited Sept. 9, 2009).

[173] ENEKEN TIKK ET. AL., CYBER ATTACKS AGAINST GEORGIA: LEGAL LESSONS IDENTIFIED 4 (Coop. Cyber Def. Ctr. of Excellence 2008), *available at* http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

[174] *Id*.

[175] *Id*. at 4-5

[176] *Id*. at 12.

[177] Brian Krebs, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, WASH. POST.COM, Oct. 16, 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (last visited Sept. 9, 2009).

weapons" and "we don't have any really clear international understandings about these matters."[178]

While the U.N. Charter prohibits the use of force, the international community appears to have concluded that unattributable DoS attacks will not automatically qualify as violating this prohibition.[179] The attack on Estonia briefly upset the operations of some government organizations, including telephone access to the emergency services.[180] However, as discussed above, NATO did not seem to view these attacks as violating the prohibition against the use of force. Ultimately, the international community characterized the Estonian attack as cyber crime or cyber terrorism.[181] The actual damage done in the Georgia incident was minimal; it included some e-mail disruption and public unavailability of some target sites. Again, there was no conclusive evidence that the Russian government executed or sanctioned either set of attacks, although there was no evidence that it tried to stop them either.[182] Similar to the Estonia example, this would probably have to be viewed as cyber crime or cyber terrorism. This would most likely hold true even if the attacks could be attributed back to Russia or if Russia was deemed to "effectively control" the non-state actor, which the Court in *Nicaragua v. U.S.* recognized as the standard for attributing the acts of a non-state actor to the state.[183] This is supported by the legal task team from the NATO-accredited Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, which concluded that "it is highly problematic to apply the Law of Armed Conflict to the Georgian cyber attacks – the objective facts of the case are too vague to meet the necessary criteria of both state involvement and gravity of effect."[184]

What level of impact would it take to rise to a prohibited use of force, and what level of government attribution would justify defensive use of force against a state? Arguably, more than just interfering with a government web site or causing minimal disruption of government services is needed to constitute a prohibited use of force. But what about the interfering with, or disruption of, supervisory control and data acquisition (SCADA) systems, which control elements of the power grid, air traffic control networks, and nuclear power plant safety systems? This is likely one of the next scenarios regarding the issue of

---

[178] Siobhan Gorman, *Cyberattacks on Georgian Web Sites Are Reigniting a Washington Debate*, WALL ST. J., Aug. 14, 2008, *available at* http://online.wsj.com/article/SB121867946115739465.html?mod=googlenews_wsj.
[179] *See* Korns & Kastenberg, *supra* note 12, at 70.
[180] *Marching Off to Cyberwar*, ECONOMIST.COM, Dec. 4, 2008, *available at* http://www.economist.com/science/tq/displaystory.cfm?story_id=12673385.
[181] Korns & Kastenberg, *supra* note 12, at 71.
[182] *Marching Off to Cyberwar*, *supra* note 180.
[183] Capaldo, *supra* note 149, at 105.
[184] Korns & Kastenberg, *supra* note 12, at 71 (citing TIKK ET. AL., *supra* note 173, at 23).

use of force and armed attack in the realm of cyber warfare operations. A recently recorded demonstration conducted by government researchers, called the Aurora Generator Test, investigated a dangerous vulnerability in computers at U.S. utility companies. The test illustrated the potential destruction caused by seizing control of a crucial part of the U.S. electrical grid—an industrial turbine spinning wildly out of control until it becomes a smoking hulk and the power shuts down.[185] The video, produced for the Homeland Security Department, shows commands quietly triggered by simulated hackers having such a violent reaction that the enormous turbine shudders as pieces fly apart and it belches black-and-white smoke.[186] While this electrical attack was a controlled test, the CIA warned in January 2008 that a cyber attack did cause a power blackout in multiple cities outside the United States.[187] Tom Donahue, a CIA senior analyst, informed attendees at a SANS Institute conference that the CIA has information that cyber attackers have disrupted power equipment in several regions outside the U.S. and, in at least one case, the disruption caused a power outage affecting multiple cities.[188] Donahue added that the CIA does not know who executed the attacks or why, but that all of the attacks involved intrusions through the internet.[189] These cyber intrusions into utility systems were deliberate and followed by extortion demands.[190] This clearly demonstrates the capability exists to bring down SCADA systems.

Arguably, a cyber attack that causes physical damage might constitute an armed attack under Article 51,[191] and the Aurora Generator Test provides an example of a cyber warfare operation resulting in physical damage. SCADA attacks could also result in death by, for example, shutting down power to a hospital or an Air Traffic Control tower.

Michael Schmitt, Dean and Professor of International Law at the George C. Marshall Center, has argued that an action can be defined as an armed attack if that action is intended to cause injury, death,

---

[185] Ted Bridis & Eileen Sullivan, *US Video Shows Hacker Hit on Power Grid*, SFGATE.COM (SAN. FRAN. CHRON.), Sept. 27, 2007, http://www.sfgate.com/cgibin/article.cgi?f=/n/a/2007/09/26/national/w165704D09.DTL&type=politics (last visited Sept. 14, 2009).
[186] *Id*.
[187] Tom Espiner, *CIA: Cyberattack Caused Multiple-City Blackout*, CNET NEWS.COM, Jan. 22, 2008, http://www.news.com/CIA-Cyberattack-caused-multiple-city-blackout/2100-7349_3-6227090.html?part=rss&tag=6227090&subj=news (last visited Sept. 9, 2009).
[188] *Id*.
[189] *Id*.
[190] *Id*.
[191] *See* Korns & Kastenberg, *supra* note 12, at 63.

damage or destruction, or such consequences are foreseeable.[192] While there is currently nothing affirming that a cyber attack equates to an unlawful use of force or armed attacked under international law, using Schmitt's analysis a cyber attack that has the potential to cause, or actually causes, physical damage, injury, or death would constitute a use of force or an armed attack. This potential consequences standard would prohibit most types of cyber warfare operations against SCADA systems, such as interfering with control elements of the power grid, air traffic control networks, or nuclear power plant safety systems, since this would cause or have the potential to cause physical damage, injury, or death. Adopting this set standard would assist nations in determining when it would be lawful to exercise their inherent right of self-defense under Article 51 of the U.N. Charter.

When responding to such an attack it is important to remember that nothing in Article 51 limits a nation's response to the method of attack utilized by the aggressor. The only limitation on exercising self-defense is that the defensive force must be necessary and proportionate to the armed attack that gave rise to the right. This limitation under customary international law was asserted by U.S. Secretary of State Daniel Webster, who in response to a British claim of self-defense in an incident known as the *Caroline Affair*, wrote that in order to be justified, the use of force in self-defense must be necessary and proportionate under the circumstances of the particular case.[193] This standard of necessary and proportionate was confirmed by the International Court of Justice in the *Nicaragua* case and in its *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*. In the *Nicaragua* case, the court found there was a well established rule in customary international law whereby self-defense would warrant only measures which were proportional to the armed attack and necessary to respond to it.[194] In its *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*, the Court stated, "the submission of the exercise of the right of self-defence to the conditions of necessity and proportionality is a rule of customary international law"[195] and "this dual condition applies equally to Article 51 of the Charter, whatever the means of force employed."[196] Therefore, a nation's response is not limited to a specific weapon or type of attack as long as the response is necessary and proportionate under the circumstances. This would

[192] TIKK ET. AL., *supra* note 173, at 20 (referencing Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, vol. 84, pt. 846 INT'L REV. OF THE RED CROSS 365 (Jun. 2002)).
[193] Michael C. Bonafede, *Here, There, and Everywhere: Assessing the Proportionality Doctrine and U.S. Use of Force in Response to Terrorism After September 11 Attacks*, 88 CORNELL L. REV. 155, 166 (2002).
[194] Military & Paramilitary Activities, *supra* note 153, ¶ 176.
[195] Legality of the Threat or Use of Nuclear Weapons, 1996 I.C.J. 226, ¶ 41.
[196] *Id*.

permit states to respond with precision bombings against known cyber warfare operation centers located within the territory of the nation that engaged in the unlawful cyber attack.

VII. CYBER WARFARE OPERATIONS AND THE LAW OF WAR

Cyber warfare operations are likely to be used in future armed conflicts. Because a state may use a cyber attack against an enemy in order to cause damage, it is indisputably a method of warfare.[197] Therefore, it is important to analyze the use of cyber warfare operations in relation to the law of war. The law of war, also referred to as the law of armed conflict, applies to a state of international armed conflict, and applies equally to all parties to the conflict. As with other areas of international law, the law of war consists of treaties and customary international law; the primary sources being the Hague Regulations, the Geneva Conventions, and the Additional Protocols to the Geneva Conventions. While the general principles of the law of war have been expressed numerous ways, this article will divide them into the following six categories: (1) military necessity, (2) distinction, (3) proportionality, (4) unnecessary suffering, (5) perfidy, and (6) neutrality. These principles provide the foundation of the law of war. This section will look at these principles, then proceed to a discussion on targeting, and conclude by addressing how potential types of cyber warfare operations during an armed conflict may be viewed in relation to the law of war.

A. General Principles of the Law of War

1. *Military Necessity*

The principle of military necessity justifies those measures not forbidden by international law which are indispensable for securing the complete submission of the enemy as soon as possible.[198] U.S. Army General Order No. 100, commonly referred to as the Lieber Code, originally codified this principle in 1863.[199] Article 52(2) of Additional Protocol I to the Geneva Conventions (Additional Protocol I) provides a definition of military objectives which many consider to reflect

---

[197] Dormann, *supra* note 13.
[198] *See* U.S. DEP'T OF ARMY, FIELD MANUAL 27-10**,** THE LAW ON LAND WARFARE para. 3(a) (July 18, 1956) [hereinafter FM 27-10]; *see also* Hague Convention IV, art. 23(g).
[199] Jefferson D. Reynolds, *Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground*, 56 A.F. L. REV. 1, 6 (2005).

customary international law.[200] It states that a military attack is lawful only against "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[201]

2. *Distinction*

According to an uncontroversial principle of customary international law, parties to an armed conflict must distinguish between the civilian population and combatants, and between civilian objects and military objectives.[202] Additional Protocol II to the Geneva Convention (Protocol II) applies in situations of internal armed conflict and also incorporates the principle of distinction. It states, "the civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations"[203] and also "the civilian population . . . as well as individual civilians, shall not be the object of attack."[204] Additional Protocol II provides that civilians shall enjoy these protections during internal armed conflicts "unless and for such time as they take a direct part in hostilities."[205]

3. *Proportionality*

The principle of proportionality prohibits the use of any kind or degree of force that exceeds that needed to accomplish the military objective.[206] Collateral damage incurred while attacking a military objective does not necessarily equate to a violation of international law, provided the collateral damage is proportional to the military advantage

---

[200] Marco Sassòli, Legitimate Target of Attacks, Under International Humanitarian Law 2 (background paper for Informal High-Level Expert Meeting on Reaff. & Dev. of Int'l Hum. Law, Cambridge, Jan. 27-29, 2003), *available at* http://www.ihlresearch.org/ihl/pdfs/Session1.pdf.

[201] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 52(2), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

[202] Sassòli, *supra* note 200, at 1. Additional Protocol I, Article 48, states this basic rule as, "the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." Additional Protocol I, art. 48.

[203] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), art. 13(1), June 8, 1977, 1125 U.N.T.S. 609, [hereinafter Additional Protocol II].

[204] Additional Protocol II, art. 13(2).

[205] *Id.* art. 13(3).

[206] Rod Powers, *Law of Armed Conflict*, ABOUT.COM: US MILITARY, at 2, http://usmilitary.about.com/cs/wars/a/loac.htm (last visited Sept. 9, 2009).

gained. The law of war requires one to weigh the expected collateral damage against the concrete and direct military advantage anticipated by the operation. The ultimate question under the principle of proportionality is whether the collateral damage is excessive in relation to the military advantage gained.

Additional Protocol I, Article 51(5)(b), provides that "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated"[207] shall be considered an indiscriminate attack. Additional Protocol I, Article 51(4), defines three types of indiscriminate attacks: (1) attacks that "are not directed against a specific military objective,"[208] (2) attacks that "employ a method or means of combat the effect of which cannot be directed at a specific military objective,"[209] and, (3) attacks that "employ a method or means of combat the effects of which cannot be limited as required by this Protocol."[210] Under Additional Protocol I, it is a grave breach to launch an attack knowing it will cause excessive collateral damage in relation to the military advantage gained.[211]

4. *Unnecessary Suffering*

Hague Convention IV, Article 22, provides that "the rights of belligerents to adopt means of injuring the enemy is not unlimited."[212] Hague Convention IV, Article 23(e), specifically prohibits the employment "of arms, projectiles, or material calculated to cause unnecessary suffering."[213] This principle prohibits the use of weapons calculated to cause unnecessary suffering and the use of otherwise lawful weapons if used in a manner that causes unnecessary suffering.

5. *Perfidy*

Treacherous or perfidious conduct in war is forbidden under the law of war because it destroys the basis for a restoration of peace short of the complete annihilation of one belligerent by the other.[214] Hague Convention IV, Article 23(b), states, "to kill or wound treacherously individuals belonging to the hostile nation or army," is forbidden.[215]

---

[207] Additional Protocol I, *supra* note 201, art. 51(5)(b).
[208] *Id*. art 51(4)(a).
[209] *Id*. art 51(4)(b).
[210] *Id*. art 51(4)(c).
[211] *See id*. art. 85(3)(b)(c).
[212] Hague Convention IV, art. 22.
[213] *Id*. art. 23(e).
[214] FM 27-10, *supra* note 198, ¶ 50.
[215] *Id*. art. 23(b).

Perfidy involves injuring the enemy by using his adherence to the law of war against him. Additional Protocol I, Article 37(1), also states, "it is prohibited to kill, injure or capture an adversary by resort to perfidy"[216] and "acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy."[217] Army Field Manual 27-10, *The Law of Land Warfare*, provides:

> The line of demarcation between legitimate ruses and forbidden acts of perfidy is sometimes indistinct, but the following examples indicate the correct principles. It would be an improper practice to secure an advantage of the enemy by deliberate lying or misleading conduct which involves a breach of faith, or when there is a moral obligation to speak the truth. For example, it is improper to feign surrender so as to secure an advantage over the opposing belligerent thereby. So similarly, to broadcast to the enemy that an armistice had been agreed upon when such is not the case would be treacherous. On the other hand, it is a perfectly proper ruse to summon a force to surrender on the ground that it is surrounded and thereby induce such surrender with a small force.[218]

Because cyber espionage is likely to become an important intelligence gathering tool, states will likely plant misinformation on their own networks to confuse or mislead the enemy. Such misinformation is synonymous with any other method for delivering misinformation.[219]

6. *Neutrality*

Neutrality is an essential tenet of international law.[220] Neutrality affords states the right to maintain relations with all belligerents.[221] States that declare themselves neutral, and behave

[216] Additional Protocol I, *supra* note 201, art. 37(1).
[217] *Id*. The following examples are provided: the feigning of an intent to negotiate under a flag of truce or of a surrender; the feigning of an incapacitation by wounds or sickness, the feigning of civilian, non-combatant status, and the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other States not Parties to the conflict.
[218] FM 27-10, *supra* note 198, ¶ 50.
[219] *See* Dormann, *supra* note 13.
[220] Korns & Kastenberg, *supra* note 12, at 73.
[221] *Id.* at 62.

accordingly, are entitled to immunity from attack.[222] Under the principle of neutrality a neutral state's territory is to be secure from assault or trespass.[223] Also, belligerents are forbidden from moving troops, munitions of war or supplies across the territory of a neutral state.[224] However, should the neutral state fail for any reason to prevent violations of its neutrality by the troops of one belligerent entering or passing through its territory, the other belligerent may be justified in attacking the enemy forces on this territory.[225] Authors in the cyber law arena have suggested that in order to remain neutral in a cyber conflict a state cannot originate a cyber attack, and it also has to take action to prevent a cyber attack from transiting its internet nodes.[226]

Neutrality becomes problematic for cyber warfare operations because the weapons of cyber warfare, such as requests being sent by computer systems from which DoS attacks originate or the malicious code that travels along networks, cannot always be predicted. For example, when one server goes down, internet traffic is automatically rerouted via another.[227] Additionally, a neutral state may not be able to prevent cyber warfare operations from leaving its jurisdiction unless it severs all connections with computer systems in other states. Placing such a duty on any and all neutral states is unreasonable and would likely grind the internet to a halt.[228]

B. Targeting

Military objectives are legitimate targets. Additional Protocol I, Article 52(2), defines military objectives as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offer a definite military advantage."[229] Objects which, by their nature, make an effective contribution to military action would include objects directly used by the armed force, such as: weapons, equipment, transports, fortifications, depots, buildings occupied by armed forces, staff

[222] *Id*.
[223] Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, art. 1, Oct. 18, 1907, 26 Stat. 2310, U.S.T. 540 (which states "the territory of neutral Powers is inviolable") [hereinafter Hague Convention V].
[224] *Id*. art. 2.
[225] FM 27-10 *supra* note 198, ¶ 520.
[226] Korns & Kastenberg, *supra* note 12, at 62; Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare,* 106 MICH. L. REV. 1444 (2008).
[227] *See* Davis Brown, *A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict,* 47 HARV. INT'L L.J. 179, 210 (2006).
[228] *Id*.
[229] Additional Protocol I, *supra* note 201, art. 52(2).

headquarters, and communication centers.[230] Location refers to objects that by their nature have no military function but by virtue of their location make an effective contribution to military action, such as a bridge.[231] Purpose is concerned with the intended future use of an object, while use is concerned with its present function.[232] Most civilian objects can become useful objects to the armed forces; for example, a school or a hotel is a civilian object, but if used to accommodate troops or headquarters staff, it becomes a military objective.[233] If there is a doubt concerning the purpose, such place must be presumed to serve civilian purposes.[234]

Next, review the phrase "definite military advantage." This phrase makes it illegitimate to launch an attack which only offers potential or indeterminate advantages.[235] Now that we have defined the phrase "military objectives," the next step is to examine specific types of targets, specifically, people, places, and dual-use targets.

1. *Targeting People*

People can be divided into two categories: combatants and non-combatants. Combatants are members of the armed forces of a state party to a conflict, other than medical personnel and chaplains.[236] These individuals have the right to participate directly in hostilities.[237] Combatants "consist of all organized armed forces, groups and units which are under a command responsible to that state for the conduct of its subordinates."[238] Combatants are required to "distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack."[239] Combatants also consist of "members of militias and volunteer corps, including those of organized resistance movements, belonging to a state, party to the conflict, provided that such militias or volunteer corps, including such organized resistance movements" meet specific requirements.[240]

---

[230] Commentary on the Additional Protocols of 8 June, 1977 to the Geneva Conventions of 12 August 1949, art. 43, ¶ 2020 (Yves Sandoz, Christophe Swinarski, Bruno Zimmermann eds., 1987), *available at* http://www.icrc.org/ihl.nsf/COM/470-750067?OpenDocument.
[231] *Id.* art. 43, ¶ 2021.
[232] *Id.* art. 43, ¶ 2022.
[233] *Id*.
[234] *Id*.
[235] *Id.* art. 43, ¶ 2024.
[236] Additional Protocol I, *supra* note 201, art. 43(2).
[237] *Id*.
[238] *Id.* art. 43(1).
[239] *Id.* art. 44(3).
[240] Convention relative to the Treatment of Prisoners of War (III), art. 4(A)(2), Aug. 12, 1949, 20 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]. These requirements include "being commanded by a person responsible for his subordinates;"

Unlike combatants, the law of war prohibits direct attacks on non-combatants. Non-combatants may be divided into two groups: civilians and enemy personnel out of combat. A civilian is a person who is not a member of the armed forces of a party to the conflict and who does not take a direct part in hostilities.[241] The general rule regarding civilians is that the civilian population, as well as individual civilians, shall not be the object of attack.[242] Additionally, acts or threats of violence, the primary purpose of which is to spread terror among the civilian population, are prohibited.[243] Civilians enjoy protection from targeting "unless and for such time as they take a direct part in hostilities."[244] The major categories of individuals considered to be personnel out of combat are prisoners of war, the wounded and sick, medical personnel, and chaplains.

2. *Targeting Places*

Hague Convention IV, Article 25, prohibits the attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings that are undefended.[245] Additional Protocol I, Article 52, provides that "civilian objects, which consist of all objects that are not military objectives, shall not be the object of attack . . . ."[246] Moreover, "in case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used."[247] Additional Protocol 1, Article 56, states: "Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."[248] This

---

wear a "fixed distinctive sign recognizable at a distance;" "carrying arms openly;" and conduct their operations "in accordance with the laws and customs of war." *Id.*

[241] Additional Protocol I, *supra* note 201, art. 50(1).

[242] *Id.* art. 51(2).

[243] *Id*.

[244] *Id.* art. 51(3).

[245] Hague Convention IV, art. 25.

[246] Additional Protocol I, *supra* note 201, art. 52(1).

[247] *Id.* art. 52(3).

[248] *Id*. art. 56(1); *see also* Additional Protocol I, *supra* note 201, art. 56(2) (provides that this special protection against attack shall cease: for a dam or a dyke only if it is used for other than its normal function and in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support; for a nuclear electrical generating station only if it provides electric power in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support; for other military objectives located at or in the vicinity of these works or installations only if they are used in regular, significant and

protection terminates, however, if the enemy is using them in specific ways to support its war effort.[249]

Moreover, "other military objectives located at or in the vicinity of these works or installations shall not be made the object of attack if such attack may cause the release of dangerous forces from the works or installations and consequent severe losses among the civilian population."[250] It needs to be noted that the U.S. has not ratified Additional Protocol I and specifically objects, for military reasons, to Article 56.[251] The objection is that this Article disregards the longstanding principle of proportionality and prohibits the attack if there are to be "severe" civilian losses, no matter how important the target may be from a military point of view.[252]

3. *Dual-Use Targets*

Dual-use targets are most commonly defined as those targets that are used for both military and civilian purposes, such as power plants that provide electricity to both civilian institutions as well as military command and control centers.[253] Civilian objects that may fall into this dual-use category would include computer networks of certain research facilities, air traffic control networks that regulate both civilian and military aircraft, computerized civilian logistics systems upon which military supplies will be moved, electronic power grid control networks, communications nodes and systems, including satellite and other space-based systems, railroad and other transportation systems, civilian government networks, and oil and gas distribution systems.[254]

As previously discussed, Additional Protocol I, Article 52(2), essentially provides two requirements for an object to qualify as a military objective. First, the target must make an effective contribution to the enemy's military action. Second, its destruction must provide a definite military advantage to the attacker.[255] The use of the phrase "make an effective contribution" does not limit targets to only military

---

direct support of military operations and if such attack is the only feasible way to terminate such support).

[249] *Id*.

[250] *Id.* art. 56(1).

[251] *See* Howard S. Levie, *The 1977 Protocol I and the United States,* 38 ST. LOUIS U. L.J. 469, 482 (1993).

[252] *Id*.

[253] Major Jeanne M. Meyer, *Tearing Down the Facade: A Critical Look at the Current Law on Targeting the Will of the Enemy and Air force Doctrine,* 51 A.F. L. REV. 143, 178 (2001).

[254] *See* Eric T. Jensen, *Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations?,* 18 AM. U. INT'L L. REV. 1145, 1160 (2003) (citing Michael N. Schmitt, *Ethics and Military Force: The Jus in Bello, Address Before the Carnegie Council on Ethics and International Affairs* (Jan. 2002)).

[255] Additional Protocol I, *supra* note 201, art. 52(2).

objects but to objects that make an effective contribution to the military. However, just as with a non dual-use object, a proportionality test must be performed to ensure the collateral damage to civilians or civilian objects is not excessive in relation to the concrete and direct military advantage anticipated" [256] A 2003 Human Rights Watch briefing paper on international humanitarian law summarized the concept of dual-use object as follows:

> Dual-use objects serve the needs of the civilian population and are also used by military forces. A dual-use object may presumptively be a legitimate military target because it contributes, in part, to concrete military aims, yet the harm to the civilian population in its destruction may still be disproportionate to the military advantage gained, rendering an attack impermissible.[257]

The international community accepts the right of states to target dual-use targets. For example, the Eritrea-Ethiopia Claims Commission determined that Additional Protocol I, Article 52(2), is customary international law.[258] The Commission, ruling on the aerial bombardment of the Hirgigo power station, stated, "a large power plant being constructed to provide power for an area including a major port and naval facility certainly would seem to be an object the destruction of which would offer a distinct military advantage."[259] The Commission ultimately found that Ethiopia's aerial bombardment of the power station was not unlawful.[260] However, many situations exist where targeting dual-use targets through cyber warfare operations would be unlawful; such as when targeting civilian morale is the main objective and destroying a legitimate military objective is secondary. For example, shutting down an entire communication network within a large city that has only a small military presence or disabling television transmissions in order to prevent the showing of military recruitment advertisements would be unlawful dual-use targeting.

---

[256] *Id.* art. 51(5)(b).
[257] Human Rights Watch Briefing Paper, *International Humanitarian Law Issues In A Potential War In Iraq* (2003), *available at* http://www.hrw.org/backgrounder/arms/iraq0202003.htm#5.
[258] Eritrea Ethiopia Claims Commission, *Partial Award, Western Front, Aerial Bombardment and Related Claims, Eritrea's Claims 1, 3, 5, 9-13, 14, 21, 25 & 26* 33 (Dec. 19, 2005), *available at* http://www.pca-cpa.org/upload/files/FINAL%20ER%20FRONT%20CLAIMS.pdf.
[259] *Id.* at 35.
[260] *Id.*

C. Analysis

Cyber warfare operations have the capability of being a very effective option during an armed conflict. Some obvious benefits include less physical destruction, less cost than other types of traditional warfare, and the ability to still achieve the same results with less risk to military personnel. An example of this would be a cyber warfare operation against another state's air defense networks to render them temporarily or permanently inoperable. At present, the weapon most often associated with the suppression of enemy air defenses, or SEAD, is the anti-radiation missile delivered by tactical fighters.[261] However, a SEAD weapon could be anything that damages or destroys a component of an air defense system.[262] Using a cyber warfare operation to accomplish this, rather than an airstrike, is a good example of satisfying Additional Protocol I, Article 57, which states, "when a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be the attack on which may be expected to cause the least danger to civilian lives and to civilian objects."[263] This example demonstrates the non-physical destruction aspect of cyber warfare operations, which in many cases will reduce the expected collateral damage to civilians and civilian property.

When analyzing the lawfulness of a cyber warfare operation one should conduct the same analysis as when determining the lawfulness of an aircraft targeting a military objective. For example, a DoS attack against enemy command and control servers could overwhelm the servers and prevent leadership from operating at their highest level. This example would appear lawful under the laws of war as the command and control servers are a lawful military objective. Furthermore, the resulting collateral damage would be limited to mere inconvenience for civilians using the shared network. Additionally, if the attacker only targets military command and control servers, one may argue that civilians on the system are taking a direct part in hostilities anyway. This operation may limit the need for traditional means and methods of warfare to impact command and control operations, such as directly targeting the structures housing the servers or the power sources to the servers through air or land attacks. This analysis also applies to cyber warfare operations that target the email accounts of military personnel and government leaders, or the telephone servers and routers servicing the same individuals. This disruption of useful electronic information exchange would also limit the collateral damage compared

[261] Wikipedia.org, SEAD, http://en.wikipedia.org/wiki/SEAD (last visited Sep. 9, 2009).
[262] *Id*.
[263] Additional Protocol I, *supra* note 201, art. 57(3).

to a conventional attack intended to accomplish the same results, and would therefore be lawful.

A more difficult example to analyze is the altering of electronic maintenance manuals of an adversary's aircraft stored on a network. While the targeting of enemy aircraft is a proper military objective, a complete analysis must consider the intent of the attack. If the operation is designed to make the aircraft inoperable, at least temporarily, then it would appear to be lawful. However, if the intent is to have the aircraft malfunction in flight, further analysis must be accomplished. Specifically, it is necessary to weigh the anticipated collateral damage against the concrete and direct military advantage gained by the operation. In this example, the military advantage gained is the anticipated loss of an adversary's aircraft and possibly the pilot. The anticipated collateral damage depends on when the malfunction occurs. Under traditional methods of attack against enemy aircraft, such as by anti-aircraft artillery or engagement by another aircraft, it is possible to attempt to minimize collateral damage by limiting the place of attacks. However, deliberately causing an aircraft to malfunction by altering maintenance manuals may result in an aircraft's malfunctioning over a highly populated area. This may, or may not, make the operation unlawful.

Alteration of electronic maintenance manuals may be a proper ruse because it aims to mislead an adversary or to induce him to act recklessly but does not infringe on any rules of international law applicable in armed conflict or invite the confidence of an adversary with respect to protection under the law. An additional goal of this type of ruse may be to cause the enemy forces to distrust electronic information, adding extra time to accomplish their tasks by resorting to the use of non-electronic methods. However, not all alterations of electronic information will qualify as a lawful ruse. For example, distributing fake orders from leaders may be found unlawful if it causes personnel to believe there is a truce or that they cannot target a particular area because it is a protected site. This would be similar to misusing a protected symbol such as a white flag or a red cross. Additionally, altering an adversary's medical records may be seen as violating the principle of unnecessary suffering if the individual is provided improper care. Moreover, the altering of medical records may also be seen as attacking a medical facility and therefore unlawful.

Cyber warfare operations that cause permanent damage may include deleting military files and inserting malicious code in military communication networks.[264] Deleting military files, or even the

[264] A network is defined as a group of two or more computer systems linked together. *See* Webopedia.com, network, http://www.webopedia.com/TERM/n/network.html (last visited Sep. 9, 2009).

annihilation of military computer networks, would constitute a proper military objective. These types of cyber warfare operations would result in the same outcome as using precision guided missiles to target specific military buildings without the resulting collateral damage to infrastructure. With proper intelligence gathering and operational planning, the attacker could avoid networks dedicated solely to medical facilities; otherwise, the attacks may be deemed to be indiscriminate.

Cyber warfare operations targeting local internet service or telecommunication providers may result in less collateral damage to the civilian population or civilian population surrounding the targeted object and, as a consequence, create more opportunities for targeting dual-use objects. In this example the military advantage to be gained is the disruption in the enemy's ability to communicate effectively. The collateral damage to civilians and civilian objects is the disruption in their ability to communicate effectively and potiential economic loss for local communication providers. When the military advantage gained is compared to the collateral damage one can logically label this an appropriate targeting of a dual-use object. The Commission in the Eritrea-Ethiopia noted, "the infliction of economic losses from attacks against military objectives is a lawful means of achieving a definite military advantage."[265]

VIII. OTHER TREATIES AND CONVENTIONS THAT MAY IMPACT CYBER WARFARE OPERATIONS

The law of state responsibility deals with the circumstances under which a state is responsible for an internationally wrongful act and the consequences of that responsibility.[266] This law of state responsibility is considered customary international law.[267] The breach of a treaty constitutes an internationally wrongful act.[268] Therefore, it is important that states are familiar with particular international obligations that may impact cyber warfare operations. This section will examine a few areas states should consider when developing plans for cyber warfare operations.

[265] Eritrea Ethiopia Claims Commission, *supra* note 258, at 35.
[266] Murphy, *supra* note 148, at 125.
[267] *Id*.
[268] *Id*.

A. International Outer Space Law

The Committee on the Peaceful Uses of Outer Space (COPUOS) was created by the U.N. in 1959.[269] The purpose of COPUOS is to review the scope of international cooperation in peaceful uses of outer space, to devise U.N. programs in this field, to encourage continued research and the dissemination of information on outer space matters, and to study legal problems arising from the exploration of outer space.[270] COPUOS is the only international forum for the development of international space law. Since its inception, the Committee concluded five international legal instruments and five sets of legal principles governing space-related activities.[271] The five international treaties are: the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty),[272] the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (Rescue Agreement),[273] the Convention on International Liability for Damage Caused by Space Objects (Liability Convention),[274] the Convention on Registration of Objects Launched into Outer Space (Registration Convention),[275] and the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (Moon Treaty).[276] The Outer Space Treaty and the Liability Convention both include language that may impact cyber warfare operations.

[269] G.A. Res. 1472 (XIV), *International co-operation in the peaceful uses of outer space* **(**Dec. 12, 1959), *available at* http://www.unoosa.org/oosa/SpaceLaw/gares/html/gares_14_1472.html.

[270] *See* United Nations Committee on the Peaceful Uses of Outer Space, http://www.unoosa.org/oosa/COPUOS/copuos.html (last visited Sep 9, 2009).

[271] United Nations Office for Outer Space Affairs (UNOOSA), *United Nations Treaties and Principles on Space Law*, http://www.unoosa.org/oosa/SpaceLaw/treaties.html (last visited Sep. 9, 2009).

[272] G.A. Res. 2222 (XXI), annex, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* (Oct. 10, 1967) [hereinafter Outer Space Treaty].

[273] G.A. Res. 2345 (XXII), annex, *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space* (3 Dec. 1968).

[274] G.A. Res. 2777 (XXVI), annex, *Convention on International Liability for Damage Caused by Space Objects* ((Sep. 1, 1972) [hereinafter Liability Convention].

[275] G.A. Res. 3235 (XXIX), annex, *Convention on Registration of Objects Launched into Outer Space* (Sep. 15, 1976).

[276] G.A. Res. 34/68, annex, *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies* (July 11, 1984).

1. *Outer Space Treaty*

The Outer Space Treaty furnishes a general legal basis for the peaceful uses of outer space and provides a framework for the developing law of outer space.[277] While, peaceful use is not defined in outer space law, some states consistently maintain the view that peaceful means non-military.[278] However, the majority of the international community generally accepts non-aggressive military uses as peaceful.[279] The U.S. maintains this view and stresses that all states possess the inherent right to defend against foreign aggression in outer space, as well as within earth's atmosphere.[280] Despite the debate over the peaceful use of outer space, its meaning has been well settled through the practice of states and it certainly includes some military activities.[281]

Article IX of the Outer Space Treaty relates to a state's duty to engage in international consultations prior to engaging in activities which the state "has reason to believe . . . would cause potentially harmful interference with activities of other States Parties in the peaceful exploration and use of outer space . . . ."[282] The wording of this Article only protects assets used for peaceful purposes, so by exclusion it may permit potentially harmful interference performed through cyber warfare operations targeting space assets, such as satellites of other States, if the targeted assets are not used for a peaceful purpose. Therefore, the targeting of a military satellite supporting the enemy's war fighting capability during hostilities would be permissible. Hence, a state may conduct a cyber warfare operation that hacks into an adversary's satellite's network and installs malicious code that causes the satellite to shut down or malfunction, or hijack control of an adversary's satellite. In these situations no international consultation would be necessary. However, the state's treaty obligations would remain in effect in regards to neutral parties. Therefore, to the extent that a cyber warfare operation in space could harmfully interfere with a non-belligerent state's asset, it would appear Article IX would require consultation with the neutral state.[283] Nevertheless, nothing in Article IX impedes carrying through with such an operation once consultations have occurred, even if the third-party state objects to the anticipated activity.[284]

---

[277] UNITED NATIONS TREATIES AND PRINCIPLES ON OUTER SPACE foreword (2002).
[278] *See* Major Robert A. Ramey, *Armed Conflict on the Final Frontier: The Law of War in Space*, 48 A.F. L. REV. 1, 79 (2000).
[279] *Id*.
[280] *Id*.
[281] *Id*.
[282] *Id.* at 77; Outer Space Treaty, *supra* note 272, art. IX.
[283] *Id*.
[284] *Id*.

Space assets also create dual-use issues, specifically regarding commercial assets. For example, remote sensing, weather and telecommunications satellites are functionally equivalent to military reconnaissance satellites. A military may use such a satellite to support the prosecution of its wartime objectives while at the same time the satellite is being used for non-military purposes.[285] Indeed, commercial entities provide about 60 percent of the satellite communications used by the U.S. military .[286] As discussed earlier, the test to determine the lawfulness of an attack against a military objective is whether the expected incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof clearly exceeds the concrete and direct military advantage anticipated.[287] On this basis, the United States lawfully destroyed major infrastructure targets during the 1991 Persian Gulf War that provided electricity both to the civilian populations and to the command and control functions of the Iraqi military.[288] A similar rationale applies to dual-use satellites. To the extent a satellite is used for the support of a military purpose, such as communications, weather, early warning of missile launch, or reconnaissance, it becomes a military objective and is lawfully subject to attack.[289]

To conclude, the Outer Space Treaty essentially prohibits potentially harmful interference with activities of other states in the peaceful exploration and use of outer space, and prohibits the use of force in outer space. However, if a state uses a space asset in a non-peaceful manner, then it should be considered a proper target for cyber warfare operations, although if such interference impacts a neutral state's peaceful exploration and use of outer space, a consultation may be required.

2. *Liability Convention*

The Liability Convention establishes procedures for determining state liability for activities in outer space. The Convention makes a launching state absolutely liable for damage caused by its space object on the surface of the Earth or to aircraft in flight.[290] In the event of damage being caused elsewhere, liability attaches only if the damage

[285] *Id*. at 148-149.
[286] Elizabeth Waldrop, *Integration of Military and Civilian Space Assets: Legal and National Security Implications*, 55 A.F. L. REV. 157, 200 (2004) (citing Katie McConnell, *Military Satellite Communications: The March Toward Commercialization*, DEFENSE DAILY (2003)).
[287] *See* Additional Protocol I, *supra* note 201, art. 51(5)(b).
[288] Ramey, *supra* note 278, at 150.
[289] *Id*.
[290] Liability Convention, *supra* note 274, art. II.

is the state's fault or the fault of persons for whom it is responsible.[291] The Convention provides exoneration from absolute liability to the extent that a launching state establishes the damage resulted either wholly or partially from gross negligence or from an act or omission done with intent to cause damage on the part of a claimant state.[292] However, no exoneration will be granted in cases where the damage has resulted from activities conducted by a launching state which are not in conformity with international law.[293]

Therefore, a state conducting cyber warfare operations against another state's satellite may be liable to the launching state for the damage done to the satellite and by the satellite, as a result of operations against it. For example, an operation that simply rendered a satellite useless may leave the state that conducted the cyber warfare operation liable for the value of the satellite. Whereas, an operation which de-orbited a satellite, causing it to fall back to earth, may leave the state liable for the resulting damage as well.[294]

The Liability Convention does not provide a military exception excusing a state from liability during an armed conflict. However, one may argue that under the law of war, a state has no duty to pay for damage done to lawful targets.[295]

B. International Telecommunications Law

Cyber warfare operations involving the targeting of telecommunication networks may implicate the International Telecommunication Union (ITU)[296] and its underlying charter, the International Telecommunication Convention (ITC),[297] as the ITC contains several provisions which may apply to cyber warfare operations. For example, Article 35 of the ITC prohibits harmful interference with the radio spectrum.

> All stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members or of recognized

[291] *Id.* art. III.
[292] *Id.* art. VI(1).
[293] *Id.* art. VI(2).
[294] *See, e.g.*, Wingfield, *supra* note 18, at 327-328.
[295] *See, e.g.*, *id*.
[296] *See* International Telectommunication Union, About ITU, http://www.itu.int/net/about/index.aspx (last visited Sept. 14, 2009). The International Telecommunication Union (ITU) is the UN specialized agency responsible for promoting international cooperation in the field of telecommunication.
[297] International Telecommunications Convention, Nairobi, Nov. 6, 1982, 32 U.S.T. 3821 [hereinafter ITU Convention].

> private operating agencies, or of other duly authorized operating agencies which carry on radio service, and which operate in accordance with the provisions of the Radio Regulations.[298]

Harmful interference is defined as "interference which endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with the Radio Regulations."[299]

Article 37 of the ITC may also impact cyber warfare operations. It requires members to prevent the transmission of false or deceptive distress, urgency, safety or identification signals, and to collaborate in locating and identifying stations transmitting such signals from their own country.[300] Other articles of the ITC worth noting include Article 19(2), which permits members to cut off private telecommunications that may appear dangerous to the security of the State or contrary to its laws, to public order or to decency[301] and Article 20, which permits members to suspend the international telecommunication service for an indefinite time, either generally or only for certain relations or for certain kinds of correspondence, outgoing, incoming or in transit.[302]

Article 38 addresses military radio stations and provides that "members retain their entire freedom with regard to military radio installations."[303] This article further notes that "these installations must, so far as possible, observe statutory provisions relative to giving assistance in case of distress and to the measures to be taken to prevent harmful interference, and the provisions of the Administrative Regulations concerning the types of emission and the frequencies to be used . . . ."[304] Radio Regulations coordinate and standardize the operation of telecommunication networks and services.[305] An example of a Radio Regulation potentially impacting cyber warfare operations is Regulation Article 18, which provides that states may not carry out the transmission of false or misleading signals.[306] This prohibition does not

---

[298] *Id*. art. 35
[299] *Id*. annex 2.
[300] *Id*. art. 37.
[301] *Id*. art. 19(2).
[302] *Id*. art. 20.
[303] *Id*. art. 38(1).
[304] *Id*. art. 38(2).
[305] Wikipedia.org, *Radio Regulations*, http://en.wikipedia.org/wiki/Radio_Regulations (last visited Sep. 9, 2009).
[306] *See* LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN, KEVIN J. SOO HOO, INFORMATION WARFARE AND INTERNATIONAL LAW 41 n.41 (1998) (citing Howard A. Bender, *The Case of the Sarah: A Testing Ground for the Regulation of Radio Piracy in the United States*, 12 FORDHAM INT'L L.J. 67, 69 (1988)).

apply to the truth or falsehood of the underlying substance of a transmission, but to the identification of its transmitter and frequency.[307]

To conclude, cyber warfare operations to disrupt private communications fitting within the exemption in Article 19(2) or to suspend international telecommunications are not prohibited. Additionally, the ITC does not specify the source or destination of the offending communications that may be cut off or suspended. Therefore, one may conclude it would be lawful to cut off or suspend communications completely within a foreign country or between locations in two foreign countries in certain circumstances, without the need for hostilities. However, cyber warfare operations that result in transmitting false or deceptive distress, urgency, safety or identification signals are unlawful, as is falsifying the identification of a transmitter and frequency. As a result, while a state may, under certain circumstances, block or suspend international communications, it may not lawfully spoof communications. However, there is ample precedent that provisions of international communication conventions are suspended between belligerents engaged in armed conflicts.[308]

C. International Aviation Law

Cyber warfare operations involving the targeting of, or interference with, civilian aviation may implicate numerous international aviation laws. Such operations may involve disrupting an air traffic control tower, modifying a flight's passenger list, or adding a name to a no-fly list. These types of operations have the potential to result in a delay or cancellation of flights, thereby interrupting travel plans of targeted belligerents.

1. *The Convention on International Civil Aviation*

The primary international law governing aviation is the Convention on International Civil Aviation, also known as the Chicago Convention.[309] This Convention established the International Civil Aviation Organization (ICAO), a specialized agency of the United Nations charged with coordinating and regulating international air travel. The Convention establishes rules of airspace, aircraft

---

[307] *Id*.

[308] *See* Dep't of Defense General Counsel, *An Assessment of International Legal Issues in Information Operations* 33 (May 1999), *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.

[309] Convention on International Civil Aviation, Chicago, Dec. 7, 1944, 15 U.N.T.S. 295, [hereinafter Chicago Convention].

registration, and safety.[310] The Convention is supported by eighteen annexes containing standards and recommended practices; these annexes are amended regularly by ICAO.[311] Annex 17 sets out the basis for the ICAO civil aviation security program and seeks to safeguard civil aviation and its facilities against acts of unlawful interference.[312] This Annex requires that each member state "have as its primary objective the safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation."[313]

A 1998 amendment to the Chicago Convention prohibits the use of weapons against civil aircraft.[314] Article 3 bis(a) specifically states that "the contracting States recognize that every State must refrain from resorting to the use of weapons against civil aircraft in flight . . . ."[315] Article 89 of the Chicago Convention allows a contracting state to disregard its obligations under the Convention in times of war or national emergency.

> [I]n case of war, the provisions of this Convention shall not affect the freedom of action of any of the contracting States affected, whether as belligerents or as neutrals. The same principle shall apply in the case of any contracting State which declares a state of national emergency and notifies the fact to the Council.[316]

Cyber warfare operations targeting civilian aviation may run afoul of a state's obligation under the Chicago Convention to safeguard against acts of unlawful interference with civil aviation. Additionally, if a cyber warfare operation targets an aircraft in flight, the operation very well may be a violation of the Article 3bis requirement to refrain from resorting to the use of weapons against civil aircraft in flight. However,

---

[310] Wikipedia.org, Convention on International Civil Aviation, http://en.wikipedia.org/wiki/Convention_on_International_Civil_Aviation (last visited Sep. 9, 2009).
[311] *Id*.
[312] *See* International Civil Aviation Organization, ANNEXES TO THE CONVENTION ON INTERNATIONAL CIVIL AVIATION Annex 17, *available at* http://www.icao.int/eshop/pub/anx_info/an17_info_en.pdf.
[313] Paul Stephen Dempsey, *Aviation Security: The Role of Law in the War Against Terrorism*, 41 COLUM. J. TRANSNAT'L L 649, 678 (2003); Chicago Convention, *supra* note 309, at Annex 17, para 2.1.1.
[314] Robin Geibeta, *Civil Aircraft as Weapons of Large-scale Destruction: Countermeasures, Article 3bis of the Chicago Convention, and the Newly Adopted German "Luftsicherheitsgesetz*, 27 MICH. J. INT'L L. 227, 228 (2005).
[315] International Civil Aviation Organization, *Amendment of Convention on International Civil Aviation with Regard to Interception of Civil Aircraft* art. 3bis(a), ICAO Doc. 9437, A25-Res. (May 10, 1984) (reprinted in 23 INT'L LEG. MATERIAL 705 (1984)).
[316] Chicago Convention, *supra* note 309, art. 89.

the Chicago Convention is unique in the fact that it specifically acknowledges that a state may lawfully disregard its obligations under the Convention in times of war or national emergency. This national emergency exception may provide some latitude in conducting cyber warfare operations in situations short of war.

2. *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*

The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, commonly referred to as the Montreal Convention of 1971, makes specific conduct unlawful.[317] Article 1 provides that a person commits an offense if he unlawfully and intentionally does or attempts to do any of the following:

> [1] performs an act of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft;[318] [2] destroys an aircraft in service or causes damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight;[319] [3] places or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight;[320] [4] destroys or damages air navigation facilities or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight;[321]or, [5] communicates information known to be false, thereby endangering the safety of an aircraft in flight.[322]

This Convention may limit the ability to conduct cyber warfare operations that interfere with an aircraft's operating system, if such an operation would render the aircraft incapable of flight. Additionally, this Convention may also place a prohibition on interfering with the networks of air navigation facilities, as it essentially prohibits the ability to disrupt air traffic control communications or other aspects of air

[317] Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, Sept, 23, 1971, 24 U.S.T. 564 [hereinafter Montreal Convention].
[318] *Id.* art. 1(1)(a).
[319] *Id.* art. 1(1)(b).
[320] *Id.* art. 1(1)(c).
[321] *Id.* art. 1(1)(d).
[322] *Id.* art. 1(1)(e).

navigation, if it interferes with their operation and endangers the safety of an aircraft in flight. Finally, this Convention may prohibit cyber warfare operations from spoofing communication if it would endanger the safety of an aircraft. However, nothing in this Convention appears to limit cyber warfare operations that do not render a flight unable to fly or endanger the safety of an aircraft in flight.

3. *Protocol for the Suppression of Unlawful Acts of Violence at Airports serving International Civil Aviation*

The Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation[323] supplemented and extended the legal framework of the Montreal Convention of 1971 to encompass unlawful acts of violence committed at airports serving international civil aviation, even where such acts do not endanger the safety of aircraft in flight. Article II sets forth the offenses covered by the Protocol. It states that any person commits an offense if he unlawfully and intentionally, using any device, substance, or weapon "performs an act of violence against a person at an airport serving international civil aviation which causes or is likely to cause serious injury or death"[324] or "destroys or seriously damages the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupts the services of the airport, if such an act endangers or is likely to endanger safety at that airport."[325] This Protocol has the potential to prohibit any cyber warfare operation that may impact service at an international airport, such as entering an airport's computer network system and altering the passenger manifests or placing an individual on a no-fly list. To be unlawful, however, the cyber warfare operation would have to endanger the safety of those at the airport.

D. Arms Control Treaties

Arms control treaties frequently contain prohibitions on interference and concealment in evading national technical means of verification.[326] For example, the 1972 Limitation of Strategic Offensive Arms Interim Agreement between the United States and the Soviet Union provided that "each Party undertakes not to interfere with the national technical means of verification of the other Party operating in

[323] Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Feb. 24, 1988, 1589 U.N.T.S. 474 [hereinafter Montreal Protocol].
[324] *Id*. art. II, para 1..
[325] *Id*.
[326] Wingfield, *supra* note 18, at 330.

accordance with paragraph 1 of this Article."[327] This agreement also provided that "each Party undertakes not to use deliberate concealment measures which impede verification by national technical means of compliance with the provisions of this Interim Agreement."[328] This became standard language in arms control treaties between the United States and the Soviet Union as evidenced by the language in Article XV of the 1979 Treaty on the Limitation of Strategic Offensive Arms and Protocol Thereto (SALT II), which states that "paragraphs 1 and 2 of this Article are adopted verbatim from the first two paragraphs of Article XII of the ABM Treaty and Article V of the Interim Agreement."[329] The third paragraph of this Article prohibits deliberate concealment measures which impede verification by national technical means of compliance with the Treaty.[330]

Arms control treaties that place a prohibition on interfering with the national technical means of a state may limit the ability of both states to conduct cyber warfare operations against the intelligence collecting capabilities of the other. However, arms control treaties, like other treaties except those defining laws of war, are suspended during war between parties.[331] Therefore, cyber warfare operations that interfere with military reconnaissance satellites used for arms control verification may violate the treaty. However, during hostilities these satellites would become a proper military objective.

E. Council of Europe Convention on Cybercrime

The Council of Europe's Convention on Cybercrime is the first international treaty on crimes committed via the internet and other computer networks.[332] The main objective of the Convention is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.[333] The U.S. ratified the Cybercrime

---

[327] Interim Agreement between the United States of America and the Union Of Soviet Socialist Republics on Certain Measures with Respect to the Limitation of Strategic Offensive Arms (SALT I Agreement), art. V(2), U.S.-U.S.S.R., May 26, 1972, 23 U.S.T. 3462. National technical means of verification include national-level strategic platforms, primarily specialized in aircraft and satellites. *See* Wingfield, *supra* note 18, at 330.

[328] *Id.* art. V(3).

[329] Treaty on the Limitation of Strategic Offensive Arms and Protocol Thereto (SALT II) art. XV, U.S.-U.S.S.R., June 19, 1979, S. Exec. Doc. Y, 96-1 [hereinafter SALT II].

[330] *Id.* art. XV(3).

[331] *See* U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, ANTI-SATELLITE WEAPONS, COUNTERMEASURES, AND ARMS CONTROL 76 (1985).

[332] Council of Europe, *Summary of the Convention on Cybercrime*, http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm (last visited Sep. 10, 2009).

[333] *Id.*

Convention in 2006. [334] This Convention covers a broad range of criminal conduct broken up into four categories: offenses against the confidentiality, integrity, and availability of computer data and systems;[335] computer-related offenses;[336] content-related offenses;[337] and offenses related to infringements of copyright and related rights.[338]

Cyber Warfare Operations would most likely run afoul of the offenses described within the first category, in particular Articles 2 through 5, which relate to illegal access, illegal interception, data interference, and system interference, respectively.[339] However, its rules do not apply to government activities, whether for law enforcement or national security purposes.[340] For example, Article 2 requires states to adopt "legislative and other measures" to establish as criminal offenses under their domestic law intentional "access to the whole or any part of a computer system without right."[341] The accompanying Explanatory Report clarifies that the "without right" caveat "leaves unaffected conduct undertaken pursuant to lawful government authority," including acts to "protect national security or investigate criminal offences."[342] Nevertheless, this Convention still poses potential problems for conducting cyber warfare operations. For example, parties to the Convention have agreed to, among other things, "co-operate with each other . . . to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[343] This may create issues for a signatory state that wishes to conduct cyber warfare operations against another signatory state. For example, if particular actions such as breaching security measures or intercepting electronic messages of a signatory state are traced back to the state conducting the cyber warfare operations, then that state's duty to assist is not plausible if it is denying liability for the attacks.

---

[334] Rasha AlMahroos, *Privacy on the Internet and in Organizational Database: Phishing for the Answer: Recent Developments in Combating Phishing*, 3 ISJLP 595, 613 (2008).
[335] Council of Europe, Convention on Cybercrime, arts. 2-6, Nov. 23, 2001, E.T.S. No. 185 [hereinafter Cybercrime Convention].
[336] *Id.* arts. 7-8.
[337] *Id.* art. 9.
[338] *Id.* art. 10.
[339] *Id.* arts. 2-5.
[340] Duncan B. Hollis, *Crimes, War Crimes, and the War on Terror Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1052 (2007).
[341] *Id.* at 1052 n.124; Cybercrime Convention, *supra* note 335, art. 2.
[342] Hollis, supra note 339, at 1052 n.124 (citing Council of Europe, Convention on Cybercrime**,** Explanatory Report, C.E.T.S. No. 185, P 38 (Nov. 8, 2001)).
[343] Cybercrime Convention, *supra* note 335, art. 23.

IX. CONCLUSION

Nothing in international law explicitly prohibits cyber warfare operations. However, legal limitations surely exist with regard to their application. Also, cyber warfare operations have the potential of constituting a use of force or a violation under the law of war.

Cyber warfare operations offer a variety of methods to impact an adversary's ability to conduct war. They may enable a state to infiltrate an adversary's network, acquire files, spread misinformation, or introduce weaknesses into an adversary's systems. Cyber warfare operations may also make it possible for a state to take control of an adversary's network for the purpose of temporarily or permanently disabling it or affecting the infrastructure it supports.[344] Additionally, cyber warfare operations have the potential of depriving an adversary of essential infrastructure that supports military actions, such as communication satellites. One advantage of cyber warfare operations is that they will often achieve their desired results with less collateral damage than traditional warfare, such as, disabling an electrical grid by accessing its network in lieu of bombing the power plant.[345]

Despite the fact that cyber warfare operations have the potential of limiting collateral damage during times of hostilities, they pose several risks to states that may employ such warfare. One example would be the potential escalation of minor hostilities into a full blown armed conflict. For example, State A, having received specific evidence establishing that State B was behind DoS attacks against State A's government, declares the acts an unlawful use of force and orders an aerial bombing campaign against State B's communication facilities, the source of the attack. State B may in turn declare the acts of State A as acts of war and launch missiles into State A. In this scenario who is to blame? Did anyone actually violate international law?

One of the greatest challenges of law is keeping up with the advancement of technology.[346] The international community has often struggled to implement standards of conduct in a timely manner regarding the advancement of weaponry.[347] In the past, when new technologies emerged, in an effort to avoid war or minimize human suffering when conflicts occur, states drafted rules resulting in, for example, treaties restricting biological, chemical, and laser weapons.[348] In March 2006, Nikolai Kuryanovich, a member of the Russian Duma, noted in a letter to an ultranationalist hacker group known as the Slavic Union that, "In the very near future many conflicts will not take place

[344] *See* Hollis, *supra* note 340, at 1031.
[345] *Id.* at 1032.
[346] Brown, *supra* note 227, at 179.
[347] *Id.*
[348] *Id*.

on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers . . . ."[349] I contend that the future Mr. Kuryanovich discusses is now, and that now is the time for states to determine what is and is not permitted under international law in relation to cyber warfare operations. Failure to do so now may result in overly restrictive, reactionary regulations in response to a cyber Pearl Harbor-like attack, rather than a well thought out, proactive, structured approach.

[349] Brian Krebs, Lithuania Weathers *Cyber Attack, Braces for Round 2*, WASH. POST.COM, July 3, 2008, *available at* http://blog.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html.

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

LIEUTENANT COLONEL JOSHUA E. KASTENBERG

Lieutenant Colonel Joshua E. Kastenberg (B.A., University of California, Los Angeles (1990); J.D., Marquette University (1996); LL.M., Georgetown University (2003)) is the Staff Judge Advocate, 332d Air Expeditionary Wing, Balad Air Base, Iraq. Prior to his current assignment, he served as the staff judge advocate for Joint Task Force-Global Network Operations, a standing joint task force under the command of United States Strategic Command. Under the Unified Command Plan, it is the sole cyber-defense operational command for the Department of Defense. He is a member of the Wisconsin Bar.

I. INTRODUCTION

On 12 May 2008, the Deputy Secretary of Defense (Dep SECDEF) issued a formal definition of cyberspace via a memorandum to the secretaries of the military departments and the rest of the Department of Defense (DOD).[1] Implicit in this memorandum was a statement of the importance of cyberspace to military operations. Specifically, the Dep SECDEF noted that combatant commands and other defense components require "the ability to operate unhindered in cyberspace."[2] Thus, it is now doctrinally accepted, without any exception within the DOD, that cyberspace is a "war-fighting domain."[3]

However, cyberspace is a domain not only used by war-fighters (indeed warfighters are a miniscule minority of users), it is accessed by a significant and growing global population for business

---

[1] Memorandum from Deputy Secretary of Defense to Secretaries of the Military Departments et al., subject: The Definition of "Cyberspace" (12 May 2008) [hereinafter Dep SECDEF Memo]. The memorandum 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." *Id*.; *see also* U.S. DEP'T OF DEF. JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS, 141 (12 Apr. 2001, as amended through 17 Mar. 2009). This definition is bolstered in part by U.S. DEP'T OF DEF. DIR. 8320.02, DATA SHARING IN A NET CENTRIC DEPARTMENT OF DEFENSE para. 4.1 (23 Apr. 2007) [hereinafter DODD 8320.02], which states, "Data is an essential enabler of network-centric warfare (NCW) and shall be made visible, accessible, and understandable to any potential user in the Department of Defense as early as possible in the life cycle to support mission objectives."

[2] Dep SECDEF Memo, *supra* note 1.

[3] *See, e.g.*, Lieutenant General Keith Alexander, *Warfighting in Cyberspace*, 46 JOINT FORCE Q. 58, 58-61 (3d Quarter 2007); General James E. Cartwright, *USSTRATCOM, a Command for the 21st Century*, 42 JOINT FORCE Q. 71 (3d Quarter 2006); JOINT CHIEFS OF STAFF, JOINT PUB. 3-11, JOINT OPERATIONS, at III-22 (13 Feb. 2008) [hereinafter JP 3-11]; JOINT CHIEFS OF STAFF, JOINT PUB. 3-13 INFORMATION OPERATIONS, at I-4 (13 Feb. 2006) [hereinafter JP 3-13]. A facet of cyberspace as a warfighting domain was already accepted in terms of net-centric warfare (NCW). *See, e.g.*, DODD 8320.02, *supra* note 1, at E 1.1.18 which defines NCW as:

> An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

Also note, in the 2004 National Military Strategy for the United States, the Chairman of the Joint Chiefs of Staff noted "the Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace." CHAIRMAN OF THE JOINT CHIEFS OF STAFF, NATIONAL MILITARY STRATEGY OF THE UNITED STATES 18 (unclassified version, 2004) [hereinafter NAT'L MIL. STRATEGY].

communications, personal recreation, intelligence collection, and a host of other uses.[4] Commensurately, cyberspace is a crowded domain, and for the warfighter, access to it requires cleared pipelines, in turn necessitating a minimization of unofficial Internet access. The DOD does not own cyberspace, or even a portion of it, in a traditional legal sense.[5] But, the DOD is able to perform functions in parts of cyberspace by creating security measures which control access to those areas.[6] The area of operations controlled by the DOD is referred to as the Global Information Grid (GIG).[7] Without access to the GIG, or the ability to protect the flow of information (or freedom of maneuver) on it, the military's capabilities are severely degraded.[8]

It is axiomatic that the success or failure of military operations in cyberspace is contingent on access to cyberspace. While much of the focus on the military's use of cyberspace is on offensive or defensive roles, attention to the management of access to cyberspace is equally important. This is because without proper management, neither the full

---

[4] U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE, (February 2003) [hereinafter NATIONAL CYBERSPACE STRATEGY]. This article's argument comports with the third of five priorities set out in the Strategy, to raise national cybersecuity awareness.

[5] Two articles containing an impressive holistic discussion of cyberspace as a commons rather than a property are: Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003); Jonathan J. Rusch, *Cyberspace and the "Devil's Hatband,"* 24 SEATTLE U. L. REV. 577 (2000).

[6] *See, e.g.*, Gregory F. Intoccia & Joe Wesley Moore, *Communications Technology, Warfare, and the Law: Is the Network A Weapon System*?, 28 HOUS. J. INT'L L. 467 (2006); Davis Brown, *A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179 (2006); Ruth G. Wedgwood, *Proportionality, Cyberwar, and the Law of War*, 76 INT'L L. STUD. 219, 222 (2002); DOROTHY E. DENNING, INFORMATION WARFARE AND SECURITY 65 (1999).

[7] U.S. DEP'T OF DEF., DIR 8100.01, GLOBAL INFORMATION GRID, OVERARCHING POLICY para. E.2.1.1 (Sept. 19, 2002; certified current Nov. 21, 2003) [hereinafter DODD 8100.00], defines cyberspace as, the notional environment in which digitized information is communicated over computer networks. The DOD portion of cyberspace is referred to as the Global Information Grid, or "GIG." DODD 8100.01 defines the GIG as:

> The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services necessary to achieve Information Superiority.

[8] *See, e.g.*, Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV. 132, 132-133 (2005).

range of offensive, defensive, or exploitive operations will occur.[9] However, the DOD is currently lacking sufficient regulatory authority to ensure the availability of access to conduct operations through cyberspace, because the conduct of its members is predicated on a number of false assumptions which are written into outdated or otherwise poorly designed current regulations. This article addresses those assumptions and existing regulations and argues for new guidance to alter the current paradigm of almost unfettered access.

This article is divided into three sections. Section I touches on the nature of DOD cyberspace and the potential harms that result from current social behaviors of the department's personnel. Section II analyzes shortcomings in existing regulations to police the use of government information systems. Section III presents differing options to provide the DOD and its commanders a means to reduce the risk of malicious code through the implementation of a new regulation or lawful order. It also includes an analysis of relevant supportive federal and state court decisions. Finally, the article contains an appendix with a draft proposed regulation and a draft order. One issue throughout this article is important to note. The article and its contents are unclassified, but much of the information on cyber-intrusions, defense methods in the networks, and the forensic work on malicious codes are classified secret and top-secret. Consequently, the article relies on open source documents, which do not contain detailed information on the tactics, techniques, and procedures or adversary conduct in cyberspace.

II: THE NATURE OF DOD CYBERSPACE: CURRENT ASSUMPTIONS AND DANGERS

There are five essential considerations which require continual understanding throughout this article, and indeed, in addressing the need to change the paradigm of almost unfettered access. The first is social behavior, which is the sole focus of this article. Most users believe that access to the internet is of only nominal cost, which results in its

[9] Offensive actions fall under the rubric of Computer Network Attack (CNA) which is doctrinally defined as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." JP 3-13, *supra* note 3, at II-5. Defensive actions fall under the rubric of computer network defense (CND) which is doctrinally defined as "actions taken . . . to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks." *Id*. Intelligence and other activities on the network, such as operations preparation of the battlespace, generally fall under the rubric of computer network exploitation (CNE). *Id*. CNE is defined as enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. *Id*.

unfettered use.[10] This assumption is false. In fiscal year 2007, the DOD through the Defense Information Services Agency procured Internet access at an annual recurring cost in excess of $105 million.[11] In July 2008, a naïve e-mail user in the DOD sent out an e-mail containing an Internet game attachment. The resulting e-mails and other net activity caused a widespread disruption across the base's server.[12]

Despite the expenditure of monies, freedom of access to the internet has also translated into the idea that the DOD or its component services will block offending or dangerous sites. Problematic to this assumption is that many otherwise legitimate sites unwittingly contain malicious code, and other sites are spoofed to enable exfiltration of critical data.[13] The National Institute of Standards and Technologies (NIST), a division of the Department of Commerce, states the problem as this: "In the 1980s, malware was occasionally a nuisance or inconvenience to individuals and organizations; today, malware is the most significant external threat to most systems, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations."[14]

---

[10] *See*, e,g,, Nick Wingfield, *The Rise and Fall of Web Shopping at Work*, WALL STREET J., Sep. 27, 2002, at B1; *Charging By the Byte*, N.Y. TIMES, June 14, 2008, at C2 (discussion of bandwidth costs); Michael W. Carroll, *Open Access Publishing and the Future of Legal Scholarship: The Movement for Open Access Law*, 10 LEWIS & CLARK L. REV. 741 (2006) (arguing for freedom of access to both primary secondary legal materials).

[11] DEF. INFO. SERVICES AGENCY ANNUAL BUDGET REVIEW (2007) (on file with author and DISA).

[12] Colonel Peter Marksteiner, *The Threat from Within: E-Mail Overload Degrades Military Decision Making*, ARMED FORCES J., Sept. 2008, at 32, *available at* http://www.armedforcesjournal.com/2008/09/3640424/.

[13] NATIONAL CYBERSPACE STRATEGY, *supra* note 4, at 6; s*ee also*, ROBERT H. ANDERSON ET AL., RAND MONOGRAPH REPORT: SECURING THE U.S. DEFENSE INFORMATION INFRASTRUCTURE 17-45 (2007). For a discussion on spoofing, *see* Marc M. Harrold, *Prosecution Responses to Internet Victimization: Panel Discussion III, Working with Corporations on Case Investigation*s, 76 MISS. L. J. 875 (2007).

[14] NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-83, GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING 2-1 (Nov. 2005) [hereinafter NIST SP 800-83]. NIST recommendations are not binding on government agencies, and in particular, national security systems are exempt from NIST directives.

> Organizations should plan and implement an approach to malware incident prevention based on the attack vectors that are most likely to be used, both currently and in the near future. Because the effectiveness of prevention techniques may vary depending on the environment (i.e., a technique that works well in a managed environment might be ineffective in a non-managed environment), organizations should choose preventive methods that are well-suited to their environment and systems. An organization's approach to malware incident prevention should incorporate policy considerations, awareness programs for users and information technology (IT) staff, and vulnerability and threat mitigation efforts.

Moreover, while it is true technologies exist to block access to specific websites, it is also true that technologies exist to bypass those web-blocks, and as such, have already been employed by service-members and other DOD personnel.[15] While accessing Internet sites from DOD computers posses only one risk to malicious code, it is the most difficult to prohibit.[16] For instance, it is likely easier to prevent the transfer of information from a personal computer via a personal thumb-drive or other removable media to a DOD computer than it is to prohibit access to sites which are not currently blocked. In response to the appearance of malicious code on government information systems of various classification levels, the DOD enacted a ban on the use of certain removable media.[17] At best, technological solutions alone deprive the DOD of the full "defense in depth" that it requires to protect its cyber capabilities or critical information.

The second consideration is that risks such as malicious code occur as a function of access and connection, rather than actual time spent on an Internet site.[18] The time to download a malicious code is often measured in nanoseconds, making it virtually instantaneous.[19] Malicious code resides primarily across the Internet, but some malicious code has been designed to traverse onto computer systems with high classification levels that do not connect to the Internet.[20] Gaps, known colloquially as "air gaps," existing between isolated classified system networks and unclassified systems connecting to the Internet were thought to serve as a protective barrier against intrusions onto the

---

Id., at 3-17; *see, e.g.*, Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. §§ 3541-49 (2006).

[15] A good discussion of this problem in found in NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-28-v2, GUIDELINES ON ACTIVE CONTENT AND MOBILE CODE 3-3 (Mar. 2005) [hereinafter NIST SP 800-28-v2].

[16] NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800-53-r2, RECOMMENDED SECURITY CONTROLS FOR GOVERNMENT INFORMATION SYSTEMS B-6 (Dec. 2007) defines malicious code as software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system, such as a virus, worm, Trojan Horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

[17] *See, e.g.*, William H. McMichael & Bruce Rolfsen, *Despite Network Virus—Avoid Thumb Drives*, A.F. TIMES, Dec. 8, 2008, at 13.

[18] NIST SP 800-28-v2, *supra* note 15, at 3-1); s*ee also* 3 HOSSEIN BIDGOLI, INFORMATION SECURITY: THREATS, VULNERABILITIES, PREVENTION, DETECTION, AND MANAGEMENT 44-45 (2006).

[19] *See, e.g.*, Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1023-26 (2001). A good discussion on the subject of malicious code is also found in *State v. Corcoran*, 522 N.W.2d 226 (Wis. Ct. App. 1994).

[20] *See, e.g.*, Lolita C. Baldor, Associated Press, *Pentagon Bans Computer Flash Drives*, THE SUNDAY OREGONIAN, Nov. 23, 2008, at A3.

classified systems.[21] But, information on the classified systems as well as the systems themselves may be in jeopardy by both the lawful transference of information, as well as the negligent transference of information between the classified levels.[22] As a result, this article is not concerned with the ethical implications of time spent in web-surfing from government information systems during duty hours, but the web-surfing itself.

The third consideration is what the reduction in unofficial Internet access traffic will give commanders overseeing military operations. United States military operations rely on decisional superiority, freedom of maneuver, and operational security.[23] Because of excessive unofficial Internet usage, the DOD decided to purchase commercial Internet service in the U.S. Central Command area of responsibility. The reduction in unofficial Internet access traffic will protect these essential operational requirements by reducing the risk to the GIG.

Fourth, the exponential growth of malicious code risks to secured information on the GIG, the ability for the DOD to freely access the GIG, and the integrity of secured information on the GIG are all part of the same concern: GIG security. While no regulation, however austere, will remove all risks, it is very apparent that nation-states and non-state actors have engaged in robust exfiltration of data from government information systems, including the DOD's systems.[24]

---

[21] *See, e.g.*, Edmund X. DeJesus, *Airborne Viruses*, INFO. SECURITY MAG., Apr. 2001, at 9, *available at* http://islab.oregonstate.edu/news/2001-04-15.pdf. Notions of "air gap" protection have changed over time. Prior to the widespread use of wireless technology, the "air gap" was thought of as a pure protection. *See, e.g.*, Steven A. Heinrich & Roxana Dastur Malladi, *News of the Wired: Security, the Network, and the Networked Office*, 56 OR. ST. B. BULL. 15, 16 (1995). The Oregon Bar advised law firms:

> The only foolproof protection against penetration of a system is an "air gap." The only way that a computer or a networked office can be fully protected from hackers is to have a physical gap separating every computer in that office system from the Internet or the telephone system. The term "air gap" means an absolute communications gap between the computer system and the Net or the telephone.

However, wireless technology has rendered this type of security obsolete.

[22] "Air gap" architecture is explained in BIDGOLI, INFORMATION SECURITY, *supra* note 18, at 522-524.

[23] These factors are found in a number of Executive Statements and DOD publications. *See, e.g.*, NAT'L MIL. STRATEGY, *supra* note 3, at 15-19; U.S. DEP'T OF DEF. DIR. 5205.2, OPERATIONAL SECURITY (OPSEC) PROGRAM (29 Nov. 1999) [hereinafter DODD 5205.2].

[24] *See, e.g.*, GENERAL JAMES T. CONWAY, ADMIRAL GARY ROUGHEAD & ADMIRAL THAD W. ALLEN, A COOPERATIVE STRATEGY FOR TWENTY-FIRST CENTURY SEAPOWER (Oct. 2007), *available at* http://www.navy.mil/maritime/MaritimeStrategy.pdf.

Moreover, the 2007 Estonian experience, in which denial of service attacks encumbered that allied government's ability to rely on its information systems, must concern the integrity of DOD systems.[25]

Fifth and finally, a definition of official use and unofficial use in terms of Internet access does not currently exist in the DOD lexicon. For the purpose of this article, unofficial use is defined as a use which does not relate to the functions or necessities of DOD personnel or mission sets.[26] For instance, individuals accessing weather information in preparation for a TDY or real estate information in preparation for a permanent change of station (PCS) move may articulate the search as related to official duty. On the other hand, when individuals access those same sites prior to a personal vacation or for non-PCS investment reasons, there is little likelihood the same articulation to mission nexus can occur.

Access to the Internet from any location occurs with a number of inherent risks. These risks include the transfer of malicious code, which may be designed to remotely corrupt or commandeer a computer system, destroy the system, implant a virtual beacon on the system to provide information to a far-way user, or convey false information through the user's system.[27] One recent study concluded that 80% of legitimate sites have malicious code implanted.[28] The exponential growth of malicious codes has affected the DOD systems, making them increasingly vulnerable to the risks noted above. Technical solutions provide only a short-term solution and a partial insurance against these

---

[25] *See, e.g.*, Steven Myers, *Cyberattack on Estonia Stirs Fears of 'Virtual War,'* N.Y. TIMES.COM, May 18, 2007, http://www.nytimes.com (last visited Sept. 15, 2009); Associated Press, *Estonian Links Moscow to Internet Attack*, N.Y. TIMES, May 18, 2007, *available at* http://www.nytimes.com (last visited Sept. 15, 2009). The Estonian cyber experience is by no means the only conflict involving cyberspace which should concern national security. NATO operations in Kosovo were frequently the target of hackers. *See, e.g.*, George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1082-1084 (2000).

[26] This definition is taken in part from U.S. DEP'T OF DEF. JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS, *supra* note 1, which defines "Official Information" as "information that is owned by, produced for or by, or is subject to the control of the United States Government." *Id.* at 390.

[27] *See Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Subcomm. on Criminal Justice Oversight of the S. Judiciary Comm and the Crime Subcomm. of the H. Judiciary Comm.*, 106th Cong. 35-37 (2000) (statement of Michael A. Vatis, Director, FBI National Infrastructure Protection Center); *see also Cyber Threats and the U.S. Economy: Joint Hearing Before the Econ. Comm.*, 106th Cong. (2000) (statement of Dr. Mark Graff, Sun Microsystems), 2000 WL 11068388.

[28] *See, e.g.*, White Hat, Malicious Code Study (2008) (on file with Joint Task Force Global Network Operations, Arlington, Va.); Symantec, Security Response Team White Papers, Privacy: A Study of Attitudes and Behaviors in US, UK and EU Information Security Professionals (Oct. 2003), http://www.symantec.com (last visited Sept. 17, 2009); MCAFEE, MAPPING THE MAL-WEB REVISITED (Jun. 4, 2008), http://www.mcafee.com (last visited Sept. 17, 2009).

risks, primarily because the ability of malicious code developers matches the ability of security advances.

Like most computer networks, DOD computer information systems provide a ready access to the Internet.[29] During any given twenty-four hour period the Internet is accessed over one billion times from roughly seven million DOD owned computers.[30] The overwhelming majority of this traffic occurs on the Non-Secure Internet Protocol Router Network (NIPRNET). In an ongoing study, over two-thirds of Internet access from DOD computers occurs for non-official purposes. The types of sites accessed including dating services, resort and vacation sites, car purchases, electronic stock and commercial trading, sports sites, and "streaming video" sites.[31] While it is remotely possible a small minority of users accessing these sites could argue the access occurred for an official DOD purpose, one would be hard pressed to believe the bulk of the access was for a mission-related function.

Despite the fact that the NIPRNET is non-secure, a number of protected, encrypted, or coded DOD functions occur across it. These functions include pay and leave access, transfer and tracking of component parts, the bulk of aircraft schedules, medical information transfers, fuel data, travel schedules of ranking officers and civilian personnel, real-time communications, and a variety of other data which is closely guarded and essential for military operations.[32] Moreover, information may be transferred to and from the NIPRNET to the Secured Internet Protocol Router Network (SIPRNET), as well as higher classified systems, placing the higher classification of SIPRNET and other access data at risk.[33]

III: INADEQUACIES OF CURRENT REGULATIONS

Prior to examining current departmental and service regulations, it is essential to examine 10 U.S.C. § 2224, which directs SECDEF to develop and maintain a "Defense Information Assurance Program."[34] The regulations examined below, in some measure, are buttressed by this law. For instance, it requires this program to "provide continuously

---

[29] *See, e.g.*, Antolin-Jenkins, *supra* note 8 at 133. Jenkins notes that 95% of military information traffic utilizes civilian networks at some stage of communication. *Id*., citing Ronald Knecht & Ronald A. Grove, The Information Warfare Challenges of a National Information Infrastructure (Mar. 22, 2009) (unpublished U.S. Army War College Strategy Research Project), *available at* http://www.dtic.mil/cgi-bin/.

[30] DEF. INFO. SERVICES AGENCY REPORT (2007) (delivered to U.S. Congress, on file with author and DISA).

[31] JOINT TASK FORCE GLOBAL NETWORK OPERATIONS REPORT (2008) (delivered to the Joint Chiefs of Staff, on file with author).

[32] *Id*.

[33] *Id*. Higher systems include Intelligence Community (IC) networks.

[34] 10 U.S.C. § 2224(a) (2006).

for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure."[35] It additionally charges SECDEF to develop a program strategy that encompasses those actions necessary to assure the readiness, reliability, continuity, and integrity of Defense information systems, networks, and infrastructure . . . ."[36]

But, as noted in the introduction, regulatory authorities do not adequately address network threats to the DOD's mission capabilities, and this fact shows a failing to comply with 10 U.S.C. § 2224. Moreover, the regulations containing rules governing Internet access are disjointed. These include departmental regulations, Chairman of the Joint Chiefs of Staff Instructions, service regulations, and individualized user agreements. Moreover, while rescission of security clearances based on Internet misuse has also been sustained by administrative law judges, this is merely a "backdoor" method for addressing the problem and available in only limited circumstances.[37] For reasons noted below, none of these regulations satisfactorily mitigates the threats described above.

A. Joint Ethics Regulation

Department of Defense Directive 5500.7-R, the *Joint Ethics Regulation* (hereafter JER)[38] governs the conduct of all DOD personnel. It was most recently updated on November 29, 2007.[39] The JER was promulgated to buttress public trust in the Department of Defense.[40] It also serves as a mirror to the Code of Federal Regulations (CFR) and other government instruments serving the same purpose.[41]

---

[35] 10 U.S.C. § 2224(b) (2006).
[36] 10 U.S.C. § 2224(c) (2006).
[37] *SSN: Applicant for Security Clearance*, ISCR Case No. 02-29244, 2005 DOHA LEXIS 681 (Defense Office of Hearings & Appeals Apr. 6, 2005); *SSN: Applicant for Security Clearance*, ISCR Case No. 02-16613, 2004 DOHA LEXIS 86 (Defense Office of Hearings & Appeals Mar. 10, 2004). Both of these cases involve a contractor's loss of clearance after violating government regulations on internet misuse prohibiting pornography.
[38] U.S. DEP'T OF DEF., DIR. 5500.7-R, JOINT ETHICS REG. (30 Aug. 1993) (C6, 29 Nov. 2007) [hereinafter JER]. The Department of Defense General Counsel manages the Joint Ethics Regulation and all programs underneath it. *Id*. § 1-407.
[39] *Id*. at 43.
[40] *Id*. § 1-300.
[41] *See* Standards of Ethical Conduct for Employees of the Executive Branch, 5 C.F.R. § 2635 (1978). Department personnel are also required to comply with 5 C.F.R § 2635.101(a) which states:

> *Public service is a public trust.* Each employee has a responsibility [to the United States Government and its citizens to place loyalty to the Constitution, laws and ethical principles above

The JER governs such areas as political activities, relationships between DOD personnel and contractors, gifts between superiors and subordinates, expenditures of government monies for conferences, and attendance at private events. The JER's primary strengths are that it is the most holistic governance for DOD personnel in regard to professional behavioral standards and it does not contradict the Uniform Code of Military Justice (UCMJ). Moreover, the JER provides the due process notice requirements for enumerated military offenses under which violations may be charged.[42] Violations of the JER may be charged against persons subject to the UCMJ through Article 92.[43]

At first glance, the JER should provide some authority to regulate unofficial access to the Internet because is a fundamental principle of administrative law that an agency is bound to adhere to its own regulations.[44] However, as a disciplinary tool, the JER has rarely served as the basis for charging UCMJ offenses in courts-martial. Indeed, the appellate record of published cases is slim. In *United States v. Crafter*,[45] the Court of Appeals for the Armed Forces (CAAF) upheld a court-martial conviction based on the provision of the JER prohibiting bribery.[46] CAAF has also upheld a conviction for accessing child pornography and bestiality websites charged under the JER.[47] However,

---

> private gain. To ensure that every citizen can have complete confidence in the integrity of the Federal Government, each employee shall respect and adhere to the principles of ethical conduct set forth in this section, as well as the implementing standards contained in this part and in supplemental agency regulations.

[42] *See, e.g.*, Parker v. Levy, 417 U.S. 733, 755 (1974) (An accused must be on notice that his conduct is unlawful and that the article fairly informs "that the particular conduct which he engaged in was punishable"). Although the notice requirement of the Joint Ethics Regulation has apparently not been challenged at the appellate level, it is reasonable to assume it meets this due process standard.

[43] *See* MANUAL FOR COURTS-MARTIAL, UNITED STATES pt. IV, ¶16a (2008) [hereinafter MCM].

[44] Frizelle v. Slater, 111 F.3d 172, 177 (D.C. Cir. 1997).

[45] United States v. Marcum, 60 M.J. 209 (C.A.A.F. 2006).

[46] *Id.* at 210. The specification read:

> [D]id, at or near Seymour Johnson Air Force Base, on or about 9 May 9 2002, violate a lawful general regulation, to wit: the Joint Ethics Regulation, Department of Defense Directive 5500.7-R, Chapter 5, ¶ 5-400(a), dated 30 August 1993, by wrongfully accepting currency of some value for arranging for Federal Prison Camp Inmate [G] to meet in private with his friend [Ms. ADP] at a billeting room at the Southern Pines Inn, a willful violation of [his] lawful duties to supervise the work of the said Federal Prison Camp Inmate.

[47] *See* United States v. Hays, 62 M.J. 158 (C.A.A.F. 2005).

bribery and child pornography are already prohibited in other regulations, raising the question as to why the JER was incorporated into a UCMJ charge and specification in the first place.

Civilian employment within the DOD has been terminated on the basis of JER violations as well, but only rarely. The Merit Systems Protection Board (MSPB), the primary governing body for adjudicating challenges to adverse employment decisions, has upheld agency decisions to terminate employment for such reasons as monetary debts to subordinates,[48] using government computers for personal business and sending sexually suggestive e-mails to other employees,[49] accepting gifts from subordinates exceeding the amount permitted under the regulation,[50] and, sexual harassment.[51]

However, it does not appear that under either the JER, or its incorporation under the UCMJ, that any charges have occurred for excessive unofficial non-pornographic Internet access or access for personal recreational purposes. Accessing pornography has been amply charged against both uniformed service members and non-uniformed DOD employees but usually not under the JER.

In terms enabling the sought-after paradigm change, the JER possesses inherent weaknesses beyond the obvious statistical evidence. To begin, the regulation in section 2-301 lumps computer use in the same category as other modes of government-owned communications, to include telephones and facsimile machines.[52] While service members have been prosecuted for using government telephones, military law favors charging unofficial telephone use under UCMJ, Article 121, prohibiting larceny, rather than under the JER.[53] It would be difficult to charge unofficial access to the Internet under the same article prohibiting larceny because that particular article requires the government to prove the user's intent to permanently deprive the owner of a property, that the property had a rightful owner, and that the property had an actual value, or at least some nominal value.[54]

---

[48] *See* 5 U.S.C. § 1204 (2006) for the authority of the MSPB. *See* also, Fine v. Peters, 2000 EEOPUB LEXIS 4525 (U.S. Equal Employment Opp. Comm. 2000).

[49] Barnes v. Dep't of Def., 2006 MSPB LEXIS 3148 (Merit Systems Protection Board 2006).

[50] Siozon-Peterson v. Dep't of the Air Force, 2005 MSPB LEXIS 2067 (Merit Systems Protection Board 2005).

[51] Reynolds v. Dep't of the Army, 2003 MSPB LEXIS 1087 (Merit Systems Protection Board 2003).

[52] JER, *supra* note 38, § 2-301(a).

[53] *See, e.g.*, United States v. Cornell, 15 M.J. 932 (C.M.A. 1983) (determining that personal telephone use could be charged as larceny, instead of under the JER); United States v. Abeyta, 12 M.J. 507 (A.C.M.R. 1981) (determining that personal telephone use could be charged as larceny, instead of under the JER).

[54] MCM, *supra* note 43, pt. IV, ¶ 46b(1); *see also* United States v. Batiste, 11 M.J. 791 (A.F.C.M.R. 1981) (theft of urine sample a proper charge for larceny even though urine generally possesses no known value). Unlike urine, which has a theoretical owner, it is

The JER does not take into account the risk to the GIG or the nature of the NIPRNET. Indeed, it does not even make use of those terms anywhere within its voluminous rules. Telephones and facsimile machines do not, as a general rule, have the capability of transferring malicious code, serve as an effective tool for the exfiltration of data, or possess the inherent capability of a takeover from an operator at a remote site.

Section 2-301(a) governs the use of DOD computers under the aegis of "Use of Government Resources."[55] The regulation defines official use to include such matters as: emergency communications, communications to military members and other DOD employees who are deployed or in extended TDY status.

Yet, the regulation permits commanders flexibility to permit DOD personnel at a normal workplace to conduct brief internet searches beyond matters involving official business or family communications under certain conditions reflecting the overarching ethics rules.[56] The JER does not define brief internet searches, leaving one to conclude that the content of such searches are only constrained by what is already prohibited under other regulations or laws such as pornography, child pornography, gambling, or political activities.[57]

As a further example of the regulation's permissive nature, wide-ranging Internet searches are permitted when that activity does not adversely affect the performance of official duties of the DOD employee or organization. Although the regulation does not define the term

---

unlikely the prosecution could claim that the government was deprived of the GIG or that the GIG possesses a quantifiable – albeit nominal – value. It may be the case that the Internet is public and therefore abandoned property. *See, e.g.*, United States v. Meeks, 32 M.J. 1033, 1035-1036 (A.F.C.M.R. 1992); United States v. Walls, 2 C.M.R. 650 (A.F.B.R. 1951). Moreover, the proof required to determine that a user who accesses the Internet for unofficial uses intended to deprive the government of its property could not likely be met by any reasonable quantum.

[55] *See* JER, *supra* note 38, § 2-301(a). The JER notes: "Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems when in use is paid for by the Federal Government) shall be for official use and authorized purposes only."

[56] *Id.*

[57] JER, *supra* note 38, § 2-301(a)(2)(d) reads:

> Do not put Federal Government communication systems to uses that would reflect adversely on the DOD or the DOD Component (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service) . . . .

"brief," it permits use that is of "reasonable duration and frequency"[58] and serves "a legitimate public interest."[59] The regulation does not define "legitimate public interest," but it provides examples such as "enhancing the professional skills of" DOD employees or "job searching."[60] Therein is the proof that the JER's drafters missed the fundamental risk factors in Internet access in that it is a matter of access and not time spent on any particular activity which creates risk in the first place.

B. Other DOD-Wide Regulations

Other regulations exist which govern the use of the government information systems as well as the GIG, but none directly addresses the social behaviors of accessing the Internet. For instance, DODD 8500.01E, *Information Assurance*,[61] articulates policy to regulate access to the internet, but primarily through technological solutions.[62] Its implementation instruction, DODI 8500.2, *Information Assurance (IA) Implementation*,[63] places on all DOD personnel the responsibility to only access data for "which they are authorized or have a need to know."[64] While 8500.02 provides defined language, it is not a regulation under which DOD personnel may be disciplined for unofficial Internet access, though arguably if the access resulted in damage or disruption to

---

[58] *See* JER, *supra* note 38, § 2-301(a)(2)(b).
[59] *Id.* § 2-301(a)(2)(c).
[60] *Id*.
[61] U.S. DEP'T OF DEF. DIR. 8500.01E, INFORMATION ASSURANCE (Oct. 24, 2002; certifie4d current as of Apr. 23, 2007) [hereinafter DODD 8500.01E].
[62] *Id.* para. 4.12.

> DOD information systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DOD information systems through physical means. This includes remote access for steelwork.

[63] U.S. DEP'T OF DEF. INSTR. 8500.2, INFORMATION ASSURANCE (IA) IMPLEMENTATION (Feb. 6, 2003) [hereinafter DODI 8500.2].
[64] *Id*. para. 5.12.

> DOD information systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DOD information systems through physical means. This includes remote access for steelwork.

Id.

DOD information systems, DOD personnel might become the subject of an investigation.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI), 6211.02C, *Defense Information Systems Network (DISN) Policy, Responsibilities, and Processes*,[65] imposes responsibility on all DOD personnel to protect classified information, including classified information on DOD networks.[66] It also provides parameters of "authorized uses" for government information systems capable of accessing the internet. But the parameters for acceptable Internet access in this instruction mirror those in the JER.[67] CJCSI 6510.01E, *Information Assurance (IA) and Computer Network Defense (CND)*,[68] provides additional authority to hold accountable individuals who place government information systems at risk through negligent conduct or intent. The range of accountability includes terminating an individual's ability to access the Internet from a government information system.[69] However, CJCSI 6510.01E does not require combatant commands, services, and agencies to reduce the amount of Internet access.

C. Service Rules and Regulations

Army Regulation (AR) 25-1, *Knowledge Management and Information Technology*, establishes the policies and assigns responsibilities for the management of information resources and

---

[65] CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION 6211.02C, DEFENSE INFORMATION SYSTEM NETWORK (DISN): POLICY, RESPONSIBILITIES AND PROCESSES (9 Jul. 2008) [hereinafter CJCSI 6211.02C].

[66] *Id*. encl. B, para. 9.r.

> DOD and non-DOD personnel (including supporting contractor personnel) are held personally and individually responsible and accountable for providing proper protection of classified information, controlled unclassified information, ISs, and/or networks under their custody and control . . . . DOD officials who hold command, management (e.g., DAA and Information Assurance Manager), or supervisory positions (e.g., Information Assurance Officer or supervisors) will ensure that the Information Security Program is efficiently implemented and managed within their areas of responsibility . . . .

Id.

[67] *Id*., para. n.

[68] CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION 6510.01E, INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND) (15 Aug. 2007, current as of 12 Aug. 2008) [hereinafter CJCSI 6510.01E].

[69] While this document articulates roles and responsibilities of commands and individuals, a CJCSI is not a regulation of a punitive nature.

information technology.[70] This regulation governs internet access for all personnel assigned to, or employed by, the Department of the Army. While the entirety of AR 25-1 is not punitive, the regulation notes there are punitive portions.[71]

Of importance, unlike the JER, the authors of AR 25-1 evidenced their understanding of the GIG by incorporating and defining the NIPRNET and SIPRNET into the regulation. Notably, AR 25-1 prohibits computer activity "that could reasonably be expected to" congest, delay, or disrupt computer service.[72]

In one sense, the language contained in AR 25-1 is superior to that found in the JER. Specific intent is not the liability standard for violations.[73] Thus only a general negligence of Internet access which

---

[70] U.S. DEP'T OF ARMY, REG. 25-1, KNOWLEDGE MANAGEMENT AND INFORMATION TECHNOLOGY (4 Dec. 2008) [hereinafter AR 25-1].

[71] *Id*. at i. The regulation notes, "Portions of this regulation, which prescribes specific prohibitions, are punitive, and violations of these provisions may subject offenders to nonjudicial or judicial action under the Uniform Code of Military Justice." *Id*.

[72] *Id*. at para. 6-1.f(5) (prohibiting the use of Army communications systems in ways "that could reasonably be expected to cause, directly or indirectly, congestion, delay, or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with others' use of communications") While the regulation provides examples of conduct which could cause a detriment, the list is not all-inclusive. The list reads:

> *(a)* Create, download, store, copy, transmit, or broadcast chain letters.
> *(b)* "Spam" to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.
> *(c)* Send a "letter-bomb" to re-send the same e-mail message repeatedly to one or more recipients, to interfere with the recipient's use of e-mail.
> *(d)* Broadcast unsubstantiated virus warnings from sources other than systems administrators.
> *(e)* Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting the relevant audience.
> *(f)* Employ applications for personal use using streaming data, audio, and video; malicious logic and virus development software, tools, and files; unlicensed software; games; Web altering tools/software; and other software that maycause harm to Government computers and telecommunications systems.
> *(g)* Disseminating large files over e-mail instead of using shared drives . . . .

Id.

[73] *See, e.g*., United States v. Hernandez-Landaverde, 65 F. Supp. 2d 567 (S.D. Tex, 1999). Specific intent is defined at common law as follows:

> The intent to accomplish the precise criminal act that one is later charged with. General intent is defined as "the state of mind required for the commission of certain crimes not requiring specific

results in system degradation is required to hold a person punitively accountable for violating the regulation. Despite the recognition of threats to the GIG, AR 25-1 incorporates the permissive access to Internet doctrine found in the JER.[74] This permissiveness includes, personal "brief Internet searches," without providing any further parameters as to the meaning of the limitation.[75]

Air Force Instruction (AFI) 33-129, *Communications and Information: Web Management and Use*, is the Air Force's counterpart to AR 25-1.[76] Like AR 25-1, it provides a framework for access, modeled on the JER.[77] Also, like its Army counterpart, AFI 33-129 provides a non-inclusive list of inappropriate use. This list is broader than AR 25-1 as it also prohibits modifying or altering the network operating system or system, and permitting an unauthorized individual to access a DOD computer system. However those two examples are

---

> intent. General intent usually takes the form of recklessness (involving actual awareness of a risk and the culpable taking of that risk), or negligence (involving blameworthy inadvertence)."

Id. at 571 (citing BLACK'S LAW DICTIONARY 813 (7th ed. 1999)).

[74] AR 25-1, para. 6-1.d(1) ("The Joint Ethics Regulation, Section 2–301, serves as the basis for Army policy on the use of telecommunications and computing systems. Users will abide by these restrictions to prevent security compromises and disruptions to Army communications systems.").

[75] AR 25-1, para. 6-1.e. The regulation states the following:

> Authorized use includes brief communications made by DOD employees while they are traveling on Government business to notify family members of transportation or schedule changes. They also include personal communications from the DOD employee's usual workplace that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief Internet searches; e-mailing directions to visiting relatives). Such communications may be permitted, provided they—
>
> (1) Do not adversely affect the performance of official duties by the employee or the employee's organization.
> (2) Are of reasonable duration and frequency, and, whenever possible, are made during the employee's personal time, such as during lunch, break, and other off-duty periods).
> (3) Are not used for activities related to the operation of a personal business enterprise . . . .

Id.

[76] U.S. DEP'T OF AIR FORCE, INSTR. 33-129, *Communications and Information:* WEB MANAGEMENT AND INTERNET USE (3 Feb. 2005, incorporating changes through 12 Sep. 2009).

[77] *See id*. para. 2.1, which states: "Appropriate Use. Government-provided hardware and software are for official use and authorized purposes only. Appropriate officials may authorize personal uses consistent with the requirements of DDOD 5500.7-R, *Joint Ethics Regulation (JER*) . . . ."

prohibited in other regulations. Moreover, AFI 33-129 is unique in prohibiting the use of measures to circumvent blocked sites or other security systems.[78]

IV. COURSES OF ACTION

There are at least four possible courses of action to effectuate a change in the current paradigm of almost-open Internet access. The DOD can draft a new regulation (or series of regulations) limiting access to the Internet through government information systems. Such a regulation would be divorced from the JER, but the JER would, in turn, require modification to section 2-301.

A second course of action is to have local commanders recognize the inherent risks of the current paradigm, preempt the JER and draft lawful orders applicable to the commander's respective installation, command, or vessel. In the legal rubric of lawful command, it is, of course, possible for the President or SECDEF to issue a lawful command limiting Internet access through government information systems. This course of action could occur at a far more rapid rate than issuing a regulation but would come at the cost of denying full input from the services, combatant commands, and field agencies.

A third course of action would be to draft a new regulation, but while the process of drafting, input, and promulgation is occurring, permit local commanders to issue lawful orders. This course of action is essentially a hybrid of the prior two. Finally, a fourth course of action is to do nothing, and permit the JER and other service regulations and user agreements to regulate internet access through government information systems.

A. Lawful Order

Historically, the most immediate means of effectuating an enforceable policy change has been the issuance of a lawful order from a command authority. While lawful orders are generally issued by officers commanding installations or vessels, the President, followed by the SECDEF, are the two highest command authorities.[79] They are

[78] *Id*. paras. 2.2.1-2.2.14 list prohibited actions. Para. 2.2.9 prohibits attempts to "circumvent or defeat security or modifying security systems without prior authorization or permission (such as for legitimate system testing or security research)."

[79] The basis for this construct is deeply rooted in American Constitutional jurisprudence. *See, e.g*. 10 U.S.C. §§ 111, 113 (2006); Martin v. Mott, 25 U.S. (12 Wheat.) 19 (1827) (authority over all military forces under the President's constitutional status as commander in chief); Little v. Bareme, 6 U.S. (2 Cranch.) 170 (1804) (presidential authority over all service members not unlimited but very broad).

constitutionally empowered to issue orders which have a service-wide effect.[80]

In terms of hierarchy and reach of authority, the three Service Secretaries, four commissioned chiefs of their respective services, and the combatant commanders follow.[81] The authority to issue a lawful order descends to the lowest command level.[82] Depending on the service, location, and chain of command, the level of authority may simply be whoever is of highest rank in a given chain.[83] But, only the President and Defense Secretary have the ability to directly order the entire Department to comply with a policy.[84]

The UCMJ, Article 92, governs the punitive nature of lawful orders. The essential attributes of a lawful order include: (1) issuance by competent authority—a person authorized by applicable law to give such an order; (2) communication of words that express a specific mandate to do or not do a specific act; and (3) relationship of the mandate to a military duty.[85] Orders are generally presumed to be lawful, and it is for a judge to decide whether this is the case.[86] An

---

[80] SECDEF may issue a general order which binds all service members (and by implication all civilian federal employees of the Department), notwithstanding that directives, regulations, and instructions are almost always conveyed in a specific format. *See, e.g.*, United States v. Brown, 25 C.M.R. 20 (C.M.A. 1957); United States v. Snyder, 4 C.M.R. 15 (C.M.A. 1952).

[81] 1986 DOD Reorganization Act, Pub. L. No. 99-433, 100 Stat. 1013 (codified as amended in scattered sections of 10 U.S.C.).

[82] *See* United States v. Voorhees, 16 C.M.R. 83, 96 (C.M.A. 1954) ("A general order or regulation is lawful if not contrary to or forbidden by the Constitution . . . an Act of Congress or the lawful order of a superior authority").

[83] *See* MCM, *supra* note 43, pt. IV, ¶¶ 14 & 16.

[84] *Id.*, pt. IV, ¶ 16(c)(1)(a); expressly gives to the SECDEF the authority to issue a punitive general order. A general order from the SECDEF may only be superseded by an order from the President or by a rescission from the SECDEF. No service or commanding general orders may contradict or modify the order. Unlike a directive or policy memo, an order is clearly applicable to all service members without distinction of position or rank (unless the order permits distinctions or exceptions based on legitimate service requirements).

[85] United States v. Deisher, 61 M.J. 313, 317 (C.A.A.F. 2005); United States v. New, 55 M.J. 95, 100 (C.A.A.F. 2001); United States v. Hughey, 46 M.J. 152, 154 (C.A.A.F. 1997); MCM, *supra* note 43, pt. 14, ¶ c(2)(a).

[86] United States v. New, 55 M.J. 95, 107 (C.A.A.F. 2001), quoting from Article 92:

> The order must relate to military duty, which includes all activities reasonably necessary to accomplish a military mission, or safeguard or promote the morale, discipline, and usefulness of members of a command and directly connected with the maintenance of good order in the service. The order may not, without such a valid military purpose, interfere with private rights or personal affairs. However, the dictates of a person's conscience, religion, or personal philosophy cannot justify or excuse the disobedience of an otherwise lawful order.

order, in addition to showing its intent to regulate some aspect of behavior of servicemen, must state clearly whether it is punitive.[87]

The issuance of multiple lawful orders across the DOD has two inherent difficulties rooted in law. Firstly, it is a fundamental due process right that DOD personnel have fair notice of the criminality of a prohibited conduct before being charged or convicted of an offense.[88] If every military base, post, encampment, or station has its own separate set of rules, those particular rules have to be visible and understood by the persons falling within the jurisdictional reach of those specific rules.[89] Even in a scenario in which major commands create their own independent rules, the issue of notice will exist, in part, because military personnel transfer from post to post. While the difficulty of providing notice is not insurmountable, it is far less difficul if the order is issued from the highest levels.

Secondly, one of the potential enforcement problems with commanders independently issuing orders in the absence of a regulation may be challenges based on the Fifth Amendment's guarantee of "equal protection."[90] Rooted in due process, "equal protection" protects individuals from differences in treatment from a convening authority.[91]

Within the services, different commanders may issue differing orders, with unique prohibitions. A violator of one order might seek to challenge a commander's decision to offer non-judicial punishment or prefer charges for violating the order. While "equal protection" challenges might arise from the fact that each of the services (or, the major commands within each service) have different prohibitions against unofficial Internet access, the majority of these challenges would

---

[87] The MCM reflects the fact that a myriad of regulations, instructions, and manuals govern virtually every aspect of military life, and that most of these issuances are not intended to establish the criminal offense of violating a lawful general regulation. *See* United States v. Nardell, 45 C.M.R. 101 (C.M.A. 1972); United States v. Hogsett, 25 C.M.R. 185 (C.M.R. 1958).

[88] *See, e.g.*, United States v. Tolkach, 14 M.J. 239 (C.M.A. 1982).

[89] *See* United States v. Pope, 63 M.J. 68, 73-75 (C.A.A.F. 2007); *see also* Cole v. Arkansas, 333 U.S. 196, 201 (1948).

[90] U.S. CONST. amend. V; *see also* Skinner v. Oklahoma, 316 U.S. 535 (1942). In *Skinner*, the Court held that "when the law lays an unequal hand on those who have committed intrinsically the same quality of offense . . . it has made as invidious a discrimination as if it had selected a particular race or nationality for oppressive treatment."*Skinner* at 541 (citing Yick Wo v. Hopkins, 118 U.S. 356 (1886)); *see also* Gaines v. Canada, 305 U.S. 337 (1938).

[91] For a good discussion of equal protection in military law see *United States v. Courtney*, 1 M.J. 438, 441 (C.M.A. 1976), and, most recently, *United States v. Paulk*, 66 M.J. 641 (A.F. Ct. Crim. App. 2008). In *Paulk*, the Air Force Court determined it was not a violation of equal protection if Air Force judges were non-tenured for a fixed term of service, while Department of the Army military judges and Coast Guard military judges served for fixed-tenure terms. The Navy-Marine Corps Court of Criminal Appeals determined similarly to the Air Force Court in *United States v. Gaines*, 61 M.J. 689 (N-M. Ct. Crim. App. 2005).

fail. "Equal protection" usually applies to constitutionally suspect classes of individuals who have historically suffered discrimination based on race, religion, or national origin.[92] In 1981, the Court of Military Appeals (the predecessor to CAAF), in *United States v. Means*,[93] determined that the rank or status of an individual could be a determining factor in a commander's decision to refer a military member to a court-martial as long as the status did not involve race, religion, national origin, or another protected factor.[94]

Lawful orders may exist in the form of standard "user agreements," in which the user of government computers agrees not to engage in non-mission related web surfing. Clearly a standard "user agreement" will be an appropriate instrument to provide notice as to a prohibition against unofficial access to the Internet. But alone, arguably the user agreement is not enough to create a culture change in Internet access.

B. Regulations

Punitive general orders issued directly from the Secretary of Defense to the entire Department have been rare since the Goldwater-Nichols Act. This is because the Department adopted a means for projecting policies, regulations, and other rules to its service members and federal employees mirroring the Code of Federal Regulations.

The issuance of regulations to the services is a function of the executive branch, which mirrors the legal construct of issuing lawful orders but occurs as a defined process.[95] However, in comparison to

---

[92] United States v. Batchelder, 442 U.S. 114 (1979); 3 R. ROTUNDA AND J. NOWAK, TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE AND PROCEDURE § 18.38, at 488, 18.41 at 495 (3d ed. 1999).

[93] United States v. Means, 10 M.J. 162 (C.M.A. 1981).

[94] *Id*, at 165. In *Means*, the Court determined that the commissioned officer status of an accused is a permissible factor in determining to refer a trial for courts-martial. The court held:

> Even if appellant's officer status had been a principal factor—indeed, the decisive factor—in the convening authority's decision to refer the case to a general court-martial, appellant would still have no valid constitutional grievance. For the Government to make distinctions does not violate equal protection guarantees unless constitutionally suspect classifications like race, religion, or national origin are utilized or unless there is an encroachment on fundamental constitutional rights like freedom of speech or of peaceful assembly. The only requirement is that reasonable grounds exist for the classification used.

Id.

[95] 10 U.S.C. § 121 (2006). "The President may prescribe regulations to carry out his functions, powers, and duties under this title." *Id*.

posting an order, the drafting and issuance of regulations is time consuming because it involves the comments and concerns of the service departments, combatant commands, and agencies.[96] On the other hand, published regulations which specifically prohibit unofficial Internet access from DOD computers are the optimum means of establishing a single department-wide framework for mitigating risks from malicious code. There are, of course, legal considerations before drafting and implementing such regulations.

As in the case of lawful orders, any regulatory changes which affect the conditions of employment will likely require negotiation with collective bargaining units.[97] While localized orders prohibiting unofficial access to the Internet will, at most, require limited notice to collective bargaining units, a DOD-wide regulation may require negotiation with multiple collective bargaining units representing personnel.

A new regulation will also require other changes. Certainly, the adaptation of a new regulation will require ancillary amendments to other existing regulations such as the JER, and the *Department of Defense Dictionary of Military and Associated Terms* will have to be updated to include the term "mission use."

Another consideration is which DOD agency should be responsible for drafting the regulation. A new regulation may be proposed and coordinated through several venues within the DOD. The Assistant Secretary of Defense for Networks and Network Integration (ASD/NII) is the DOD's Chief Information Officer (CIO). The ASD/NII CIO is charged with the responsibility for protecting the DOD's net-centric data.[98] The commander, U.S. Strategic Command (USSTRATCOM), is charged with overall responsibility for GIG

---

[96] For a comprehensive overview on the drafting and promulgation of regulations, as well as amending current regulations, see generally U.S. DEP'T OF DEF. INSTR. 5025.1, DOD DIRECTIVES PROGRAM (Oct. 28, 2007) [hereinafter DODI 5025.1].

[97] "Coordination with Unions Granted National Consultation Rights. DOD issuances containing substantive changes in conditions of employment, including personnel policies and practices and other bargaining unit matters that affect DOD civil service and non-appropriated fund employees, shall be forwarded to the appropriate unions for comment. . . ." *Id.* at Encl. 3, para. 7.h.

[98] DODD 8320.02, *supra* note 1, para. 5.1.1.3, directs ASD/NII CIO to:

> Develop the policies and procedures to protect Net-Centric data while enabling data sharing across security domains and with multi-national partners, other Federal Agencies, and State and local governments in accordance with law, policy, and security classification, in coordination with the Under Secretary of Defense For Intelligence and the Under Secretary of Defense For Policy.

operations and network defense in coordination with the CJCS and other combatant commands.[99]

Joint Task Force Global Network Operations (JTF-GNO), a standing joint task force under the command of USSTRATCOM, is organized to protect and defend the GIG.[100] Of the twelve doctrinally assigned tasks to JTF-GNO, the first is listed, "direct GIG NETOPS to ensure confidentiality, integrity, availability, and efficiency of the GIG infrastructure and information services."[101] In 2004, SECDEF ordered the services, combatant commands, and field agencies to comply with USSTRATCOM directives on securing the NIPRNet and SIPRNet.[102]

At a minimum, a regulation must comprehensively and clearly articulate proscribed conduct. This conduct should include limitations on access to the Internet for official purposes only. It should also prohibit DOD personnel from engaging in other risky activity such as transferring DOD information on personal thumb-drives. It must also prohibit the use of software to by-pass technical blocking of websites. Finally, the regulation must educate personnel as to the importance of safeguarding government information systems.

C. Hybrid Approach

Because of the length of time it may take for the DOD to promulgate a new regulation, independent commands may draft lawful orders or local regulations designed to reduce the amount of unofficial internet traffic. The only difficulty, other than those enunciated above,

---

[99] JOINT CHIEFS OF STAFF, JOINT PUB. 6-0, JOINT COMMUNICATIONS SYSTEM II-20 (20 Mar 2006) [hereinafter JP 6-0]. The joint doctrine states, "USSTRATCOM has overall responsibility for GIG operations and defense in coordination with CJCS and combatant commands. CDRUSSTRATCOM is responsible for coordinating and directing DOD-wide CND. USSTRATCOM through its JTF-GNO component executes the DOD mission." *Id*.

[100] *See, e.g*., *id*. at II-21-23; Cartwright, *supra* note 3, at 73.

[101] JP 6-0, *supra* note 99, at II-21.

[102] Memorandum from Secretary of Defense to Secretaries of the Military Departments et al., subject: Assignment and Delegation of Authority to Director, Defense Information Systems Agency (DISA) (18 Jun. 2008) (on file with USSTRATCOM).

> Upon receipt, the military departments will organize to execute global network operations and network defense under the Service Headquarters assigned to USSTRATCOM. Defense agencies will align their global network operations and network defense capabilities to provide USSTRATCOM visibility and insight into network status. Military departments and agencies will respond to USSTRATCOM's orders and direction, allowing USSTRATCOM to defend the Global Information Grid.

Id.

is that commands may have to rescind orders if these conflict with the regulation.

D. Support from Other Jurisdictions.

While the issuance of regulations or orders limiting access to the internet for official use is important, guidance from federal and state courts, as well as administrative decisions should to be considered in the enforcement of rules. For instance, in *Eliserio v. United Steelworkers of America, Local 310,*,[103] the Eighth Circuit Court of Appeals, in overruling a lower court's grant of summary judgment, found that the enforcement of rules against Internet misuse was arbitrary and could have occurred as a result of unlawful discrimination.[104]

In *Thompson v. State Civil Service Commission*,[105] the Pennsylvania Appellate Court upheld a county's decision to terminate an individual's government employment resulting from violations of the county's computer use policies. Although part of the decision to terminate employment occurred as a result of the individual accessing sites containing nudity, evidence that the individual "surfed" the Internet for at least twenty to thirty percent of the workday was also a reason.[106]

Decided by the Connecticut Supreme Court this year, *McCann v. Department of Environmental Protection*[107] is the most compelling and relevant case to the issue of reducing risk through regulations on social behavior. McCann began his employment with the state government in 1985.[108] Over time, the state issued McCann a laptop computer. In 1998, the state government issued a directive to its employees that government-issued computers were for "official and authorized business purposes."[109] The state informed its employees that

---

[103] Eliserio v. United Steelworkers of Am., Local 310, 398 F.3d 1071 (8th Cir. 2005).

[104] *Id.*, at 1079. While the court found that five separate complaints of Internet misuse were made against the appellant, it also found that the appellant was the only employee disciplined by Firestone, the employer, in an eight-year period. Moreover, the appellant was not notified of any infractions for the first four complaints. *Id.*

[105] Thompson v. State Civil Serv. Comm'n, 863 A.2d 180 (2004). Thompson also raised claims that his firing resulted from disparate treatment based on his union activities. *See* Thompson v. County of Beaver, 2006 U.S. Dist. LEXIS 807 (W.D. Pa. 2006).

[106] Thompson, 863 A.2d. at 183.

[107] McCann v. Dep't of Envtl. Protection, 952 A.2d 43 (Conn. 2008).

[108] *Id*.

[109] *Id*. The policy stated:

> All computer resources, including devices, programs, and data, electronic or hard copy, owned or leased by the State of Connecticut, and facilities of the State of Connecticut, which include but are not limited to the department,, shall only be used for legitimate and authorized business.

violations of the directive could result in discipline including job termination. In 2001 and 2002, McCann's supervisors reiterated the state directive's prohibitions against unofficial use and articulated a "zero tolerance" policy towards violators.

In 2002, the state discovered McCann had downloaded a K-Mart commercial software package onto his computer after he brought his computer to a repair center. A supervisor verbally reprimanded McCann after this discovery. During an "upgrade," in 2004, a Wal-Mart Internet commercial software program was found on a second state-issued computer used by McCann. Additionally, computer technologists discovered over 7,000 commercial web entries and a latent virus capable of degrading the state's computer networks. Later that year, a third state-issued laptop computer used by McCann was infected after he accessed several unofficial websites.

The state notified McCann it had decided to terminate McCann's employment based on numerous violations which placed the state's information systems at risk. Because McCann belonged to a collective bargaining unit, he was entitled to an administrative hearing. The arbitrator determined McCann was given enough notice that his conduct violated state rules and the employment termination was justified. Important to this article's advocacy was the arbitrator's determination that "unauthorized use of [McCann's] laptop …caused it to be infected with a virus that threatened the [s]tate's entire computer network, no small matter."[110]

McCann appealed to a state trial court, which ruled that the arbitrator failed to consider whether the state "offered McCann progressive discipline" and improperly excluded evidence of prior arbitrated agreements between the state and third parties who engaged in similar conduct, as well as the issue as to whether the state had disciplined employees for similar conduct.[111] The trial court determined that the evidence did not support the arbitrator's assessment of the risk to Connecticut's state computer systems caused by McCann's conduct.[112]

The Connecticut Supreme Court reversed the trial court's determination as to the arbitrator's failure to include disputed evidence but agreed that the arbitrator could not have made the risk determination based on the quantum of evidence the state provided.[113] However, the state supreme court upheld the arbitrator's decision to support McCann's employment termination and, more importantly, left open the prospect that conduct such as McCann's, which created vulnerabilities

[110] *Id*.
[111] McCann v. Connecticut, 2007 Conn. Super. LEXIS 1528 (Conn. Super. Ct. 2007).
[112] *Id*., at 8.
[113] *McCann*, 952 A.2d at 46.

to malicious code, could be the basis for disciplinary action.[114] This is precisely the construct which the DOD should adopt in enforcing regulations on unofficial Internet access.

V. CONCLUSION

One need only to look at the open source headlines and academic literature to understand the depth of the problem facing the DOD. These threats span a wide range, from the exfiltration of data to full scale denial of service attacks. As previously noted, a well-intentioned e-mail user within the DOD sent a link to an infected Internet game site. Two current nation-state adversaries, or their citizens, have repeatedly attempted to probe weak-points within the DOD and defense contractors.[115] At least three weeks prior to the Russian invasion of Georgia, Russian government agencies, or its citizens, independently stepped up cyber attacks on Georgia.[116] The potential for a terrorist strike against DOD information systems must be considered. The primary vector of attack will be through the Internet to the NIPRNet connection points. In essence, the threat to DOD information systems through cyberspace is very real, and a defense in depth is required to meet it. The defense should begin with social behavior, in essence, modifying the culture of permissive use, but include technical solutions as well.

It may be the case that commanders, judge advocates, and DOD personnel will view the implementation of a new regulation or series of orders designed to reduce the amount of Internet access traffic as a draconian measure. But, a decision to maintain the *status quo* and continue the permissive browsing of the Internet increases the risk of dangers ranging from exfiltration of data to a cyber "Pearl Harbor."

Understandably, the DOD and its commanders possessing UCMJ authority may want to resist measures which will likely be detrimental to morale. Certainly, a DOD-wide regulation should exempt deployed servicemembers, as well as personnel assigned to naval vessels operating at sea, because an alternative private means to access the Internet is unlikely to exist in austere locations. It is also understandable that commanders and departmental leaders will worry

---

[114] *Id*.

[115] *See, e.g.*, Julian E. Barnes, *Cyber-attack on Defense Department Computers Raises Concerns*, L.A. TIMES, Nov. 28, 2008, *available at* http://articles.latimes.com (analysis of Russian based cyber actions against DOD computers and the DOD's response); *see also U.S. Faces Cyber Threat from China*, SAN FRAN. CHRON., Nov. 28, 2008, at B-10, *available at* http://www.sfgate.com (articulating that the Chinese government may have over 250 "hacker teams" in its employ, targeting the DOD and defense contractors).

[116] *See*, Colonel Steven Korns & Major Joshua Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, 2008, at 60; *see also* John Markoff, *Before the Gunfire, Cyber Attacks*, N.Y. TIMES, Aug. 12, 2008, *available at* http://www.nytimes.com.

about recruiting and retention, both for uniformed personnel and the civilian workforce, and therefore not wish to create a policy limiting use. One solution may be for the acquisition of Internet connected computers in cafes and kiosks not connected to the .mil network. This solution, while outside the scope of this article, should be considered for later advocacy.

Social behavior, even in the armed services, cannot change without education and the development of policy. This is true, particularly, where the behavior to be limited is predicated on the assumption that no harm is caused by it. But the risk factors involved in unfettered internet access are too great to ignore. As a result, the DOD, or, in the absence of DOD action, responsible commanders with the support of their military legal community, should lay the groundwork for changing the paradigm.

Department of Defense

DIRECTIVE

NUMBER XXXX
[Month][Day], [Year]

Appendix 1

SUBJECT: Protection of DoD Information Systems

References: (a) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(b) DoD 5025.1-M, "DoD Directives System Procedures," current edition
(c) DoD 5500.7-R, Joint Ethics Regulation
(d) Chapter XX of title 10, United States Code

1. PURPOSE

This directive:

1.1. Establishes policy for eliminating the high level of unofficial use of Department of Defense (DoD) information systems, including systems used to access NIPR, SIPR, and other information systems.

1.2. Assigns responsibilities, and prescribes procedures for the Military Departments, Combatant Commands (COCOMS), and agencies regarding the use of DoD information systems and reporting of violations of this instruction.

1.3. This instruction does not supplant or replace other regulations, policies, and instructions governing the use of government property or the protection, handling, and use of classified information.

2. APPLICABILITY AND SCOPE

This directive applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.2. The Coast Guard when it is not operating as a Military Service in the Department of the Navy by agreement with the Department of Homeland Security; and the Commissioned Corps of the United States Public Health Service (USPHS) and the National Oceanic and Atmospheric Administration (NOAA), under agreements with the Department of Health and Human Services (hereafter referred to collectively as "Other Uniformed Services"). The term "Military Services," as used herein, refers to the Army, the Navy, the Air Force, the Marine Corps, and the Coast Guard; and their respective National Guard and Reserve components. The term "Uniformed Services" refers to the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Commissioned Corps of the USPHS, and the Commissioned Corps of the NOAA.

2.3. DoD-owned information systems (IS) and DoD controlled IS operated by contractors or other entities on behalf of the DoD that receive, process, store, or display, or transmit DoD information, regardless of classification or sensitivity, consistent with Reference (x).

3. DEFINITIONS

Terms used in this directive are defined in Enclosure 1.

4. P OLICY

Commensurate with the determination that Global Information Grid (GIG) is a war-fighting domain, it is DoD policy to protect the confidentiality, integrity, and availability of classified and unclassified,

but protected information, located on the GIG; and, to ensure the DoD components have complete access to the GIG per mission needs.

4.1. Internet traffic from DoD information systems has exponentially increased each year, creating challenges to unhindered GIG access. These challenges include risks posed by malicious code, as well as clogged pipelines. Furthermore, it is estimated that in FY 2007 at least 60% of all internet traffic originating from DoD information systems is accessed for unofficial (non-mission related) purposes.

4.2. DoD information systems are also placed at risk through the interface of private computer systems and information transfer technologies.

4.3. With the growth and increasing complexity of malicious code, unofficial use of the DoD information systems on the NIPRNet must be curbed to the maximum extent practicable.

4.4. Unofficial use includes, but is not limited to: accessing internet sites not directly related to military duty, "web-surfing," accessing non DoD web-mail from DoD information systems, and, the transfer of official files from DoD computers to non-DoD computers without the prior authorization of the first general officer in a chain of command or civilian equivalent. It also includes the use of privately owned (non-DoD appropriated) information transfer technologies such as personal thumb-drives, on DoD information systems.

4.5. This directive exempts DoD personnel deployed to the CENTCOM AOR or other deployed regions, DoD personnel aboard naval vessels or space vehicles as a local commander may direct.

5. RESPONSIBILITIES

5.1. The Commander, United States Strategic Command (CDRUSSTRATCOM) shall:

5.1.1. Draft and implement policy to limit the unofficial access to the internet through DoD information systems, consistent with the authority to operate and defend the GIG.

5.1.2. Test and evaluate scientific and technological methods for limiting unofficial access to the internet.

5.1.3. In cooperation with the Assistant Secretary of Defense for Networks and Network Integration, draft and develop enforceable policy to hold accountable DoD agencies and personnel who place the GIG at increased risk.

5.1.4. Monitor compliance with DoD policy limiting the use of access to internet for official purposes and make a quarterly report to OSD.

5.1.5. Develop policy for investigating Cyber intrusion and malicious code events.

5.1.6. Report to the Secretary of Defense the results of investigations, the availability of the GIG, and DoD compliance to this directive.

5.2. The Assistant Secretary of Defense for Networks and Network Integration (ASD/NII) shall:

5.1.1. In cooperation with USSTRATCOM, draft and implement policy to limit the unofficial access to the internet through DoD information systems.

5.1.2. In cooperation with USSTRATCOM, monitor compliance with this instruction

5.3 The General Counsel to the Office of the Secretary of Defense shall:

5.3.1. Modify DoD 5500.7-R, the *Joint Ethics Regulation*, to comport with this policy, and modify other departmental regulations as needed.

5.4. The Secretaries of the Military Departments shall:

5.4.1. Draft and implement punitive regulations to curb the use of DoD information systems to access the internet for unofficial purposes.

5.4.2. Modify existing service regulations to comport with this directive.

5.4.3. Educate members of their respective services as to the inherent dangers posed by internet access from DoD information systems.

5.4.4. Support CDRUSTRATCOM or the designated agency within the COCOM on all cyber intrusion investigations.

5.5. The Chairman of the Joint Chiefs of Staff shall:

5.5.1 Develop or modify joint doctrine and associated joint tactics, techniques, and procedures for the GIG and ensure the compatibility of the Chairman of the Joint Chiefs of Staff Instructions with this regulation.

5.6. Authorized Users of DoD information systems shall:

5.6.1. Access the internet only for mission related purposes as defined in enclosure (A)

5.6.1. Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

5.6.2. Use only DoD issued hardware and software for transferring electronic data.

5.6.3. Report suspected violations of DoD policy to an immediate supervisor, or if not practicable, to the next highest level.

6. EFFECTIVE DATE

This Instruction is effective immediately.

ENCLOSURE

DEFINITIONS

E1. Global Information Grid (GIG)

E1.1 The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

E1.2. Includes any system, equipment, software, or service that meets one or more of the following criteria: transmits information to, receives information from, routes information among, or interchanges information (DODD 8100.1).

E3. NIPRNET. Non-Classified Internet Protocol Router Network. A computer network for unclassified, but sensitive information supporting the DoD (JP 6-0).

E4. SIPRNET: Secret Internet Protocol Router Network. The worldwide SECRET-level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry (JP 6-0).

E5. UNOFFICIAL USE: Use which does not relate to the functions or necessities of DoD personnel or mission sets.

SECDEF GENERAL ORDER #1

From: Honorable Robert M. Gates
SECDEF
To:
Date:

1. Statement of Military Purpose and Necessity: The amount of DoD network resources devoted to internet and web traffic has increased exponentially over the past several years. Analysis indicates the majority of this traffic occurs for non official purposes. Not only does this drain resources better devoted to the DoD mission, but each connection exposes DoD networks to additional risk. The aggregate risk across DoD associated with this unnecessary exposure is substantial and unacceptable. DoD personnel have long operated on the assumption that using DoD network resources for personal purposes was cost free. It is not. DoD networks must be reclaimed for official use only.

2. Prohibited Activities:

a. Use of DoD computers and/or networks to access the internet and world wide web resources if the intended purpose of that access does not serve an official purpose. Examples of prohibited activities include recreational web surfing; personal use of social networking, gaming, and shopping sites; and the use of peer-to-peer networks.

b. The connection of any personal electronic device or media to DoD computing equipment.

c. Connection from DoD networks to any web-mail services hosted outside the .mil domain.

d. The transfer of non-public DoD files to home systems; the transfer of files from home system back to DoD systems.

3. Email: This order does not place additional restrictions on whether DoD personnel may send personal email from DoD-supplied email accounts beyond what is already regulated through DoD Directive 5500.7, dated 30 August 1991 (Joint Ethics Regulation), or prohibited by other laws and policy.

4. Punitive Order: Paragraph 2 of this General Order is punitive. Persons subject to the Uniform Code of Military Justice may be

punished thereunder. Civilians serving with or employed by the Armed Forces of the United States may face adverse administrative action for violation of this General Order.

5. Individual Duty: All persons subject to this General Order are charged with the individual duty to refrain from any use of DoD computers and networks in a manner that unnecessarily (other than an official purpose) connects them through the Internet/World Wide Web to non DoD systems. Questions regarding whether a particular use serves an official purpose should be referred, in advance, to a supervisor or commander.

6. Unit Commander Responsibility: Unit commanders and supervisors are charged to ensure all personnel are briefed on the prohibitions and requirements of this General Order. Commanders and supervisors are expected to implement monitoring programs to assist with enforcing this order.

7. Effective Date: This General Order is effective immediately.

8. Expiration: This general order will remain in effect until rescinded, waived, or modified.

9. Waiver Authority: Authority to waive or modify the prohibitions of this order is delegated to the first Flag, General Officer, or SES in an individual's chain of command or supervision. Any waiver or modification must be documented in writing and indicate the specific factors that justify the waiver or modification.

LEGAL PROPRIETY OF PROTECTING DEFENSE INDUSTRIAL BASE INFORMATION INFRASTRUCTURE

LIEUTENANT COLONEL TODD A. BROWN

Lieutenant Colonel Todd A. Brown (B.S., Birmingham-Southern College (1989); J.D., University of Alabama (1997), M.S., Air War College (2008)) serves as the Staff Judge Advocate, 187th Fighter Wing, Montgomery, Alabama. He is a member of the Alabama Bar.

I. INTRODUCTION

On 20 August 2009, in a joint announcement, the Secretary of the Air Force and the Chief of Staff of the Air Force announced how the Air Force would implement Department of Defense (DOD) cybersecurity efforts.[1] The announcement referred to an earlier decision by the Secretary of Defense to stand up a sub-unified command designated as the United States Cyber Command (USCYBERCOM).[2] In support of the DOD efforts, the Air Force has designated its Space Command as the lead Air Force major command to meet the cyberspace mission, and established the Twenty-Fourth Air Force (24 AF), recommending that it be the Air Force's service component to USCYBERCOM.[3] Among other things, the Air Force will give the commander of 24 AF authority over the Air Force network and will realign various new and existing commands under the purview of 24 AF.[4]

Regardless of how USCYBERCOM or the Air Force attempts to accomplish their missions, private industry will be involved. As with any other area in today's military, contractors and other private companies will likely be heavily involved in constructing the infrastructure the Air Force will use. The Air Force will likely use various vendors to provide computer and communications equipment it will use to accomplish its mission. In fact, the network connections between various components of the Air Force's, and even more broadly, the U.S. government's, are owned by private companies.

Obviously, the United States must protect the various parts of the information infrastructure used by its military. The more the military relies upon evolving information technologies, the more vulnerable it becomes to attacks on the supporting infrastructure. The Air Force is concerned about the number of onslaughts to these networks.[5] The main concern involves data manipulation, data loss, and espionage.[6] But, to what extent may the military, in general, and the Air Force in particular, become involved in protecting these networks, the data traveling on them, and the data residing on the various Air Force computer systems? Air Force Lieutenant General Charlie Croom,

---

[1] Memorandum from the Secretary of the Air Force & the Chief of Staff, U.S. Air Force, to all Airmen, subject: Air Force Cyberspace Mission Alignment (Aug. 20, 2009), [hereinafter Cyberspace Memo] *available at* https://newafpims.afnews.af.mil/shared/media/document/AFD-090821-046.pdf.
[2] *Id*.
[3] *Id*.
[4] *Id*.
[5] Jen DiMascio, *Cyber Experts See Need for Government Cooperation, Policy Changes*, DEFENSE DAILY, Oct. 25, 2007, http://www.defensedaily.com/publications/c4i/1051.html (last visited Sep. 13, 2009).
[6] *Id*.

director of the Defense Information Systems Agency, and the commander of the Joint Task Force for Global Network Operations, asserted in a panel discussion at the Association of the United States Army conference that numerous laws and regulations constrain the activities of the DOD in this area.[7] The question is as follows: what may the Air Force do, within the framework of these laws, to protect the information technology (IT) infrastructure on which it so heavily depends?

In answering this question, several issues must be resolved. First, is it appropriate for the Air Force to become involved in the protection of IT infrastructure? Specifically, what gives the Air Force the authority to protect this infrastructure when the majority of it is the property of members of private industry?

Second, does protecting private industry's infrastructure create some responsibility for the Air Force to protect the IT infrastructure of either members of the defense industrial base (DIB) or to protect current defense industry members in future endeavors? Could a potential future private sector DIB member successfully claim that current DIB contractors have an unfair competitive advantage when it comes to future contract awards?

Finally, given the answers to the above issues, what options exist for the Air Force? How can or should the Air Force proceed with protecting the IT infrastructure on which it has become so dependent?

After a review of commonly-used terms with regard to protecting the DIB's critical IT infrastructure in Section II, this article discusses applicable legal authorities in Section III. Section IV discusses practical concerns likely to be encountered by any Air Force effort to protect the infrastructure, particularly with regard to complications in the area of contracting for IT services or products. Section V addresses possible solutions to these concerns, and Section VI is the conclusion.

II. DEFINITIONS

Before discussing the issues above, this article must define a number of terms utilized throughout. Defining these terms is critical because, along with the laws and regulations which govern this area, these particular terms delineate the degree to which the DOD can protect privately owned critical IT infrastructure. Some of these terms have even reached term-of-art status and have moved away from their traditional, dictionary meanings.

[7] *Id*.

Critical Component is, for purposes of Title 50:

> such components, subsystems, systems, and related special tooling and test equipment essential to the production, repair, maintenance, or operation of weapon systems or other items of military equipment identified by the Secretary of Defense as being essential to the execution of the national security strategy of the United States. Components identified as critical by a National Security Assessment conducted pursuant to . . . 10 U.S.C. § 113(i) . . . or by a Presidential determination as a result of a petition filed under . . . 19 U.S.C. § 1862 . . . shall be designated as critical components . . . unless the President determines that the designation is unwarranted.[8]

Critical Industry for National Security is "any industry (or industry sector) identified pursuant to . . . 10 U.S.C. § 2503(6) . . . and such other industries or industry sectors as may be designated by the President as essential to provide industrial resources required for the execution of the national security strategy of the United States."[9]

Critical Infrastructure is "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[10] The definition applicable within Title 50, varies only slightly, but because some of the contractual requirements with regard to the Department of Defense (DOD) relate in some fashion to Title 50, its definition of Critical Infrastructure is also provided: "any systems and assets, whether physical or cyber-based, so vital to the United States that the degradation or destruction of such systems and assets would have a debilitating impact on national security and national public health or safety."[11]

---

[8] 50 U.S.C. app. § 2152(1) (2006).
[9] *Id*. § 2152(2).
[10] 42 U.S.C. § 5195c(e) (2006) This definition is also adopted by the Homeland Security Act of 2002, as codified in Title 6, United States Code, 6 U.S.C. §101(4), and the Directive on Critical Infrastructure Identification, Prioritization, and Protection, 39 WEEKLY COMP. PRES. DOC. 1816 (Dec. 22, 2003) para. 6(e) [hereinafter HSPD-7].
[11] 50 U.S.C. app. § 2152(3) (2006).

Critical Infrastructure Information is

> information not customarily in the public domain and related to the security of critical infrastructure or protected systems (A) actual, potential, or threatened interference with . . . critical infrastructure or protected systems by either physical or computer-based attack . . . that violates Federal, State, or local law, harms interstate commerce of the United States, . . . or threatens public health or safety; (B) the ability of any critical infrastructure or protected system to resist such interference . . . ; or, (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems . . . .[12]

Critical Technology is "any technology that is included in 1 or more of the plans submitted pursuant to [42 U.S.C. § 6681 or 10 U.S.C. § 2508] (unless subsequently deleted), or such other emerging or dual use technology as may be designated by the President."[13]

Critical Technology Item is "materials directly employing, derived from, or utilizing a critical technology."[14]

Defense Contractor is "any person who enters into a contract with the United States (A) to furnish materials, industrial resources, or a critical technology for the national defense; or (B) to perform services for the national defense."[15]

Domestic Defense Industrial Base is "domestic sources which are providing, or which would be reasonably expected to provide, materials or services to meet national defense requirements during peacetime, graduated mobilization, national emergency, or war."[16] The DOD elaborates on this definition in its sector-specific plan. That plan defines the defense industrial base as the "DoD, the U.S. Government, and the private sector worldwide industrial complex with capabilities to perform research and development (R&D), design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements."[17]

---

[12] 6 U.S.C. § 131(3) (2006).
[13] 50 U.S.C. app. § 2152(4) (2006).
[14] *Id.* § 2152(5).
[15] *Id.* § 2152(6).
[16] *Id.* § 2152(7).
[17] U.S. DEP'T OF DEF., DEFENSE INDUSTRIAL BASE: CRITICAL INFRASTRUCTURE AND KEY RESOURCES SECTOR-SPECIFIC PLAN AS INPUT TO THE NATIONAL INFRASTRUCTURE

Domestic Source is

> a business concern (A) that performs in the United States or Canada substantially all of the research and development, engineering, manufacturing, and production activities required . . . under a contract with the United States relating to a critical component or a critical technology item; and (B) that procures from business concerns described in subparagraph (A) substantially all of any components and assemblies required . . . .[18]

Essential Weapon System is "a major weapon system and other items of military equipment identified by the Secretary of Defense as being essential to the execution of the national security strategy of the United States."[19]

Federal Departments and Agencies include the following executive departments: Department of State, Department of the Treasury, DOD, Department of Justice, Department of the Interior, Department of Agriculture, Department of Commerce, Department of Labor, Department of Health and Human Services, Department of Housing and Urban Development, Department of Transportation, Department of Energy, Department of Education, Department of Veterans Affairs, and, Department of Homeland Security (DHS).[20] This definition also includes independent establishments as defined in 5 U.S.C. § 104(1), government corporations as defined in 5 U.S.C. 103(1), and the United States Postal Service.[21]

Foreign Source is "a business entity other than a 'domestic source.'"[22]

Full and Open Competition "means that all responsible sources are permitted to submit sealed bids or competitive proposals on the procurement."[23]

PROTECTION PLAN 4 (2007) [hereinafter DIB SSP], *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA469334&Location=U2&doc=GetTRDoc.pdf.
[18] 50 U.S.C. app. § 2152(8) (2006).
[19] *Id.* § 2152(9).
[20] 5 U.S.C. § 101 (2006).
[21] HSPD-7, *supra* note 10, para. 6(d).
[22] 50 U.S.C. app. § 2152(11) (2006).
[23] 41 U.S.C. § 403(6) (2006).

Industrial Resources are "materials, services, processes, or manufacturing equipment . . . needed to establish or maintain an efficient and modern national defense industrial capacity."[24]

Key Resources are "publicly or privately controlled resources essential to the minimal operations of the economy and government."[25]

National Defense is defined in Title 50 as

> programs for military and energy production or construction, military assistance to any foreign nation, stockpiling, space, and any directly related activity. Such term includes emergency preparedness activities conducted pursuant to title VI of The Robert T. Stafford Disaster Relief and Emergency Assistance Act and critical infrastructure protection and restoration.[26]

Organizational Conflict of Interest is when "because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage."[27]

Sector-Specific Agency is a U.S. "department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category."[28]

Small Business Concern is "a business concern that meets the requirements of section 3(a) of the Small Business Act and the regulations promulgated pursuant to that section . . . ."[29]

Small business concern owned and controlled by socially and economically disadvantaged individuals is

> a small business concern (i) which is at least 51 per centum owned by one or more socially and economically

[24] 50 U.S.C. app. § 2152(12) (2006).
[25] 6 U.S.C. § 101(9) (2006). This definition is also adopted by HSPD-7, *supra* note 10.
[26] 50 U.S.C. app. § 2152(14) (2006).
[27] GEN. SERVS. ADMIN. ET AL, FEDERAL ACQUISITION REG. pt. 2.101 (Jul. 2007) [hereinafter FAR]; see also *id.* at subpart 9.5.
[28] HSPD-7, *supra* note 10, para. 6(g). According to HSPD-7, Sector-Specific Agencies conduct their activities with guidance provided by the Secretary of Homeland Security. *Id.*
[29] 50 U.S.C. app. § 2152(17) (2006).

> disadvantaged individuals . . . ; and (ii) whose management and daily business operations are controlled by one or more of such individuals. The contractor shall presume that socially and economically disadvantaged individuals include Black Americans, Hispanic Americans, Native Americans, Asian Pacific Americans, and other minorities, or any other individual found to be disadvantaged by the Administration pursuant to section 8(a) of the Small Business Act.[30]
>
> Source Selection Information is
>
> any of the following information that is prepared for use by an agency for the purpose of evaluating a bid or proposal to enter into an agency procurement contract, if that information has not been previously made available to the public or disclosed publicly: (1) Bid prices submitted in response to an agency invitation for bids, or lists of those bid prices before bid opening; (2) Proposed costs or prices submitted in response to an agency solicitation, or lists of those proposed costs or prices; (3) Source selection plans; (4) Technical evaluation plans; (5) Technical evaluations of proposals; (6) Cost or price evaluations of proposals; (7) Competitive range determinations that identify proposals that have a reasonable chance of being selected for award of a contract; (8) Rankings of bids, proposals, or competitors; (9) Reports and evaluations of source selection panels, boards, or advisory councils; or (10) Other information marked as "Source Selection Information" . . . .[31]
>
> Unfair Competitive Advantage is
>
> where a contractor competing for award of any Federal contract possesses (1) Proprietary information that was obtained from a Government official without proper authorization; or (2) Source selection information that is relevant to the contract but is not available to all competitors, and such information would assist that contractor in obtaining the contract.[32]

[30] 15 U.S.C. § 637(d)(3)(C) (2006). This definition is used in Title 50 U.S.C. 50 U.S.C. app. § 2152(18) (2006).
[31] FAR, *supra* note 27, at 2.101.
[32] *Id*. at 9.505(b).

These terms, and their specific meanings, significantly influence the degree of protection a government entity such as the DOD may provide to privately owned portions of the critical IT infrastructure. In some cases, the terms themselves may operate to constrain DOD activity to the same level as the laws and regulations discussed herein.

III AUTHORITY FOR THE AIR FORCE TO PROTECT THE INFORMATION INFRASTRUCTURE OF THE DEFENSE INDUSTRIAL BASE

The United States Constitution established the authority for the federal government to, among other things, provide for the common defense.[33] Article I, Section 8 (the Commerce Clause), empowers Congress to regulate commerce with foreign nations and among the states.[34]

Congress has acted upon that authority with regards to the topic of protecting the IT infrastructure of the DIB. In 2002, it enacted the Homeland Security Act of 2002.[35] This act was codified as Title 6 of the United States Code.

The executive branch joined the legislative branch by becoming increasingly involved in attempting to protect critical IT infrastructure. In particular, as it relates to the protection of infrastructure following the September 11, 2001, terrorist attacks, the President issued numerous directives, executive orders, and national strategies addressing these issues.

From the very beginning, the Founding Fathers of this country recognized the need for providing for the common defense, and included that very provision within the first paragraph of the Constitution.[36] The Constitution clearly gives the government the authority to protect its own infrastructure. By way of extension, it gives components of the government, including the DOD, the authority to protect the infrastructure that it owns. No one doubts the Air Force's authority to defend its bases, aircraft, personnel, equipment, or even its technology infrastructure. In fact, in its doctrine, the DOD addresses the computer network defense of "unauthorized activity within DOD information systems and computer networks."[37] But, what about the Air Force's authority to protect resources that it does not own? Can the Air Force protect parts of the nation's IT infrastructure that it uses but does not own?

---

[33] U.S. CONST. pmbl.
[34] U.S. CONST. art. I, § 8.
[35] Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 202, 221, 116 Stat. 2135 (2002).
[36] U.S. CONST. pmbl.
[37] JOINT CHIEFS OF STAFF, JOINT PUB. 3-13, INFORMATION OPERATIONS, at II-5 (13 Feb. 2006).

The Constitution, in creating the executive branch, empowered it to defend the nation.[38] It designated the President, as the embodiment of the executive branch, as the Commander in Chief of the military.[39] However, the list of powers granted to the President in carrying out his duties as Commander in Chief is devoid of any authority to defend private industry.[40] Thus, by extension, the Air Force cannot protect the infrastructure of the private sector unilaterally.[41] In fact, the executive branch has long recognized that private sector participation in the government's protection of its infrastructure is clearly voluntary.[42] This poses a problem because the private sector controls ninety percent of the nation's critical infrastructure.[43]

However, the Constitution authorizes Congress to regulate interstate and foreign commerce.[44] That authority has led, most recently, to the passage of the Homeland Security Act of 2002. By passing the Homeland Security Act, Congress empowered the DHS as the lead agent for, among other things, the protection of the nation's critical infrastructure.[45] In fact, one of the rationales for consolidating many different agencies into the DHS in 2002 was the desire to grant authority to one specific department that alone would have responsibility for securing critical infrastructure.[46]

In the Homeland Security Act, Congress authorized the President and the Secretary of Homeland Security to designate critical infrastructure protection programs.[47] Within that authority, the President issued a number of directives designating critical infrastructure protection programs and describing responsibilities therein.

The President designated the DHS to play the central role in implementing the *National Strategy to Secure Cyberspace* in May 2003.[48] The DHS also serves as the primary focal point-of-contact for

---

[38] U.S. CONST. art. III, § 2, cl. 1.
[39] *Id*.
[40] *Id*.
[41] *See* Colonel Allen F. Woodhouse, Information Assurance: A National Policy Struggling with Implementation 4 (Apr. 10, 2001) (unpublished U.S. Army War College Strategy Research Project), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD-ADA390580&Location-US&doc-GetTRDoc.pdf.
[42] Michael J. O'Neil & James X. Dempsey, *Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry*, 12 DEPAUL BUS. L.J. 97, 101 (2000); DIB SSP, *supra* note 17, at 4.
[43] Joe D. Whitley et al., *Homeland Security, Law, and Policy through the Lens of Critical Infrastructure and Key Asset Protection*, 47 JURIMETRICS J. 259, 262 n.15 (2007).
[44] U.S. CONST art. I, § 8, cl. 3.
[45] 6 U.S.C. §§ 111, 112, 131, 132 (2006).
[46] 148 CONG. REC. H5633 (daily ed. Jul. 25, 2002) (statement of Rep. Thornberry).
[47] 6 U.S.C. § 132 (2006).
[48] THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 54 (2003),

state and local governments and the private sector on cyberspace security issues.[49] Additionally, in concert with the White House, the DHS coordinates and supports non-federal tasks recommended in the *National Strategy to Secure Cyberspace*.[50]

A. Homeland Security Presidential Directive 7

On 17 December 2003, the President issued Homeland Security Presidential Directive 7 (HSPD-7). This plan superseded Presidential Decision Directive/NSC-63 of 22 May 1998.[51] The purpose of the directive was to establish a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources.[52] Interestingly, the directive specifically focused on protecting critical infrastructure and key resources "from terrorist attacks."[53] HSPD-7 specifically excludes non-terrorist attacks on critical infrastructure, leaving to all federal departments and agencies the reduction of "consequences of catastrophic failures not caused by terrorism."[54]

With regard to terrorist threats, HSPD-7 establishes, as policy, the enhancement of protecting critical infrastructure and key resources from acts that could

> (1) cause catastrophic health effects or mass casualties comparable to those caused from use of a weapon of mass destruction; (2) impair Federal departments' and agencies' abilities to perform essential missions, or ensure the public's health and safety; (3) undermine State and local governments' capacities to maintain order and deliver minimum essential public services; (4) damage the private sector's ability to ensure the orderly functioning of the economy and deliver essential services; (5) have negative impact upon the economy; or, (6) undermine the public's morale and confidence in national economic and political institutions.[55]

---

available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.
[49] *Id*.
[50] *Id*.
[51] HSPD-7, *supra* note 10, at para. 37.
[52] *Id*. para. 1.
[53] *Id*.
[54] *Id*. para. (22)(i).
[55] *Id*. para. 7.

The overall responsibility for the protection of the nation's critical infrastructure falls to the Secretary of Homeland Security.[56] Recognizing that certain other departments have special expertise within infrastructure sectors, however, HSPD-7 assigns a limited number of sector-specific agencies.[57]

Among the sector-specific agencies is the DOD, with responsibility for the DIB.[58] What are the DOD's responsibilities with regard to the DIB? With guidance provided by the Secretary for Homeland Security, the DOD shall: (1) *collaborate* with Federal, State, and local governments, departments, and agencies, and the private sector; (2) conduct or facilitate *vulnerability assessments* of the sector; and, (3) *encourage risk management strategies* to protect or mitigate effects of any attack on the DIB.[59]

Two things are of note with regard to these responsibilities. First, the guidance within this area comes from the Secretary for Homeland Security, not the Secretary of Defense. Second, the DOD is given only limited authority within the DIB sector. Specifically, while charged with collaborating within the sector, assessing vulnerabilities, and encouraging risk management strategies, the DOD is not authorized to "protect" the DIB. This does not appear to be an oversight, as HSPD-7 specifically defines the term "protect." As used within HSPD-7, "protect" and "secure" are defined as "reducing the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks."[60] Thus, the fact that the President could have, but did not, authorize the DOD to actually protect the DIB reflects an intentional limitation of DOD action. Also of note, HSPD-7 does not authorize the DHS to actually protect the DIB, either. HSPD-7 does grant the DHS the power to "coordinate protection activities" for an enumerated number of sectors, none of which include the DIB.[61] Thus, it appears that, between the Departments of Homeland Security and Defense, the extent of the federal government's involvement with regard to the DIB is purely an assistance role.

HSPD-7 does authorize the DHS to coordinate protection activities for the IT and telecommunications sectors.[62] Thus, one must explore the relationship between the IT and telecommunications sectors generally and with regard to those same sectors owned by the private sector. For example, the DOD owns certain IT and telecommunications resources and has the right to protect them. Others belong to other

[56] *Id*. paras. 12-17.
[57] *Id*. para. 18.
[58] *Id*. para. 18(g).
[59] *Id*. para. 19 (emphasis added).
[60] *Id*. para. 6(h).
[61] *Id*. para. 15.
[62] *Id*. para. 15.

government and private sectors, which the DHS is authorized to protect. Some of these resources belong to private sector DIB partners for which the DOD is designated as the sector-specific agency. The question becomes what, if any, government agency is authorized to protect these infrastructures where these resources overlap?

Overlap exists in other areas within HSPD-7. For example, it tasks the Department of Commerce with improving cyber system technology which, at times, seems to also involve parts of the DIB.[63] The implementation of HSPD-7 directs the Secretary for Homeland Security to produce a comprehensive National Plan for Critical Infrastructure and Key Resources Protection.[64] It also directs all federal agencies to submit protection plans by July 2004.[65]

In response to this directive, in June 2006, the DHS published the National Infrastructure Protection Plan (NIPP). The NIPP purports to meet the requirements set forth in HSPD-7 and provide an overarching approach for integrating the many critical infrastructure and key resource protection initiatives into a single plan.[66] It also asserts that it "sets forth a comprehensive risk management framework" and "clearly define[s the] roles and responsibilities for the [DHS]," along with sector-specific agency such as the DOD "and private partners implementing the NIPP."[67]

B. National Infrastructure Protection Plan

The NIPP recognizes, as delineated within HSPD-7, that certain departments have expertise within various infrastructure sectors. Thus, the NIPP intends to implement procedures recognizing the sector-specific nature of critical infrastructure and key resource protection.[68] Consistent with HSPD-7, the NIPP defines the roles and responsibilities of the sector-specific agencies established in HSPD-7.[69] As in HSPD-7, the responsibility for the DIB sector falls to the DOD.[70] Thus, the DOD is tasked with collaborating with the private sector and encouraging development of appropriate information-sharing and analysis mechanisms within the DIB.[71] Specifically, the DOD should establish coordinating mechanisms within the DIB to "facilitate sharing of information on physical and cyber threats, vulnerabilities, incidents,

[63] *Id*. para. 22(c).
[64] *Id*. para. 27.
[65] *Id*. para. 34.
[66] U.S. DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN (2009) [hereinafter NIPP], *available at* http://www.fas.org/irp/agency/dhs/nipp.pdf.
[67] *Id*. at i-ii.
[68] *Id*. at 11-12.
[69] *Id*. at 18-21.
[70] *Id*. at 19.
[71] *Id*. at 18.

recommended protective measures, and security-related best practices."[72] In addition, the DOD should encourage "*voluntary* security-related information sharing, where possible, among private entities within the [DIB], as well as among public and private entities."[73] The DOD, working in collaboration with security partners within the DIB, is also responsible for developing and submitting a sector-specific plan and providing performance feedback, related to the DIB sector, to the DHS for assessment of any gaps between critical infrastructure and key resource sectors.[74] The DOD is required to provide an annual report to the Secretary of Homeland Security on its efforts to identify, prioritize, and coordinate critical infrastructure and key resource protection within the DIB, including an outline of protection requirements and budget projections as a component of its annual budget submission to the Office of Management and Budget.[75] It is worth noting again that guidance within this area comes from the Secretary for Homeland Security, not the Secretary of Defense. Within the NIPP construct, the DOD operates merely in a supporting role to the DHS.

Finally, the NIPP lists a number of additional responsibilities for the DOD. Those include:

(1) identifying, prioritizing, and coordinating protection of DIB critical infrastructure and key resources, focusing particularly upon infrastructures and resources that could be exploited in such as a way as to cause catastrophic health effects or mass casualties comparable to those produced by a weapon of mass destruction;

(2) managing the overall process for building security partnerships and leveraging critical infrastructure and key resource security expertise, relationships, and resources within the DIB, including sector-level oversight and support of the sector partnership model described in chapter 4 of the NIPP;

(3) coordinating, facilitating, and supporting comprehensive risk assessment and management programs for high-risk critical infrastructure and key resources, identifying protection priorities, and incorporating critical infrastructure and key resource protection activities as a key component of the all-hazards approach to domestic incident management within the DIB;

(4) facilitating the sharing of real-time incident notification, as well as critical infrastructure and key resource protection best practices and processes, and risk assessment methodologies and tools within the DIB;

---

[72] *Id*.
[73] *Id*. (emphasis added).
[74] *Id*. at 17-18.
[75] *Id*. at 18.

(5) promoting critical infrastructure and key resource protection education, training, and awareness in coordination with State, local, tribal, and private sector partners within the DIB;

(6) informing the annual Federal budget process based on critical infrastructure and key resource risk and protection needs in coordination with security partners and allocating protection resources;

(7) monitoring performance measures for DIB critical infrastructure and key resource protection and NIPP implementation activities to enable continuous improvement, and reporting progress and gaps to DHS;

(9) contributing to the annual National Critical Infrastructure Protection Research and Development (NCIP R&D) Plan;

(10) identifying and recommending appropriate strategies to encourage private sector participation;

(11) supporting data calls initiated by the DHS to (a) populate the National Asset Database (NADB); (b) enable national-level risk assessment; and, (c) inform national-level resource allocation;

(12) supporting protocols for the Protected Critical Infrastructure Information (PCII) Program;

(12) working with the DHS to develop, evaluate, validate, or modify risk assessment tools related to the DIB;

(13) supporting sector-level dependency, interdependency, consequence, and other analysis as required;

(14) coordinating sector-level participation in the National Exercise Program, Homeland Security Exercise and Evaluation Program (HSEEP), and other activities within the DIB;

(15) assisting DIB security partners in their efforts to organize and conduct protection and continuity-of-operations planning, and elevate awareness and understanding of threats and vulnerabilities to their assets, systems, and networks; and, identify and promote effective critical infrastructure and key resource protection practices and methodologies specific to the DIB;

(16) identifying and implementing plans and processes for increases in protective measures that align to all-hazards warnings, specific threat vectors as appropriate, and each level of the Homeland Security Advisory System;

(17) understanding and mitigating cyber risk by developing or encouraging appropriate protective measures, information-sharing mechanisms, and emergency recovery plans for cyber assets, systems, and networks within the DIB and interdependent sectors; and,

(18) supporting efforts of the Departments of Homeland Security and State to integrate national critical infrastructure and key resource protection programs into the international and global markets, and address relevant dependency, interdependency, and cross-border issues.[76]

Again, "[p]rivate sector participation in executing the NIPP is voluntary."[77] In essence, then, according to the requirements set forth in the NIPP, the DOD simply stands ready to support and assist others in the protection of privately owned critical infrastructure. The DHS maintains an inventory of critical infrastructures and key resources.[78] Information included in that inventory related to the DIB comes from inventories conducted by the DOD or voluntarily submitted directly from DIB security partners.[79] Although the NIPP does not specifically address the various components that make up the inventory, it clearly places a great deal of importance upon the cyber dimension.[80] Those cyber systems include positioning, navigation, and timing services utilized heavily by the military and the DIB.[81]

C. Defense Industrial Base Critical Infrastructure and Key Resources Sector-Specific Plan

Consistent with the requirement set forth in the NIPP, the DOD published its sector-specific plan in May 2007. The plan—fully titled Defense Industrial Base Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan—resulted from extensive collaboration between the DOD, interagency partners, and representatives of the private sector, from the smallest proprietors to Fortune 500 corporations.[82] The plan recognizes that the DIB is an unmatched element of national power that differentiates the United States from potential opponents.[83] But, once again, the plan reminds us that private sector DIB participation in the critical infrastructure and key resource protection process is voluntary.[84]

The DIB plan claims to address the critical infrastructure protection efforts mandated by HSPD-7, which involves terrorism-related threats.[85] This contrasts with the Defense Critical Infrastructure Program (DCIP), dated 19 August 2005, which addresses DIB assets

[76] *Id*. at 18-20.
[77] DIB SSP, *supra* note 17, at 4.
[78] NIPP, *supra* note 66, at 29-30.
[79] *Id*. at 30-31.
[80] *Id*. at 32.
[81] *Id*.
[82] DIB SSP, *supra* note 17, at i.
[83] *Id*.
[84] *Id*. at i, 4.
[85] *Id*. at 3

owned by the private sector and DOD-owned elements of the DIB.[86] Thus, the DIB plan purports to focus on the privately owned and operated efforts at DIB facilities rather than on the small fraction of DIB facilities owned by the DOD.[87] Likewise, the plan specifically excludes commercial infrastructures, such as power, communications, transportation, and other utilities that support DOD efforts.[88] These infrastructures are covered by other sector-specific agencies and departments, such as the Departments of Energy, Commerce, and Transportation.[89] Notwithstanding the plan's claim that it only addresses private-sector DIB critical infrastructure and key resource as directed by HSPD-7 (i.e., from an anti-terrorism perspective only), the plan does address threats from nation states, national and transnational criminal entities, accidents, and acts of nature within its risk assessment section.[90] This risk assessment strategy is more expansive than either HSPD-7 or the NIPP calls for and likely exceeds the scope of what the DIB plan was designed to accomplish.

Furthermore, the DIB plan is fairly general. It divides the DIB into segments, sub-segments, and commodities.[91] Those segments and sub-segments include, among other things, IT; command, control, computers and intelligence (C3I); information security; and various pieces of electronic equipment like optics, guidance systems, Global Position System (GPS) receivers, and software.[92] After identifying these various elements of the DIB, the plan falls somewhat short in identifying exactly what efforts the DOD will take to coordinate the protection of those assets with the private sector. The plan avoids any real effort to define its plan to coordinate the protection of these assets. Instead it basically restates the edicts of HSPD-7 and the NIPP and points out that the DOD will work with the DHS to identify overlaps and gaps in responsibility with other sector-specific agencies with regard to DIB assets that belong to other sectors.[93]

One area where the DIB plan appears to be particularly inadequate is its reference to cyber security risks. In fact, the plan clearly states that although "cyber security is an issue that could affect any facility, DoD does not perform network- or system-level assessments."[94] Instead, the plan points out that DIB assets are primarily owned by the private sector; and that (1) there are no regulatory requirements for conducting formal risk assessments,

---

[86] *Id*.
[87] *Id*. at 5.
[88] *Id*.
[89] *Id*.; HSPD-7, *supra* note 10, paras. 18(d), 22(c), 22(h).
[90] DIB SSP, *supra* note 17, at 17-20.
[91] *Id*. at 5-6.
[92] *Id*.
[93] *Id*. at 13.
[94] *Id*. at 17.

(2) large companies conduct their own risk assessments as part of prudent business practices, and (3) the DOD *aims to* ensure awareness and risk management best practices throughout the DIB.[95] This stance is far from visionary. What about smaller private-sector DIB members? How exactly does the DOD *aim to* ensure awareness across the sector? The plan does not address these questions.

The DIB plan also fails to fully comply with the HSPD-7 directive that the tasked departments share information about cyber threats.[96] The NIPP suggests a networked approach to information-sharing.[97] "NIPP implementation [relies] greatly on critical infrastructure information provided by the private sector."[98] In fact, Congress specifically enacted an information analysis and infrastructure protection program, created a Directorate for Information Analysis and Infrastructure Protection within the DHS, and established an Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection, an Assistant Secretary for Information Analysis, and an Assistant Secretary for Infrastructure Protection, all to be appointed by the President.[99]

How does the DIB plan address information sharing? Rather than coming up with some innovative mechanism to coordinate information-sharing, the plan states that DOD "relies on private industry organizations to exchange information on DIB infrastructure."[100] The plan seems to relegate responsibility for these efforts back to the DHS. Again, rather than taking the issue head on, DOD seems to take on only a supporting role to the DHS in its efforts to address cyber incidents, conduct vulnerability assessments, develop risk management strategies, and facilitate information-sharing.[101] Even where it is specific about information collection activities, the DIB plan is superficial. The plan calls for such data collection efforts as questionnaires and Internet information sources.[102] Certainly, an adequate effort to collect critical infrastructure and key resource data cannot be successfully completed using Google or Yahoo search engines.

Notwithstanding the vital national security importance of information-sharing to a successful critical infrastructure and key resource protection effort, the simple fact that private sector participation is voluntary presents the most substantial hurdle within information-sharing efforts.[103] Because much of the information in the

---

[95] *Id*.
[96] HSPD-7, *supra* note 10, para. 25(b).
[97] NIPP, *supra* note 66, at 56.
[98] *Id*. at 66.
[99] 6 U.S.C. § 121 (2006).
[100] DIB SSP, *supra* note 17, at 7.
[101] *Id*. at 8
[102] *Id*. at 14.
[103] NIPP, *supra* note 66, at 58.

possession of private sector is either sensitive business or security information that could cause serious damage to private industry, the economy, public safety, or public security, unauthorized disclosure or access to it is a critically important risk.[104] Accordingly, Congress imposed on the government a statutory responsibility to safeguard the information related to critical infrastructure and key resource activities.[105] This information assurance guarantee may be the incentive required to urge the DIB to share critical infrastructure and critical resource information. The next section explains why.

D. Federal Statutory Provisions

First, the Homeland Security Act of 2002 requires that any information collected pursuant to the DHS' information analysis and infrastructure protection efforts be "protected from unauthorized disclosure and handled and used only for the performance of official duties."[106] Further, the DHS must ensure that

> any intelligence information [collected pursuant to this program] is shared, retained, and disseminated consistent with the authority of the Director of Central Intelligence to protect intelligence sources and methods under the National Security Act of 1947 (50 U.S.C. 401 *et seq.*) and related procedures and, as appropriate, similar authorities of the Attorney General concerning sensitive law enforcement information.[107]

Next, the DHS has established the Protected Critical Infrastructure Information (PCII) Program, which was authorized by the Critical Infrastructure Information Act of 2002 (CII Act).[108] The CII Act enables the DHS to "collaborate effectively to protect America's critical infrastructure, eighty-five percent of which is in the private sector's hands."[109] The CII Act gives the DHS the authority to accept, store, and maintain critical infrastructure and key resource information from various sources, including the public, owners and operators of critical infrastructure, and State, local, and tribal governments. The CII Act provides a major benefit to defense contractors and a significant incentive for submitting critical infrastructure. It allows for information

[104] *Id*. at 66.
[105] 6 U.S.C. § 121(d)(12) (2006).
[106] *Id*. § 121(d)(12)(A).
[107] *Id*. § 121(d)(12)(B).
[108] *Id*. §§ 131-134.
[109] Procedures for Handling Critical Infrastructure Information, 71 Fed. Reg. 52,262 (Sept. 1, 2006) (to be codified at 6 C.F.R. pt 29).

collection while limiting public disclosure of sensitive information under the Freedom of Information Act (FOIA), and other laws, rules, and processes. Specifically, critical infrastructure information, including the identity of the submitting person or entity, which is voluntarily provided to the DHS is:

(1) protected from disclosure under FOIA;[110]

(2) not subject to agency rules or judicial doctrine regarding *ex parte* communication with a decision-making official;[111]

(3) protected from being used directly by Federal, State, or local authorities, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;[112]

(4) protected from use or disclosure by any officer or employee of the United States for any other purpose than (a) in furtherance of an investigation or prosecution of a criminal act, or (b) to Congress, or its representatives, or the Comptroller General, or its representatives, without written consent;[113]

(5) if provided to a state or local government, protected from disclosure to state or local laws requiring disclosure if information or records, to any party by the state or local government without written consent of the submitter; or, for any purpose other than protecting critical infrastructure or in furtherance of investigating or prosecuting a criminal act;[114] and,

(6) not to be considered a waiver of any applicable privilege or protection provided under the law, to include trade secret protection.[115] Furthermore, federal officers or employees who discloses this information in an unauthorized manner subjects themselves to imprisonment of up to one year and civil and criminal fines and must be removed from office or employment.[116]

PCII may be shared with authorized government agencies for purposes of securing critical infrastructure.[117] It should be used for analysis, warning, study, infrastructure, and recovery or reconstitution.[118] Other permissible uses include to generate advisories, alerts, and warnings to parties, including the private sector; however, these statements cannot contain sensitive information provided by the submitter.[119] The PCII Program Office is responsible for managing the PCII program, including developing methodologies for handling PCII,

[110] *Id*. § 133(a)(1)(A).
[111] *Id*. § 133(a)(1)(B).
[112] *Id*. § 133(a)(1)(C).
[113] *Id*. § 133(a)(1)(D).
[114] *Id*. § 133(a)(1)(E).
[115] *Id*. § 133(a)(1)(F).
[116] *Id*. § 133(F).
[117] *Id*. §§ 133(a)(1), 143, 145.
[118] *Id*. § 133(a)(1).
[119] *Id*. § 133(e).

raising awareness of information-sharing, and assuring information is safeguarded.[120]

E. Critical Infrastructure Information Sharing Issues

Why is the sharing of critical infrastructure information so important? If the Air Force is going to become involved in protecting the critical IT infrastructure of the DIB, it will be primarily protecting information and its transmission, as opposed to facilities, equipment, etc. For example, the Air Force cannot possibly protect every network cable, telephone line, or microwave tower transmitting DIB-related data. Thus, the DIB security partners must focus on protecting and securing the data that travels along those routes. As it relates to equipment most vulnerable to attacks by hackers and the like, the means for protecting and securing that equipment will most likely involve information as to how the equipment is designed and operates. This information may be classified and is certain to contain trade secrets of one form or another. Thus, how the private sector DIB partners choose to pass that information along to the Air Force, and how the Air Force is able to assure that information remains safeguarded, is crucial.

From the perspective of the private sector, what information remains safeguarded and to what extent it is protected might be different than the U.S. government's point of view, and the DOD in particular. For example, assume a DIB partner provides information regarding the inner workings of a router, which it uses to support a DOD mission, to the DOD for purposes of protecting it and its associated critical infrastructure. Also assume that the information is of a sensitive, but unclassified, business nature—no other router manufacturer uses the same technology and it is extremely valuable. Obviously, it would be very important to the contractor that the DOD safeguard that information and prevent its disclosure to its competitors.

Then, assume a person or entity inquires into some area of DOD records, either under the auspices of FOIA or related to some civil law suit. The civil suit might even be a legitimate suit related to a contract awarded to the initial DIB partner. What prevents the disclosure of the information provided to the DOD? As discussed above, the CII Act clearly protects information provided to the DHS regarding the protection of critical infrastructure from terrorist attack. The same is not so clear with regard to information the DIB partner provides to its DOD counterpart, despite the fact that the DIB partner has a direct working relationship with the DOD. The DIB partner may have some level of protection in accordance with FOIA exemption number four if the information qualified as a trade secret, but not the expansive protection

[120] 6 C.F.R. § 29.4 (2009).

of the CII Act.[121] In the end, the lack of guarantees with regard to the release of information to the public or to other industry members creates a potential disincentive to information-sharing between the DIB and the DOD.

Furthermore, what gives the DOD the authority to provide threat and vulnerability information directly to its private-sector DIB counterparts? For a DIB partner providing IT and other computer-related support, protection of the DIB partner's IT infrastructure might involve information about the vulnerabilities of both DOD-owned and privately owned systems. This information may be classified or otherwise sensitive to military operations. In particular, the means by which the DOD came across these vulnerabilities might be more sensitive or classified. In fact, disclosure of the vulnerabilities might itself reveal classified or sensitive collection methods. How does the DOD go about sharing this information with its DIB counterparts? Criminal provisions certainly regulate improper disclosure of classified information.[122] But, how can the DOD and its DIB IT partners forge a successful working relationship if these two groups are unable to freely provide information to each other? Also, how can a critical infrastructure protection effort be successful without a free flow of the information related to that infrastructure? Clearly, within the IT arena, the most important issue with regard to the most vulnerable aspect of the DIB IT infrastructure is the protection and sharing of information.

What does the DOD propose with regard to sharing critical infrastructure information? Other than referencing the NIPP and the CII Act, it says very little. The DIB plan makes cursory mention to the fact that the DOD will "*support* and *facilitate* sharing of threat information through *appropriate government and commercial channels*."[123] The plan also calls for the DOD to share information related to criticality determinations with whatever organization is tasked with protecting that asset.[124] However, the plan is thin on specifics.

The DIB plan claims that the DOD identified the venues and mechanisms for information-sharing with its Critical Infrastructure Protection communities of interest.[125] The plan identifies these communities as "domestic organizations (including industry); international private industry; international coalitions and allies; Federal, State, and local governments and agencies; and other DOD organizations to identify and coordinate protection of critical DIB assets."[126] The venues identified by the DIB plan include "DIB

[121] 5 U.S.C. § 552(b)(4) (2006); FED. R. CIV. P. 26-37.
[122] 18 U.S.C. § 798 (2006).
[123] DIB SSP, *supra* note 17, at 24 (emphasis added).
[124] *Id*. at 25.
[125] *Id*. at 44.
[126] *Id*.

[Government Coordinating Council], [Sector Coordinating Council], and [Critical Infrastructure Partnership Advisory Council] meetings; [Defense Critical Infrastructure Program] Awareness Visits; Industry association meetings and expositions; Academic symposia and conferences; Electronic and traditional mail; and World Wide Web and restricted network portals."[127] The mechanisms for communicating

> *roles, responsibilities, and concepts* for effective DIB [Critical Information Protection] efforts include: Published policy, directives, instructions, guidance, and methodology; Documented concept (sic) of operations; Presentations and speaking engagements at association, international, Federal, State, and local events, expositions, and conferences; Onsite awareness presentations at DIB sites; Participation in exercises and published lessons learned; and, Curricula at Defense and other schools.[128]

However, even discussing information sharing from the point of "roles, responsibilities, and concepts" misses the mark. What about the actual information related to the private sector's critical DIB infrastructure?

The DIB plan does not propose any new mechanism for sharing sensitive or classified DIB threat or vulnerability information directly with its security partners. Rather, it relies on the DHS's PCII program to accomplish the information-sharing effort. The DIB plan relies on the protections afforded by the CII Act, such as protection from FOIA disclosure, state and local disclosure laws, and use in civil litigation; but does not have any DIB-specific protections.[129] The DIB proposes to appoint a PCII Officer to oversee handling, use, and storage of PCII; ensure secure handling of that information; establish a self-inspection program focusing on compliance with PCII handling, use, and storage requirements; and ensure coordination with the PCII Program Manager regarding requests, challenges, or complaints regarding PCII regulation implementation.[130]

In addition, "DOD plans to develop an accreditation plan for obtaining and certifying PCII."[131] Some of this information requires security classification in accordance with previously established regulations.[132] The plan recognizes that it must encourage voluntary

---

[127] *Id*.
[128] *Id*. (emphasis added).
[129] *Id*. at 45.
[130] *Id*.
[131] *Id*.
[132] *Id*.

sharing of information and analysis.[133] It also admits that there has been, in fact, very little interaction between DOD and industry with regard to information-sharing.[134] The plan goes on to recognize that this situation must be remedied in order to achieve a successful collaborative effort to protect the DIB infrastructure.[135]

The real problem with the DIB plan's approach to information-sharing is its lack of specificity and innovation. The DIB plan lists information security and information assurance as two of its goals.[136] With regard to the information security goal, the plan contends that "[a]ll information that identifies or otherwise describes characteristics of a critical DIB asset that is created, held, and maintained by the government or the private sector *will be protected from unauthorized disclosure* according to *established procedures* appropriate to the particular level of information."[137] The plan does not, however, address the lack of statutory authority to protect information provided by the private sector directly to the DOD. Merely relying on "established procedures" does not give statutory teeth to the process, nor should it instill any particular level of confidence in members of the private sector that their proprietary information would remain secure.

As it relates to the information assurance goal, the plan states that "DIB asset owners/operators will have functional and adequate plans in place for exercising prudent information assurance methods to protect the DIB asset, to control processes over the production or provisioning of the product or service, and to protect the product or service delivery systems, including the supply chain."[138] Yet, the DIB plan does not specify how it proposes to accomplish this goal or to enforce the requirement.

F. DOD Critical Infrastructure Challenges

The Government Accountability Office (GAO) noted many of the shortfalls of DOD efforts to protect the DIB's critical infrastructure. The GAO analyzed the DCIP, recognizing that DOD relies so heavily on non-DOD infrastructure assets that their unavailability could critically hinder the DOD's ability to project, support, and sustain forces and operations worldwide.[139] As alluded to earlier, the DCIP (DODD

[133] *Id*.
[134] *Id*.
[135] *Id*.
[136] *Id*. at 11.
[137] *Id*. (emphasis added).
[138] *Id*.
[139] U.S. GOVERNMENT ACCOUNTABILITY OFFICE, DEFENSE INFRASTRUCTURE: ACTIONS NEEDED TO GUIDE DOD'S EFFORTS TO IDENTIFY, PRIORITIZE, AND ASSESS ITS CRITICAL INFRASTRUCTURE 1 (2007) [hereinafter GAO-07-461], *available at* http://www.gao.gov/new.items/d07461.pdf.

3020.40) is the DOD plan to protect DIB infrastructure regardless of where a threat originates. In conducting its analysis, the "GAO was asked to evaluate the extent to which DOD has (1) developed a comprehensive management plan to implement DCIP and (2) identified, prioritized, and assessed its critical infrastructure."[140] Again, the GAO evaluated the DOD's efforts with regard to the DCIP (published in August 2005) and not the DIB plan (published in May 2007—the same month the GAO released its report). Thus, the GAO evaluation strictly focused on DOD-owned critical infrastructures. Nevertheless, the GAO found several interesting things during the course of its first evaluation that related to non-DOD-owned infrastructures. First, the GAO learned that the DOD only identified an estimated twenty-five percent of the critical infrastructure that it owns.[141] Further, the GAO found that the DOD did not even expect to identify the remaining seventy-five percent of its critical infrastructure until the end of fiscal year 2009.[142] To make matters worse, the DOD identified significantly less of the infrastructure that it does not own and did not even have an estimated completion date for that effort.[143] Accordingly, the GAO conducted further analysis specifically related to non-DOD-owned DIB infrastructures. The size of this analysis would be extensive as an estimated 200 non-DOD-owned DIB assets are mission critical—approximately eighty-five percent of the entire DIB sector.[144]

In August 2007, the GAO released its follow-up report regarding non-DOD-owned DIB infrastructures.[145] The GAO found that the DIB is comprised of hundreds of thousands of industrial sites predominately owned by the private sector.[146] The GAO analyzed the protection of this infrastructure more broadly than called for by either HSPD-7 or the NIPP. Specifically, the GAO analysis covered threats not only from terrorist attacks but also from criminal activity, technological failure, natural disaster or a man-made catastrophe.[147] In this second report, the GAO analysis focused on two issues: (1) the status of DOD efforts to develop and implement a risk management approach to ensure the availability of DIB assets which support mission-essential tasks, and (2) challenges faced by the DOD in its approach to

---

[140] *Id*. at 4.
[141] *Id*. at 25.
[142] *Id*.
[143] *Id*. at 25-26.
[144] *Id*.
[145] U.S. GOVERNMENT ACCOUNTABILITY OFFICE, DEFENSE INFRASTRUCTURE: MANAGEMENT ACTIONS NEEDED TO ENSURE EFFECTIVENESS OF DOD'S RISK MANAGEMENT APPROACH FOR THE DEFENSE INDUSTRIAL BASE (2007) [hereinafter GAO-07-1077], *available at* http://www.gao.gov/new.items/d071077.pdf.
[146] *Id*. at 1.
[147] *Id*.

risk management within the DIB sector.[148]

The cornerstone of the NIPP, and by extension the DIB plan, is a risk-management framework that establishes priorities based on risk and calls for protection and continuity initiatives to mitigate those risks.[149] The DCIP, which again addresses more than just terrorist threats against DOD infrastructures, assigns lead agents for each of ten identified sectors—one of which is the DIB.[150] The Under Secretary for Acquisition, Technology, and Logistics is responsible for DOD efforts related to the DIB's critical infrastructure.[151] Due to its established working relationship with private sector DIB owners and operators, the lead agent for the DIB sector is the Defense Contract Management Agency (DCMA).[152] In analyzing the status of DOD efforts to develop and implement a risk management approach, the GAO examined DIB plans; DCMA efforts to identify, assess, and remediate critical DIB assets; criteria established by the DCMA to identify important and critical DIB assets; the DCMA's asset prioritization model used to rank critical assets; and vulnerability assessment standards, including their implementation by National Guard teams tasked with conducting those assessments.[153]

The DIB plan provides a coordinated strategy to (1) identify and prioritize a critical asset list, (2) perform vulnerability assessments on the high priority critical assets, and (3) encourage private sector contractors to address vulnerabilities found during these assessments.[154] In identifying DIB critical assets, the DCMA and supporting personnel, using a tiered process, compiled a list of approximately 900 important defense contractor assets from the hundreds of thousands of entities constituting the DIB, ultimately narrowing that list down to 203.[155] Then, the DMCA used an asset prioritization model it developed to determine a criticality score so that it could rank critical assets.[156] The DCMA collected the data used to develop this score from DCMA surveys, supplemented by commercial and government sources, including the Defense Logistics Agency, the military services, and the combatant commands.[157] Once identified, critical DIB should undergo a standardized mission assurance vulnerability assessment.[158] However,

---

[148] *Id*. at 4.
[149] *Id*. at 2.
[150] *Id*.
[151] U.S. DEP'T OF DEF., DIR. 3020.40, DEFENSE CRITICAL INFRASTRUCTURE PROGRAM (DCIP) para. 5.3 (19 Aug. 2005).
[152] DIB SSP, *supra* note 17, at 7.
[153] GAO-07-1077, *supra* note 147, at 11-17.
[154] *Id*. at 11.
[155] *Id*. at 11-12.
[156] *Id*. at 11.
[157] *Id*. at 14.
[158] *Id*. at 11.

as of 1 June 2007, only eight of the some 203 critical assets had undergone a vulnerability assessment.[159] At the same time, DOD has developed a remediation planning guide to address the vulnerabilities identified through the assessments.[160] However, this guide was designed in a general way that does not suggest deadlines because of the voluntary nature of the DIB in the DCIP process.[161]

With regard to its analysis of the DOD's challenges in developing and implementing its approach, the GAO compared policies for identifying mission-essential tasks and related defense critical assets with the DCMA's approach of identifying a critical DIB asset list. The GAO also examined the development and use of the DCMA asset prioritization model. It reviewed DCIP efforts by the services related to protection of the DIB. Finally, the GAO reviewed private sector contractor challenges, including contractors' willingness to participate in the program.[162] The GAO found four separate challenges that the DOD must address to ensure its risk management approach is sound.[163]

The first challenge identified by the GAO is that the critical asset list used by the DCMA does not yet incorporate comprehensive, mission-essential task information from the military services.[164] Information from the 2006 list came primarily from the DCMA, Army, and Navy.[165] The Air Force provided no input to the 2006 list.[166] For the 2007 list, the Air Force merely reviewed and validated critical DIB assets identified and complied by the DCMA; it made no independent submissions of DIB assets.[167] The services are still in the process of identifying mission-essential tasks and the defense critical assets that support them, including critical DIB assets.[168] To date, the DOD has not established a plan for identifying all service mission-essential tasks, or targets and time frames.[169]

Second, the critical asset prioritization model developed and used by the DCMA has yet to undergo an external review, and it lacks both contractor-specific data and comprehensive threat information.[170] One of the most controversial aspects of the model is the subjective decisions the DCMA interjects into the model.[171] The DCMA model

---

[159] *Id*. at 11-12.
[160] *Id*. at 17.
[161] *Id*. at 18.
[162] *Id*. at 18-26.
[163] *Id*.
[164] *Id*. at 18.
[165] *Id*.
[166] *Id*.
[167] *Id*.
[168] *Id*. at 19.
[169] *Id*.
[170] *Id*. at 19-21.
[171] *Id*. at 19.

relies heavily upon data from private sector contractors. However, the GAO review identified missing contractor-specific data for a number of critical assets.[172] The DCMA attempted to collect the needed information via two surveys but failed to do so, because collection of this information depends upon contractors' willingness to provide business information, which is sometimes of a sensitive nature.[173] To make matters worse, when missing needed information, the DCMA defaults to a high-risk score, the most conservative assumption.[174] Accordingly, within the prioritization list, it is not always apparent whether the DCMA identified some contractors as high risk because data was unavailable or because data actually justified the high risk rating.[175] In 2005, only thirty percent of surveyed DIB entities responded to DCMA surveys.[176] The DCMA did not even conduct a survey in 2006.[177] Further, the DOD lacks comprehensive threat information because intelligence sources provide information through *ad hoc* agreements rather than by formal arrangements.[178] Absence of this information likewise undermines the utility of the score used to prioritize DIB contractors.[179] Until the DCMA formulates a procedure for collecting the comprehensive threat data it needs, its asset prioritization model will remain unreliable.[180]

The third challenge facing DOD relates to the fact that the DCMA is not scheduling and conducting vulnerability assessments in accordance with its own rankings from its prioritization model.[181] Currently, the DCMA is scheduling and conducting vulnerability assessments based upon the accessibility of DIB contractors rather than in accordance with its own established procedures, which calls for the highest priority assets to receive assessments first.[182] Coordinating vulnerability assessments can be complicated and sensitive.[183] Because the DCMA cannot inform uncleared contractors that they are on the classified critical asset list or discuss vulnerabilities found at their facilities, the lack of facility security clearances significantly complicates the DCMA's ability to get DIB contractors to participate in the risk management program.[184] Currently, "About 52 percent of the

---

[172] *Id*. at 20.
[173] *Id*.
[174] *Id*. at 14, 20.
[175] *Id*. at 20.
[176] *Id*.
[177] *Id*. at 21.
[178] *Id*.
[179] *Id*.
[180] *Id*.
[181] *Id*. at 21-24.
[182] *Id*. at 21.
[183] *Id*. at 22.
[184] *Id*.

DIB facilities identified as critical lack security clearances for the facility or its personnel, and thus cannot receive vulnerability assessments or discuss needed remediation actions."[185] So, rather than scheduling assessments for DIB contractors with the highest priority first, the DOD provides the first assessments to contractors who can demonstrate they have the appropriate security clearances.

Furthermore, some DIB contractors have expressed concerns about sharing proprietary business information with the government and about resulting increases in cost and liabilities related to correcting vulnerabilities identified as a result of sharing information pursuant to this program.[186] Of primary concern is the DOD's ability to protect information DIB contractors deem proprietary or potentially damaging if released or disclosed.[187] This is obviously a serious concern to a private industry whose success depends on the profit it generates, which is often directly tied to proprietary information and intellectual property. Additionally, "some significant DIB contractors are involved in classified, special access programs that could involve military mission-essential tasks and as a result may not be allowed or willing to share certain types of information."[188] Thus, DCIP efforts may not even include some significant critical DIB assets.[189] To overcome this problem, DCMA primarily resorted to having high-level DOD officials contact the contractors directly or developing memoranda of agreement specifying duties of the parties.[190] The DOD is also considering accreditation of a PCII Program effort to provide safeguards to concerned contractors.[191] However, the PCII Program was created to address terrorist-related threats and not the all-encompassing list of threats addressed by the DCIP, the NIPP, and the DIB plan.[192] It remains unclear whether using the PCII Program beyond the scope of the terrorist concern is even authorized.

The GAO report goes on to point out that nothing prevents private sector DIB entities or other sources from sharing information directly with the DOD.[193] However, the report does not address the issue that voluntary sharing of information does not come with protections from disclosure afforded by such statutes as the CII Act. Until the government can demonstrate the ability to provide adequate security for contractor-provided information, nonfederal entities will be reluctant to release sensitive information to the DOD because of the lack

---

[185] *Id*.
[186] *Id*.
[187] *Id*.
[188] *Id*. at 22-23.
[189] *Id*. at 23.
[190] *Id*.
[191] DIB SSP, *supra* note 17, at 44-45.
[192] 6 C.F.R. § 29.1(a) (2009).
[193] GAO-07-1077, *supra* note 147, at 24.

of certainty regarding full protection of information they provide.[194] In an effort to remedy this problem, the DCMA proposed new legislation and additional provisions in the Defense Federal Acquisition Regulation Supplement (DFARS)[195] to address information protection, thereby increasing private-sector DIB participation, but these proposals were never enacted.[196] Currently, no plans exist within the DOD to further pursue legislation regarding this issue.[197] Also, the DCMA recommended DFARS provisions which would mandate that contractors be responsible for physical protection and security of their own critical infrastructures, that they have comprehensive security plans relating to facility security, and that the government be permitted to conduct or facilitate vulnerability assessments under the DCIP.[198] But, these provisions were not submitted to the Defense Acquisition Regulation Council, which develops policy for approval by the Director of Defense Procurement.[199]

The fourth and final DOD challenge identified by the GAO is that it lacks a plan for identifying and addressing challenges in assessing vulnerabilities of critical foreign contractors.[200] This effort requires interagency cooperation, particularly with the Department of State.[201] But, to date, the DCMA has yet to conduct any assessments on foreign contractors.[202] This effort would obviously impact existing treaties and embassies and host governments and would require coordinated efforts.[203] A strategic action plan for foreign countries with DIB assets must also be developed.[204] The DOD must address all of these challenges in order to ensure successful protection of the DIB critical infrastructure by the DOD and its sector partners.

G. Recent Developments

Interestingly, in 2008, President Bush seemingly changed course on the issue of attacks on computer systems, at least as it relates to those systems owned by federal agencies. As previously mentioned, the federal government may clearly protect computer and other information management systems owned by any given federal agency. Nevertheless, President Bush, by means of a classified directive signed

---

[194] *Id*.
[195] U.S. DEP'T OF DEF., DEFENSE FEDERAL ACQUISITION REG. SUPP. (July 1, 2009).
[196] *Id*. at 24.
[197] *Id*. at 25.
[198] *Id*.
[199] *Id*.
[200] *Id*. at 25-26.
[201] *Id*. at 25.
[202] *Id*.
[203] *Id*. at 25-26.
[204] *Id*. at 26.

on 8 January 2008, authorized federal intelligence agencies, in particular the National Security Agency (NSA), to monitor the computer networks of all federal agencies, including those they had not previously monitored.[205] Pursuant to this directive, a task force headed by the Office of the Director of National Intelligence (ODNI) will coordinate efforts to identify the source of cyber-attacks against government computer systems.[206] The DHS and DOD will take ancillary roles in this effort—protecting systems and devising strategies for counterattacks.[207]

This joint directive—designated as the National Security Presidential Directive 54/Homeland Security Presidential Directive 23—followed a number of attacks on computer systems owned by the Departments of State, Commerce, Defense, and Homeland Security since mid-2006.[208] U.S. officials and cyber-security experts identified Chinese websites involved in the largest of these attacks in 2005.[209] These particular attacks included U.S. nuclear laboratories and large defense contractors.[210] The DHS observed 37,258 cyber-attacks on government and private networks in 2007, compared to 4095 in 2005.[211] Thus, President Bush requested an initial six billion dollars to begin building a thirty-billion-dollar system to protect these networks from attack.[212]

In coordinating the efforts of the DHS and the DOD, which has been involved in computer system and network protection for some time, the "NSA has particular expertise in monitoring a vast, complex array of communications systems—traditionally overseas."[213] Not surprisingly, there is some concern about using NSA's computer network monitoring capabilities in the domestic context.[214]

But, while this new intelligence-led effort addresses computer systems owned by the government, some have recognized the gap in coverage, discussed above, regarding private industry, in particular DIB-owned, networks. Alan Paller, research director for a cyber-security group assisting companies facing attacks, noted, "If you don't include industry in the mix, you're keeping one of your eyes closed because the hacking techniques are likely the same across government

---

[205] Ellen Nakashima, *Bush Order Expands Network Monitoring*, WASH. POST, Jan. 26, 2008, at A3.
[206] *Id*.
[207] *Id*.
[208] *Id*.
[209] *Id*.
[210] *Id*.
[211] Siobhan Gorman, *Bush Looks to Beef Up Protection Against Cyberattacks*, WALL ST. J., Jan. 28, 2008, at A8.
[212] *Id*.
[213] Nakashima, *supra* note 205.
[214] *Id*.

and commercial organizations."[215] It is within this private-sector gap that some analysts say 90 percent of the threat exists.[216] The previous Director of National Intelligence, Mike McConnell, claimed ninety-five percent of the problem lies within the private sector. According to media sources, this initiative will address private networks in some fashion.

A 2008 Wall Street Journal article reported that "[t]he program would first be used on government networks and then adapted to private networks."[217] The same article indicated that protection of "private computer systems would likely require the government to install sensors on private, company networks. . . ."[218] These private networks would include such systems as those used by Wall Street.[219] Currently, however, there is no information that indicates what legal authority the government would have to install such sensors on, or otherwise protect, private computer networks.

Thus, while former Deputy Defense Secretary Gordon England has proclaimed that "[c]yber warfare is already here," he failed to address a specific, critical issue: his definition of "cyber warfare" seemingly included attacks on private computer systems.[220] Secretary England, noting President Bush's newly established task force on 3 March 2008, referred to efforts to safeguard computers in general, failing to differentiate between privately owned and government-owned IT infrastructure.[221] This failure appears to be pervasive. Former Director McConnell also addressed cyber warfare issues with regard to information systems involving the "money supply, electric power distribution, transportation and that sort of thing," notwithstanding the fact that private-sector entities own or operate the majority of these information systems.[222]

Security of IT infrastructure is obviously not only a domestic concern. The cyber attack on Estonia in 2007 stimulated international discussion of the defense of cyber networks.[223] But, like the United States, other countries seem reluctant to exclude privately owned information systems when discussing cyber security and protection of those systems by military assets. The attacks on Estonia were directed against such privately owned organizations as daily newspapers and

---

[215] *Id*.
[216] *Id*.
[217] Gorman, *supra* note 211.
[218] *Id*.
[219] *Id*.
[220] John J. Kruzel, *Cyber Warfare a Major Challenge, Deputy Secretary Says*, AMERICAN FORCES PRESS SERVICE, Mar. 3, 2008, *available at* www.af.mil/news/story.asp?storyID-123088782.
[221] *Id*.
[222] *Id*.
[223] *Id*.

banks.[224] Thus, the implication is that even NATO is comfortable with considering the use of the military to protect privately owned computer networks and data, notwithstanding potential legal impediments.

The Obama Administration certainly has cybersecurity on its radar screen. The extent to which this effort will cover private IT networks and which governmental agency, if any, will be responsible for this infrastructure is unclear at this early stage of President Barrack Obama's first term. The Administration, noting that the strength and vitality of the U.S. economy, infrastructure, public safety, and national security were built on the foundation of cyberspace, insists that the U.S. global digital infrastructure, based largely upon the Internet, is not secure or resilient enough today or for future purposes. [225] The Obama Administration initially took the position that the government should partner with academia, the private sector, the civil liberties community, international partners, the Congress, and state and local governments to innovate and adopt cutting edge technology, while enhancing national security and the global economy.[226]

So, on 9 February 2009, President Obama directed a sixty-day review of the government's plans, programs and activities that address U.S. communications and information infrastructure.[227] The review's purpose was to develop a strategic framework to ensure that the government's initiatives in this area were integrated, resourced, and coordinated within the Executive Branch and with Congress and the private sector.[228] In April, the interagency group undertaking the review concluded its work and submitted its findings and recommendations for President Obama's review.[229] The inclusion of the private sector within this review may shed some light on the Administration's upcoming position on whether a government agency should be involved in the protection of private sector infrastructure, including the DIB, but no final decision has been articulated at this point.

In addition to the Obama Administration's cybersecurity efforts, Congress is in the process of addressing this issue as well. In August 2009, cybersecurity legislation previously introduced by Senate Commerce Chairman John (Jay) Rockefeller and Senator Olympia Snowe underwent major changes.[230] The senators sent the revised

---

[224] *Id*.

[225] The White House, Homeland Security and Counterterrorism, http://www.whitehouse.gov/issues/homeland_security (last visited Sept. 1, 2009).

[226] *Id*.

[227] Press Release, Office of the White House Press Secretary, Statement by the Press Secretary on Conclusion of the Cyberspace Review (Apr. 17, 2009), *available at* http://www.whitehouse.gov/the_press_office/Statement-by-the-Press-Secretary-on-Conclusion-of-the-Cyberspace-Review/.

[228] *Id*.

[229] *Id*.

[230] Andrew Noyes, *Cybersecurity Draft Significantly Altered*, NEXTGOV, Aug. 25, 2009,

version of the bill to the Commerce and Intelligence committee aides for review following the August 2009 recess.[231] The bill addresses various cybersecurity issues. Prominent in the revised bill are provisions instructing the Commerce Secretary to work with the White House Office of Personnel Management to hire, train, and certify government cyber professionals.[232]

In the new version, the drafters ultimately curtailed a section of the prior legislation that would have allowed the president, during a cyber emergency, to limit or even shut down Internet traffic to and from any compromised government or U.S. critical infrastructure information system or network.[233] The new proposal directs the president to work with industry during a cyber emergency on a national response as well as the timely restoration of affected networks.[234] This alteration illuminates one of the primary issues surrounding any potential DOD or Air Force involvement in protecting DIB IT infrastructure: can the government legally impede a private network that it does not own, even if for a just purpose—protecting its networks?

The drafters also eliminated earlier language requiring an advisory panel to ensure national security would not be compromised before approving the renewal or modification of a contract between the U.S. government and the entity that oversees global Internet addresses.[235] Certainly, there are by necessity a number of issues in the contracting realm, especially with regard to sharing information between the government and private entities, as discussed in Section IV below.

The reworked draft includes a biennial cyber review beginning in 2013 to review the current posture of the country's IT infrastructure, including an unclassified summary of roles, missions, accomplishments, plans, and programs associated with securing that infrastructure.[236] The bill also sets up a cybersecurity advisory panel of representatives from industry, academia, nonprofit organizations, interest and advocacy groups, and state and local governments.[237] In addition, the legislation would create state and regional cybersecurity enhancement programs and a threat and vulnerability clearinghouse for the government and the private sector.[238] The initial bill specified that the Commerce Department would serve as home to the clearinghouse, but the latest

---

http://www.nextgov.com/nextgov/ng_20090825_4908.php?oref=search (last visited Sept. 21, 2009).

[231] *Id.*
[232] *Id.*
[233] *Id.*
[234] *Id.*
[235] *Id.*
[236] *Id.*
[237] *Id.*
[238] *Id.*

version leaves its designation vague.[239] However, the inclusion of the Commerce Department in the discussion should not be overlooked. The connection between private industry and commerce regulations may be the conduit for initial government involvement in private sector cybersecurity efforts.

Other provisions would require a comprehensive analysis of the federal statutory and legal framework applicable to cyber-related activities in the United States and a joint intelligence threat assessment by the ODNI and the Commerce and Homeland Security secretaries.[240] Interestingly, the early press reports do not mention the military's possible involvement in these efforts. Whether that indicates a retreat from this earlier proposal or a failure of accurate reporting is unknown at this point. But, the 20 August 2009 Air Force memo about supporting the USCYBERCOM mission discussed earlier does not mention protection of privately owned critical IT infrastructure either.[241]

H. Summary of Authority

Thus, in regard to this issue, the DOD shares some responsibility with the DHS in protecting the nation's critical infrastructure. Particularly, the DOD takes a leading role in assisting in the protection of critical infrastructure with its partners in the DIB sector. Neither the DOD, nor any other governmental entity, has the authority to unilaterally protect infrastructure that it does not own, whether it is part of the DIB sector or not. This includes the IT infrastructure not owned by the DOD.

Based on current law and policy, participation in the protection of critical infrastructure by private-sector DIB members is completely voluntary. Based on those same laws, the federal government at least affords some protection to private-sector DIB members who provide information through the PCII Program. Although, it appears the law does not call for the PCII Program to receive information not related to potential terrorism, nor does the CII Act's protections appear to extend to information provided directly to the DOD. Nevertheless, information provided to the DHS can then be used to coordinate protection of all IT critical infrastructure components, including members of the DIB. But, it is unclear as to what degree intelligence agencies such as the NSA—which, as of the early part of 2009, may be more involved than in the past—may share information it collects, either overseas or domestically, with the DHS, the DOD, and more importantly, the DIB.

So, given the limited ability for the DOD to assist in protecting

[239] *Id*.
[240] *Id*.
[241] Cyberspace Memo, *supra* note 1.

the DIB IT critical infrastructure, how should the Air Force proceed with the current effort and should the Air Force push to expand its abilities in this area, and if so, how? Before answering those questions, one must analyze what, if any, contractual liabilities the Air Force may face by assisting in the protection of individual defense contractor's information infrastructure.

IV. WHAT RESPONSIBILITY DOES THE AIR FORCE INCUR, IF ANY, BY ASSISTING IN OR PROTECTING INFORMATION TECHNOLOGY OF SELECTED DEFENSE CONTRACTORS?

In 1984, Congress passed the Competition in Contracting Act (CICA).[242] The provisions of CICA that apply to the DOD are codified at 10 U.S.C. §§ 2304-2305. A few additional competition provisions applicable to all federal agencies are found in Title 41, United States Code.[243] "[I]t is a fundamental principle of government procurement that competition must be conducted on an equal basis, that is, offerors must be treated equally and be provided with a common basis for the preparation of their proposals."[244] Could a potential defense contractor successfully claim that an incumbent contractor possesses an unfair competitive advantage if the DOD protected the existing contractor's IT infrastructure or provided that contractor with information that allows the contractor to protect their own infrastructure? With respect to this issue, a contractor would have an unfair competitive advantage if a contractor possessed "source selection information" relevant to the contract not available to all competitors and that information would assist in obtaining the contract.[245] Also, the presence of an "organizational conflict of interest" may also lead to a claim of unfair competitive advantage.[246]

A. Unfair Competitive Advantage Based on Possession of Source Selection Information

As referred to in the definitions section above, the term "unfair competitive advantage" is a term of art defined within the FAR. Generally, a contractor competing for the award of a federal contract may have an unfair competitive advantage if that contractor possesses proprietary information that it obtained from the government in an

---

[242] Competition in Contracting Act of 1984, Pub. L. No. 98-369, 98 Stat. 1175 (codified in scattered sections of 10 U.S.C. and 41 U.S.C.).
[243] 41 U.S.C. §§ 401-424 (2006).
[244] Bath Iron Works Corp., B-290470, B-290470.2, 2002 U.S. Comp. Gen. LEXIS 122 (Aug. 19, 2002).
[245] FAR, *supra* note 27, at 9.505(b)(2).
[246] *Id*. at 2.101, 9.505(a).

unauthorized manner, or it possesses "source selection information" relevant to the contract that was not available to all competitors and that information would assist that contractor in winning the contract award.[247] Obviously, the unauthorized possession of proprietary information by a contractor would be problematic. However, with regard to potential protests by contractors who object to current contractors having their IT infrastructure protected by the government, this type of unfair competitive advantage is irrelevant.

Is there, then, any relevance to the second type of unfair competitive advantage claim—one where source selection information is at issue? At first glance, one might say yes. However, the real answer lies within the definition of "source selection information." Source selection information is also a term of art defined by the FAR.[248] This category of information includes information primarily related to an agency's evaluation of a bid or proposal to enter into a government contract.[249] This type of information includes such information submitted by a potential contractor as bid prices, costs, technical evaluation plans, ranking of bids by competitors, the list of competitors making bids, evaluations of bids, and the like.[250] It does not, however, include the type of information that is relevant to the issue at hand.

For example, refer back to the previous discussion of a DIB partner exchanging information with the Air Force for purposes of protecting that DIB partner's critical IT infrastructure. In order to adequately protect IT infrastructure of the DIB, there must be a meaningful exchange of information between the DOD and private sector DIB partners. This information would include, among other things, information about how different IT systems work and vulnerabilities that exist on them. The result would be that certain defense contractors would possess threat and vulnerability information to protect their IT infrastructure that other private sector companies would not have. This information would provide a significant benefit to defense contractors and could place them in an advantageous position with respect to the DOD's confidence that the DIB partner's IT infrastructure was as secure as possible.

Now fast forward—what about a future procurement? If the security of the bidding contractors' IT infrastructure is a factor in selecting the eventual award winner, would not existing DIB contractors, who have received threat and vulnerability information from DOD sources, be in the best position to prove that their IT systems are secure and thus they are the right company for the job? By extension, would private companies who are not defense contractors be

[247] *Id*. at 9.505(b).
[248] *Id*. at 2.101.
[249] *Id*.
[250] *Id*.

at a disadvantage in the bidding process? The initial response to those questions is likely yes. But is that particular question relevant to having an unfair competitive advantage, as that term is defined in the FAR? It does not appear likely.

First, the type of threat and vulnerability information in the possession of private DIB companies does not meet the FAR definition of "source selection information." Threat and vulnerability information is not related to the bids being placed by companies vying for a contract, nor does it reveal any sort of evaluation of companies, their capabilities, or resources that would allow a certain company to know what its competitors are contending they can provide to the government if they are selected for the contract. It is this type of insider information that the FAR seeks to prevent from getting into the hands of one company, thus giving it an unfair competitive advantage over the others, not the threat and vulnerability information that some company has received through its previous relationship with the DOD.

Second, it will likely be no surprise to any competitor for this type of DOD contract that the security of its IT infrastructure would be at issue. The request for proposals disseminated by the DOD will probably list this as one of the requirements for winning the contract. That same proposal will likely discuss what the DOD-contractor relationship will be once the contract is awarded, with regard to the winner's infrastructure security. While the competitors will probably not know the details of each other's IT vulnerabilities, it is equally likely that all competitors will know that some vulnerabilities must exist. Thus, the question becomes: if this threat and vulnerability information is not the kind of source selection information that the FAR seeks to prohibit a contractor from possessing, could a competitor successfully claim that information nonetheless gives that contractor an improper advantage in some future procurement process because the previous relationship that the contractor had with the DOD creates a conflict of interest?

B. Organizational Conflict of Interest

An organizational conflict of interest (OCI) may be a more fertile area for complaints with regard to efforts by the Air Force to protect DIB critical IT infrastructure. Increasingly, OCIs have appeared in federal procurements.[251] There are several reasons for this phenomenon. First, "the consolidation within the industries serving the U.S. Government, particularly in the information technology and

[251] Daniel I. Gordon, *Organizational Conflicts of Interest: A Growing Integrity Challenge*, 35 PUB. CONT. L.J. 25, 26 (2005).

defense industries" has increased the number of OCI problems.[252] This is a result of fewer contractors that produce a particular good or service, so each ends up producing a wider range of goods or services.[253] Second, the government is utilizing contractors more frequently for various services that require some level of judgment by those contractors.[254] For example, rather than hiring a private contractor to provide computer repair services, the government might contract with a firm that advises the government on which computer hardware or software to purchase.[255] The third reason for the increasing occurrence of OCIs in government procurements is the use of marketing-encouraging contracts.[256] These "umbrella" contracts involve multiple companies covering multiple federal agencies, and because they provide low minimum dollar guarantees, a contractor's profit is increasingly dependent upon its ability to market to federal agencies.[257] A recent example of this situation occurred in connection with a Department of Interior contractor providing IT services under a General Services Administration (GSA) Federal Supply Schedule program that allowed the contractor to provide IT services to numerous agencies.[258]

The following elements must be established to prove an OCI exists. First, there must be a conflicted party.[259] The definition of a conflicted party is more expansive than one might imagine. For example, the definition might be triggered when an individual in a firm's research and development office helps a government agency draft specifications for a new weapon system and the management office of the same firm competes for the contract to build that same weapon system for the government.[260]

Second, there must be some interest or benefit in the conflicted party's involvement.[261] Third, the conflicted party must have some responsibility to a third party, which is usually the government.[262] The most frequent example is when the third party (for example, the DOD) is attempting to obtain an unbiased opinion (for example, on how to structure a military IT network) from a conflicted party (for example, a defense contractor).[263] An OCI's definition also includes a provision for a situation when a conflicted party has an "unfair competitive

[252] *Id*. at 26.
[253] *Id*. at 27.
[254] *Id*.
[255] *Id*.
[256] *Id*.
[257] *Id*.
[258] *Id*.
[259] *Id*. at 29.
[260] *Id*.
[261] *Id*.
[262] *Id*. at 30.
[263] *Id*.

advantage."[264]

There are three major categories of OCIs.[265] The first is the "biased ground rules" group.[266] This describes a situation "where a company sets the ground rules for a future competition by, for example, writing the specifications that competitors for a contract must meet."[267] The second category deals with "impaired objectivity."[268] This situation refers to a company being asked to perform some task that requires objectivity, but some other role within the company calls into question the company's ability to be unbiased.[269]

The third category, and the one most relevant to issues of the DOD's involvement in protecting private-sector DIB IT infrastructure, is the "unequal access to information" situation.[270] This situation occurs when a company has access to nonpublic information, often because it has previously been involved with a government contract of the same or similar nature, which gives it an upper hand in competing for a later contract.[271] With regard to "unequal access to information" OCI challenges, courts have examined the following issues more broadly: (1) whether a particular offeror had access to nonpublic information that was unavailable to a protestor, (2) whether that information was competitively useful in responding to a solicitation, (3) whether the awardee was afforded an unfair advantage by having unequal access to that information, and (4) whether having unequal access to that information prejudiced the protestor.[272]

The means by which to challenge a procurement alleged to involve an OCI is a bid protest.[273] A contractor may protest a bid with the contracting agency, the GAO, or the United States Court of Federal Claims (COFC).[274] A dissatisfied entity may protest either the propriety of the solicitation (i.e., before the contract is awarded) or the actual awarding of a contract.[275] When a protestor alleges that OCI tainted a contract award, resolution of that protest will generally hinge on the existence of the claimed "taint."[276] Generally, involvement by the winner of a contract award in the evaluation and selection process will

---

[264] FAR, *supra* note 27, at 2.101.
[265] Gordon, *supra* note 251, at 32.
[266] *Id*.
[267] *Id*.
[268] *Id*.
[269] *Id*.
[270] *Id*.
[271] *Id*.
[272] Masai Technologies Corp. v. United States, 77 Fed. Cl. 433, 448 (2007) (citing ARINC Eng'g Servs., L.L.C. v. United States, 77 Fed. Cl. 196, 202 (2007)).
[273] Gordon, *supra* note 251, at 32.
[274] *Id*. (citing 31 U.S.C. §§ 3551-56, and 28 U.S.C. § 1941(b)(4)).
[275] FAR, *supra* note 27, at 33.103(e).
[276] Gordon, *supra* note 251, at 34.

establish taint.[277] If that taint is proven to have existed, then the follow-on issue is whether any harm was actually done in regards to the OCI.[278]

A second type of OCI can occur in situations where performance of a contract, rather than the awarding of it, can lead to a future OCI if a particular company is awarded the contract.[279] This situation generally arises when a contractor is hired to perform some service, and then that same contractor, or more frequently a related company or subcontractor, is responsible for evaluating the quality of the general contractor's services.[280]

In either of these situations, the associated contractor has a duty to identify and evaluate potential OCIs as early in the acquisitions process as possible.[281] The contracting officer must avoid, neutralize, or mitigate significant OCIs before contract award.[282] There is also a provision for waiving rules regarding OCIs when doing so is deemed to be in the government's interest.[283] But when protests have been upheld on OCI grounds, the situation usually involves an agency failing to recognize an OCI, or if it did recognize the OCI, it failed to adequately deal with it.[284] In these situations, the GAO and the COFC appear to show little deference to the government's position.[285] Obviously, in "unequal access to information" OCI cases, the government could alleviate or mitigate the problem by sharing information with all competing offerors, if they are cleared to have access to that information.[286] Fortunately, if the DOD takes steps to aggressively address potential OCI situations by avoiding, neutralizing, or mitigating them, the GAO and COFC appear ready to deny protests concerning them.[287] Also, when a contracting officer identifies a contractor that might create an OCI and excludes it from a competition, the GAO and COFC appear to be reluctant to uphold a protest from the excluded contractor.[288]

Thus, in the context of the DOD taking a role in protecting the critical IT infrastructure of the DIB, the ultimate concern in awarding future contracts will probably be those situations where a particular company has unequal access to information. In this case, one might question whether threat and vulnerability information related to a

[277] *Id*.
[278] *Id*. at 35.
[279] *Id*. at 36.
[280] *Id*. at 36-37.
[281] FAR, *supra* note 27, at 9.504(a)(1).
[282] *Id*. at 9.504(a)(2).
[283] *Id*. at 9.503.
[284] Gordon, *supra* note 251, at 38.
[285] *Id*.
[286] *Id*.
[287] *Id*. at 39.
[288] *Id*. at 40.

contractor's, and even the DOD's, IT infrastructure may give that contractor an unequal access to information that places it in such an advantageous position that it becomes the favorite for the awarding of contracts. Again, the threat and vulnerability information a current contractor possesses places that contractor in a better position to argue that its IT infrastructure is secure. It further allows that contractor to claim that not only is its infrastructure secure, but it has already been certified, to some degree, by the DOD. Certainly, this provides the contractor with some advantage in future procurement projects. But, does it create a true OCI?

Using the analysis above, one must first analyze whether there is a "conflicted party." One could imagine a situation that would involve a conflicted party in the context of information sharing. For example, assume a current defense contractor (Contractor A) continually undergoes meaningful dialogue with the DOD about threats and vulnerabilities regarding its IT infrastructure. Also, assume these discussions result in Contractor A obtaining various software patches or other means by which to make its IT infrastructure secure to a level satisfactory to the DOD.

Further, assume that Contractor A and DOD together routinely test the known vulnerabilities and search for new ones. Contractor A gives significant input into searching for vulnerabilities and providing solutions regarding its IT infrastructure and the DOD's infrastructure, to include best methods for the two to interface, to the extent that the infrastructures almost become one. Then, at some point the DOD decides it needs some other contractual support for another one of its missions. Next, the DOD determines that the mission requires an IT infrastructure that possesses a certain level of security. Assuming Contractor A attempts to obtain the contract, Contractor A might then be a conflicted party based on the fact that it had access to information about the existing IT infrastructure that no other competitor for that contract would be authorized to have. At that point, Contractor A would likely be considered a "conflicted party."

Assuming that Contractor A is a conflicted party, then the next question is fairly simple to answer. Does Contractor A have some interest in its involvement in this process? Given the fact that the Contractor A is now bidding for a new contract with the government, it is clear that Contractor A has a financial interest in obtaining the contract.

Finally, does Contractor A have some responsibility to the third party in this scenario, the DOD? It appears so, maybe on two levels. First, Contractor A already has a significant working relationship with the DOD. In fact, not only is Contractor A privy to information about its and the DOD's IT infrastructure, it has been actively involved in testing vulnerabilities and modifying the infrastructure to the extent that

Contractor A's infrastructure and the DOD's nearly merged into one. The situation now exists that, based on its access to certain information, only Contractor A, or others using its interfacing methodologies, can interface with the DOD IT infrastructure. Secondly, Contractor A may be involved in establishing the criteria by which the body that selects the winner of the new contract measures the security level of each competitor's IT infrastructure. In other words, Contractor A becomes, in essence, the evaluator of each competitor's compliance with the established security requirement for the new contractor's IT infrastructure. Either of these situations would lead one to believe that Contractor A has some significant responsibility with respect to DOD concerns.

At this point, all three elements exist for a potential competitor to protest either the solicitation for the award, or the actual awarding of the contract to Contractor A. Does that necessarily mean that Contractor A may not be allowed to bid for or win the contract? First, any OCI could be eliminated by the DOD providing all competitors with whatever information they need to secure their IT infrastructure and to interface with the DOD systems. Then Contractor A would not have any advantage based on its prior dealings with the DOD. Second, even if the competitors did not receive the threat and vulnerability information, if the contracting officer becomes aware of the potential OCI, he or she needs only to neutralize or mitigate the conflict. This could be done in any number of ways, but sharing the information with the competitors seems to be the optimal solution. Finally, the head of the agency, in this case the DOD, may waive conflict rules, upon a written request and a determination by the agency head that it is in the government's interest to do so.[289]

V. OPTIONS

Given the foregoing potential contractual liabilities, what are the Air Force's options relative to the mandate that the DOD assist in protecting critical DIB infrastructure? There are some graduated solutions to this issue. First, at the most minimal level, the Air Force can negotiate memoranda of agreement (MOAs) with defense contractors currently operating under contract with the Air Force. This is obviously a reactive response to the problem and requires cooperation from the private sector businesses. The government cannot impose mandatory information-sharing on the private sector under current law, and the Air Force and its DIB partners would have to reach some consensual agreement. But, it would seem to be in the best interest of all parties to enter into such agreements, in light of the capabilities that

[289] FAR, *supra* note 27, at 9.503.

both parties possess. Any such MOA should include provisions for safeguarding information, with the understanding that there may be some legal issues as to enforcement of these safeguard provisions if the private sector passes information directly to the Air Force. There appears to be no statutory guarantee to protect information passed in this manner from disclosure. One adjustment to this option is to have contractors submit information directly to the DHS through its PCII Program, but this appears to be an inefficient way to conduct business, and the DHS may not be able to fully protect information passed for purposes other than protecting critical infrastructure from terrorist attack.

A second option is to require protection in all future contracts with DIB partners. This option targets future DIB partners and current partners on future endeavors. Within this option there are additional choices on how to approach information-sharing. First, future contract solicitations could mandate that all competitors prove their IT infrastructures meet some level of security. The solicitations could describe the required level of security and offer DOD resources to evaluate security compliance. Once the competitor's IT infrastructure is deemed adequate, the contract could mandate that the DIB partner pass on all information related to its IT infrastructure to the Air Force and also allow for routine Air Force inspections of systems to ensure continuing compliance with these requirements. Again, there may be some information safeguarding issues with this approach, and efforts must be made through the procurement process to ensure that no one competitor obtains an unfair advantage over its other competitors.

A less desirable sub-option in the contract arena might be for the Air Force to instead offer the same level of protection for potential contractors who are not already part of the DIB as that received by current DIB contractors. This is an unappealing resolution for a number of reasons. First, it really does not improve the situation over its current status. In essence, it only formalizes information included in the MOAs suggested above into the contract process. Second, this option relies much too heavily upon voluntary cooperation with DIB contractors. However, this option does avoid the opportunity for any competitor to argue that it has not received the same treatment as existing DIB partners.

The most aggressive and comprehensive approach to overcome this obstacle is the passage of new legislation or, at a minimum, amendments to current regulations such as the FAR. A new federal statute could mandate IT security for all DIB members and could include information-sharing, compliance assessments, and information safeguard provisions. The statute could mirror those applicable to the DHS within the Homeland Security and CII Acts. In addition, the existing DHS structure, including the PCII Program, could probably be

simply modified. For example, the DOD could act as the conduit for throughput of information into the PCII Program from DIB members. This would avoid the potential issue that currently exists regarding a DIB member's ability to deal directly with DOD rather than having to volunteer information to the DHS only. The legislation should include non-terror protection issues such as attacks by state actors, criminals, and natural disasters, as well.

The new legislation approach would likely meet a great deal of resistance. No doubt business lobbies would object to mandates of this type. Also, the effort required to meet these statutory mandates would be extensive and expensive. In 2003, there were an estimated 250,000 firms in 215 distinct industries within the DIB.[290] Thus, any statutory requirement to protect these assets would be daunting. But does that mean an effort to create new legislation is impossible? Probably not, in fact, a model for the DOD may already exist.

The Department of Energy (DOE) is tasked as the sector-specific agency for critical infrastructure in the energy sector.[291] This sector encompasses 2,800 power plants and 300,000 oil and gas producing sites.[292] The DOE is responsible for protecting nearly every energy asset with the exception of commercial nuclear power facilities.[293] To assist the DOE in its efforts, Congress enacted the Electricity Modernization Act of 2005.[294] This act requires the owners and operators of the nation's electric power grid to, among other things, ensure reliability of the grid.[295] The act also establishes the Electric Reliability Organization to ensure that all energy sector partners comply with the reliability mandates of the act.[296] Given the similarity in size and importance of the DIB and energy sectors, could not a similar statute mandate some form of DOD protection of the DIB infrastructure? Could not the Air Force be designated as the compliance evaluator for critical DIB IT infrastructure, just as the Electric Reliability Organization does for the energy sector? These situations are not entirely analogous, but the similarities give rise to some thought that this is a potential framework for a solution to the DIB IT protection issue.

---

[290] TED G. LEWIS, CRITICAL INFRASTRUCTURE PROTECTION IN HOMELAND SECURITY: DEFENDING A NETWORKED NATION 50 (2006).
[291] NIPP, *supra* note 66, at 3.
[292] LEWIS, *supra* note 290, at 50.
[293] NIPP, *supra* note 66, at 3.
[294] Pub. L. No. 109-58, 119 Stat. 594 (2005).
[295] 16 U.S.C. § 824o (2006).
[296] *Id*. § 824o(a)(2), (c) (2006).

VI. CONCLUSION

Current law mandates that the DOD assist in the protection of private-sector DIB critical infrastructure from terrorist attacks. This infrastructure includes, among other things, information technology infrastructures within the DIB. The Air Force's creation of 24 AF provides a unique opportunity for the Air Force to use its capabilities to assist in this effort. While the other services are certainly tasked with protection of the critical infrastructures of the DIB, the Air Force could possess the organizational capabilities to address the IT portion of the infrastructure.

Several obstacles to these efforts exist, however. Current law, in the form of federal statutes, directives, and national plans and strategies, does not allow the Air Force to thoroughly accomplish this mission. Currently, participation by the private-sector DIB partners is almost entirely voluntary. The voluntary nature of these partners' participation extends to sharing of critical infrastructure information. While the information-sharing aspect of critical IT infrastructure protection is critically important, private-sector DIB members are reluctant to provide the information because they lack the assurance that this information, which can be classified or trade secret information, will be completely safeguarded. There may not be an appropriate mechanism that contains adequate statutory safeguards for DIB members to provide such information directly to DOD components. Plus, the mechanisms currently in place, which do appear to have adequate safeguards for this type of information, call for private companies to provide information to the DHS rather than the DOD, and only for terrorist-related protection of critical infrastructure rather than all-encompassing threats.

Even if private DIB members provide information to the DOD, potential contractual liabilities exist with relation to the protection of those members by DOD components. Many of these contractual obligations may eventually disappear if the correct avenue to handle DIB critical infrastructure is chosen. However, in the meantime, DOD components should be aware that protection of, or assistance with protecting, private-sector critical DIB IT infrastructure may result in litigation. Contracting officers within organizations such as 24 AF should understand how to vigilantly detect and avoid, or at least mitigate, any potential conflicts.

Nevertheless, options exist for addressing all of these issues. Current defense contractors should be approached regarding entering into MOAs establishing requirements to protect this infrastructure. All future contracts should require defense contractors to protect their IT infrastructure and to allow DOD evaluation assessments of the compliance in this area. But, given the importance of the defense

industry to the success of DOD missions, a more permanent solution is needed. The natural permanent solution is new legislation or amendments to current regulations. Congress should enact a national defense-oriented statute that mirrors DHS statutes related to homeland security. The statute should address not only terrorist threats but should be flexible enough to also address threats by state actors, criminals, and natural disasters, among others. Legislation should also address information safeguarding issues. The approach used with regard to the energy sector may also be a model for future DOD-related legislation.

The hurdle presented by this mandate is not insurmountable, and it is imperative that the DIB critical infrastructure be protected. Cheap, shortcut methods to address this issue will be insufficient to achieve the ultimate goal. Congress, at the urging of the DOD, should make this effort one of its highest priorities before an attack on these infrastructures proves how important they really are.

INFORMATION FOR CONTRIBUTORS

The Air Force Law Review publishes articles, notes, comments, and book reviews. The Editorial Board encourages readers to submit manuscripts on any area of law or legal practice that may be of interest to judge advocates and military lawyers. Because the *Law Review* is a publication of The Judge Advocate General's Corps, USAF, Air Force judge advocates and civilian attorneys are particularly encouraged to contribute. Authors are invited to submit scholarly, timely, and well-written articles for consideration by the Editorial Board. The *Law Review* does not pay authors any compensation for items selected for publication.

Manuscript Review. Members of the Editorial Board review all manuscripts to determine suitability for publication in light of space and editorial limitations. Manuscripts selected for publication undergo an editorial and technical review, as well as a policy and security clearance as required. The Editor will make necessary revisions or deletions without prior permission of, or coordination with, the author. Authors are responsible for the accuracy of all material submitted, including citations and other references. The *Law Review* generally does not publish material committed for publication in other journals. In lieu of reprints, authors are provided four copies of the issue containing their work.

Manuscript Form. Manuscripts may be submitted by disc or electronic mail in Microsoft Word format. Please contact the Editor at the address on the inside front cover for further formatting requirements and submission information before submitting articles. Authors should retain backup copies of all submissions. Footnotes must follow the format prescribed by A UNIFORM SYSTEM OF CITATION (18th ed. 2005). Include appropriate biographical data concerning the author(s), such as rank, position, duty assignment, educational background, and bar affiliations. The Editorial Board will consider manuscripts of any length, but most articles selected for publication are generally 60 pages of text or less, and notes or comments are generally 20 pages of text or less. The *Law Review* does not return unpublished manuscripts.

Distribution. *The Air Force Law Review* is distributed to Air Force judge advocates. In addition, it reaches other military services, law schools, bar associations, international organizations, foreign governments, federal and state agencies, and civilian lawyers.


THE JUDGE ADVOCATE GENERAL'S SCHOOL
UNITED STATES AIR FORCE