THE FOURTEENTH ANNUAL SOMMERFELD LECTURE[1]

THE WRONG QUESTIONS ABOUT CYBERSPACE

GARY D. BROWN[*]

If they can get you asking the wrong questions, they don't have to worry about answers.
—Thomas Pynchon, *Gravity's Rainbow*[2]

[*] Colonel (Retired), U.S. Air Force. Colonel Brown recently retired from a twenty-four-year career as U.S. Air Force Judge Advocate, culminating in his assignment as the first Staff Judge Advocate (SJA), U.S. Cyber Command (USCYBERCOM), Fort Meade, Maryland. The U.S. Cyber Command is responsible for planning and conducting operations in and through cyberspace, as well as operating and defending Department of Defense (DoD) cyber networks.

Before his assignment at USCYBERCOM, Colonel Brown served five tours as a SJA or Senior Legal Advisor at the Combined Air Operations Center, Southwest Asia, Senior Officials Directorate, Air Force Inspector General's Office, 20th Fighter Wing, Shaw Air Force Base, South Carolina; 422d Air Base Squadron, Royal Air Force, Crouhton, England; and 363d Air Expeditionary Wing, Prince Sultan Air Base, Saudia Arabia. He also served as Chief of International and Operational Law at the U.S. Strategic Command and in installation legal offices at Howard Air Force Base, Royal Air Force, England and Whiteman Air Force Base, Missouri.

Colonel Brown is a prolific author and speaker. His work has appeared in the *Military Law Review*, *Naval Law Review*, *Military Review*, *Journal of Military Ethics*, *JAG Magazine*, *Strategic Studies Quarterly* and *Joint Force Quarterly*. He wrote the first chapter on cyber operations for *Air Force Operations and the Law*, a publication similar to *The Judge Advocate General's Legal Center and School Operational Law Handbook*. He frequently presents on cyber issues to military and civilian audiences. He was the keynote speaker at cyber conferences at Berkeley and George Washington University during the past year, in additional to presentations at many other events.

His military decorations include the Defense Superior Service Medal, Bronze Star Medal, Defense Meritorious Service Medal, Meritorious Service Medal (with three oak leaf clusters), and addition expeditionary medals. In 2001, the Air Force selected him as the Albert M. Kuhfeld Outstanding Young Judge Advocate of the Year, and in 2012 honored him with the Thomas P. Keenan, Jr. award for his superior contributions to the development of international law and military operations. Upon retiring from the Air Force, he joined the Washington Delegation of the International Committee of the Red Cross as the Deputy Legal Advisor, where he provides advice on the protection of civilians in armed conflicts, customary international law, new warfare technologies and the scope of the battlefield, among other areas.

[1] Established in 1999, the Sommerfeld Lecture series was created at The Judge Advocate General's Legal Center and School to provide a forum for discussing current issues relevant to operational law. The series is named in honor of Colonel (Ret.) Alan Sommerfeld. A graduate of the 71st Officer Basic Course, Colonel Sommerfeld's Army judge advocate career was divided between the Active and Reserve Components. After six years of active duty, he became a civilian attorney at Fort Carson, Colorado, and then

I. Introduction

One of the first things to learn as one enters the field of cyber law and policy is that there are two ways to look at cyberspeed. On one hand, things happen fast. Packets of data travel incredibly rapidly and the machines that make up the Internet react almost instantly. This kind of speed defies description and human understanding. For example, information traveling through the Internet can make a round trip between the United States and Europe in about 70 milliseconds, or around fourteen times in a second. That means that in the time it takes you to read this sentence, it can cross the Atlantic 140 times. When it comes to Internet speed, superlatives lose their meaning; we can just say "fast."

On the other hand, when we talk about cyber policy and law, rather than a cyber operation that has been launched, "cyberspeed" is fundamentally different. In 1998, the U.S. government officially made critical infrastructure protection a national goal and set out a strategy for cooperation between the government and the private sector to protect systems essential to the nation's security.[3] Sadly, fifteen years later, implementation of a plan to defend critical infrastructure is still pending, although the threat to it has increased. In 2013, the height of cyber policy achievement is an Executive Order and a Presidential Policy Directive that both, at their heart, say U.S. government agencies should cooperate among each other and private industry to ensure the nation's cyber security. The cyber provisions of the Standing Rules of Engagement for the Department of Defense (DoD), due for an update by 2010, were still incomplete as of the date of this writing.[4] Classified Presidential Policy Directive (PPD) 20, as reported by the *Washington*

at the Missile Defense Agency. He continued to serve in the Army Reserve, and on September 11, 2001, Colonel Sommerfeld was the Senior Legal Advisor in NORAD's Cheyenne Mountain Operations Center, where he served as the conduit for the rules of engagement from the Secretary of Defense to the NORAD staff. He was subsequently mobilized for two years as a judge advocate for Operation Noble Eagle and became a founding member of the U.S. Northern Command (USNORTHCOM) legal office, where he served as its Deputy Staff Judge Advocate and then interim Staff Judge Advocate. He retired from the Reserves in December 2003.

[2] Thomas Pynchon, Gravity's Rainbow, V262 (1973).

[3] PRESIDENTIAL DECISION DIR./NSC 63, CRITICAL INFRASTRUCTURE PROTECTION (May 22, 1998).

[4] Amber Corrin, *Cyber Rules of Engagement Still Unfinished*, FCW (Nov. 1, 2012), http://fcw.com/Articles/2012/11/01/cyber-rules-of-engagement.aspx?Page=1.

Post, was an attempt by the Executive Branch in 2012 to clear up years of debate over the appropriate role of the military in cyber operations and the definitions of cyber offense and defense. According to an official quoted in the article, the PPD "will spur a more nuanced debate" over cyber policy.[5] So, compared to the technology and the growing threat to national security, the development of policy and law relevant to cyberspace is slow.

My experience with cyber law and policy began in 1998 when the DoD was starting to develop policy on cyber operations. I moved from that assignment in 1999 and had little involvement in cyber operations law after that until I was assigned as Staff Judge Advocate (SJA) of the Joint Functional Component Command–Network Warfare (JFCC-NW)[6] in 2009. I was dismayed to discover that the U.S. government (and academia) was continuing to struggle to answer the same questions. We had made little progress.

Even since 2009, little ground has been gained in developing U.S. cyber policy. The progress made has been driven by outside events, three of which are highlighted below. Three incidents led to the advancement of the cyber discussion in the United States. This should come as no surprise, because history shows in times of challenge, those who do not straighten their own lines have them straightened by the adversary. One might conclude from these three critical situations that the United States was fortunate to have relatively minor incidents to provide the motivation to straighten its cyber lines: Operation Buckshot Yankee in 2008, Stuxnet Reporting in 2010, and Shamoon in 2012

[5] Ellen Nakashima, *Obama Signs Secret Directive to Help Thwart Cyber Attacks*, WASH. POST (Nov. 14, 2012), http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military- role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_print.html.

[6] Joint Functional Component Command–Network Warfare (JFCC-NW) became U.S. Cyber Command in 2010.

II. Operation Buckshot Yankee (2008)[7]

In 2008, the DoD's classified military computer networks were compromised by malware. A flash drive pre-loaded with targeted malware was inserted into a military computer at a U.S. base in the Middle East. The malicious code copied itself onto U.S. Central Command's computer network, from which it spread across the military system, infecting both classified and unclassified computers. The malware was designed to discover what information resided on the network, report that information back to its controller and then export information chosen by the controller. The DoD concluded the malware was distributed by a foreign intelligence agency.[8]

This operation established beyond a shadow of a doubt there was a cyber threat to U.S. national security, extending even to classified computer systems previously thought to be secure.[9] As a result of this action, the DoD established U.S. Cyber Command to integrate cyber defense activities in the department and changed many procedures regarding cyber security within the DoD. These changes also resulted in a deeper discussion of the connection between cyber security and national defense.

III. Stuxnet Reporting (2010)

The second important event was the Stuxnet incident in 2010, which the U.S. government declines to discuss, but has been widely attributed to the United States and Israel in the press.[10] Because the United States did not publicly disclose anything about Stuxnet, it was not the event itself that drove policy forward. The in-depth reporting of the incident was the relevant factor.

[7] William Lynn & Nicholas Thompson, *Defending a New Domain*, FOREIGN AFF. (Sept./Oct. 2010).

[8] *Id.*

[9] Ellen Nakashima, *Cyber-Intruder Sparks Massive Federal Response—and Debate Over Dealing with Threats*, WASH. POST, Dec. 8, 2011, *available at* http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html?hpid=z2

[10] William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, *available at* http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0

Simply put, Stuxnet was a precision-guided virus, aimed at the industrial control systems running Iran's uranium enrichment facility at Natanz. It was distributed by a self-replicating worm that propagated over computers running the Windows operating system.[11] Ultimately, the virus found its way to the target and destroyed around a thousand high-tech centrifuges at the Natanz facility, setting back Iran's nuclear weapons program by at least two years.[12] An interesting side note for lawyers is that the collateral damage prevention aspects of Stuxnet that, for example, limited the number of times an infected device could pass on the virus to three and caused the entire virus to delete itself on a given date, telegraphed that it was the work of a Western government. No independent hacker or criminal would bother with such niceties.[13]

Stuxnet was the first time a cyber activity could indisputably be labeled a cyber attack, and provided an actual context in which lawyers, strategists, scholars, and policymakers could debate the issues surrounding the use of cyber as an instrument of national policy.[14] It was one of the first examples, and the best example, of state practice in the area, so it was important for the development of international norms. These advantages came about as a result of reporting on the incident, not because the United States or Israel chose to discuss it.

IV. Shamoon (2012)

In an October 11, 2012, speech, Secretary of Defense Panetta called attention to the August 2012 cyber events experienced by the Saudi Arabian State Oil Company, Aramco and by RasGas of Qatar.[15] He

[11] Michael Joseph Gross, *A Declaration of Cyber War*, VANITY FAIR (Apr. 2011), http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

[12] David E. Sanger, *Obama Ordered Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (Jun. 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

[13] Ralph Langner, *Stuxnet's Secret Twin*, FOREIGN POL'Y, Nov. 21, 2013, *available at* http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack.

[14] Robert Windrem, *The Worm that Turned: How Stuxnet Helped Heat Up Cyberarms Race*, NBC News Investigations, Jun. 27, 2013, *available at* http://investigtions.nbcnews.com/_news/2013/06/27/19175276-the-worm-that-turned-how-stuxnet-helped-heat-up-cy-berarms-race.

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

described how the "Shamoon" malware overwrote some system files on about 30,000 computers.[16] These computers, according to the Secretary, were "rendered useless and had to be replaced."[17] Secretary Panetta indicated use of the Shamoon malware against the energy companies marked "a significant escalation of the cyber threat."[18] He went on to state that intruders had gained access to industrial control systems in the United States and the unnamed intruders continue working to develop advanced attack tools against U.S. chemical, electrical, water, and transportation systems.

Even before the DoD weighed in on the issue, a State Department Legal Adviser gave a comprehensive statement on how international law applies to conflicts in cyberspace.[19] Mr. Koh did not specifically tie his statement to Shamoon, but the timing indicates the two may have been related. The Shamoon event served as a wake-up call, as previous incidents had not, that the U.S. government really needed to do something about defending national infrastructure from cyber aggression.[20]

Perhaps the biggest challenge in developing policy and legal guidance for cyber operations is that the people who understand cyberspace and cyber operations are not interested in writing policy, and the lawyers, who are largely responsible for interpreting law and

[16] Gregg Keizer, *Shamoon Malware Cripples Windows PCs to Cover Tracks*, COMPUTERWORLD, Aug. 17, 2012, *available at* http://www.computerworld.com/s/article/9230359/Shamoon_malware_cripples_Windows_PCs_to_cover_tracks.

[17] On this point, the Secretary's statement is inconsistent with technical accounts of the incident, which suggest the computers were disabled but not destroyed. Kelly Jackson Higgons, *New Targeted Attack Destroys Data at Middle East Energy Organization*, DARK READING (Aug. 16, 2012), http://www.darkreading.com/advanced-threats/167901091/security/news/240005715/new-targeted-attack-destroys-data-at-middle-east-energy-organization.html.

[18] Ellen Nakashima, *Cyberattack on Mideast Energy Firms was Among Most Destructive, Panetta says*, WASH. POST, Oct. 11, 2012, *available at* http://articles.washingtonpost.com/2012-10-11/world/35502244_1_crucial-system-files-shamoon-secretary-leon-e-panetta.

[19] Harold Koh, *International Law in Cyberspace*, USCYBERCOM Inter-Agency Legal Conference comments (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm.

[20] Byron Acohido, *Why the Shamoon Virus Looms as Destructive Threat*, USA TODAY, May 16, 2013, *available at* http://www.usatoday.com/storycybertruth/2013/05/16/shamoon-cyber-warfare-hackers-anti-american/2166147/.

authoring policy, are generally blissfully unpossessed of anything but the shallowest understanding of cyberspace. There is a reason for this.

Lawyers love to reason by analogy—even if it is said to be the weakest form of argument. Unfortunately, analogies fail us in cyber operations. Cyberspace is so different from physical space that most attempts to draw analogies are doomed to fail.

One example of how enamored attorneys can be of analogies is offered by Tom Standage's 1998 book *The Victorian Internet*, in which he describes the development and some early uses of the telegraph as similar to the Internet revolution.[21] Standage's book is a pleasant read, but let's face it, the telegraph does not come close to expressing what happens on the Internet (or in cyberspace).

The problem of analogies aside, perhaps the major reason there has been so little progress in answering questions about cyber operations is that we are asking the wrong questions. I often found myself during my career arguing that the legal adviser needed to be in the room with the senior officers asking questions about the operation, rather than having the commander's questions relayed after the meeting of the commanding gray beards. One of the primary roles of a legal adviser is to shape the questions before they are asked, but that is only possible when the lawyer is in the room early in the process.

When the topic of a meeting is cyber operations in any context, one of the inevitable questions that will land on the legal adviser's plate is whether "X" constitutes a cyber attack. Another common question is: does "Y" violate sovereignty?

One of the reasons we have not been able to reach satisfactory conclusions in cyber policy and law dilemmas is that we are asking the wrong questions. The remainder of this lecture suggests why the most common questions are not the best ones to ask, and offers some alternative ways to look at issues that might help jolt us from our intellectual paralysis in the area.

[21] TOM STANDAGE, THE VICTORIAN INTERNET: THE REMARKABLE STORY OF THE TELEGRAPH AND THE NINETEENTH CENTURY'S ON-LINE PIONEERS (1998).

In over three years as the senior attorney for the United States military cyber command, I was asked many questions about the law and policy surrounding cyber operations. I was asked these questions because of my position, not because I knew any more about them than anyone else. The mission of a judge advocate is to provide answers to commanders, which I did with the help of a phenomenal staff of young attorneys. Three of the most common question we were asked were:

—What is a cyber attack?
—Do non-destructive cyber activities violate national sovereignty?
—Are we militarizing cyberspace?

The first question on the list was far and away the most common, but the other two were frequently asked as well. Although all of these are thoughtful, reasonable questions, as set out below, our collective obsession with them is one reason advances in the policy and law surrounding cyber operations have been so few.

V. What Is a Cyber Attack?

Perhaps because no one has yet suggested a clever, more accurate term to replace it—that also sells newspapers—"cyber attack" remains the most common way to describe any noxious cyber incident. Our historical perspective is largely in the kinetic realm, where the term attack has fairly specific connotations and consequences, so the choice to use "cyber attack" is not without effect. Excessive concern over this question gets us nowhere, because the real answer is no help at all.

The unsatisfactory answer to "what is a cyber attack?" is: exactly what we decide is a cyber attack at a given time under given circumstances that cannot be determined in advance. As accurate as this answer is, it is completely unhelpful, of course. But if a nation determines it is under attack, it is obligated to respond in some meaningful way or risk losing the confidence of its population or its standing in the international community. The determination that something is an attack, which implicates the history and law relevant to attacks through history, has far-reaching consequences. As a result, both the attacking and the defending nation have a lot at stake in this determination.

The difficulty inherent in labeling something a cyber attack can be demonstrated by Iran's reaction to the Stuxnet event, described above. Although by most definitions the event constituted an attack because it physically destroyed equipment, Iran did not respond to it as if it were an attack.[22] There are many possible reasons for the nonresponse, but one of them is not that physically destroying something does not constitute an attack.[23] In this case, the government of Iran apparently decided it was not in its best interest to determine that Stuxnet was a cyber attack.

Since the 1990s, the DoD has been determined to use a broad definition of attack in its cyber discussions. It called aggressive cyber events "computer network attacks," or CNAs, which is 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."[24] As related to the international consequences of a real attack, the "dastardly Ds" of deny, degrade, disrupt, or destroy never made any sense. It is difficult to envision a computer operation, whether it is hacking or espionage or Stuxnet, that does not involve some element of at least disrupting or degrading a computer system. This low bar for defining cyber attacks bled any meaning from the phrase, yet made every action the DoD might have proposed sound like the first shot in World War III. The United States has never treated as attacks the relatively low-level cyber incidents it suffers, such as penetrations of the DoD and defense industry classified networks that would meet this definition. Inconsistently, however, U.S. government discussions still tend to define even proposed low-level U.S.-initiated action as "attacks," as that term has traditionally been

[22] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE r. 30 (2013) ("A cyber attack is a cyber operation, whether offensive or defensive in nature, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.").

[23] Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*," JOINT FORCES Q. (4th Quarter, 2011).

[24] This DoD term and definition remained nearly unchanged from 1998 until November 2012, when the term was removed from the *DoD Dictionary*. JOINT CHIEFS OF STAFF, JOINT PUB. 1-02, DOD DICTIONARY (Nov. 8 2010, as amended through Nov. 15, 2013).

used.[25] This disconnect has led to the United States being unable to mount an appropriate defense to cyber assaults, and unwilling to carry out the same type of operation in response.[26]

In any event, the issue of what constitutes a cyber attack may be a pertinent academic question, but has little meaning in political discussions unless it is in the context of an actual event. Any definition of cyber attack may not align well with political reality, with it sometimes being defined too strictly and sometimes too loosely. For example, if the press reports are correct about Stuxnet, and if the United States is a law-abiding nation, we have to assume the United States has determined that destroying critical pieces of a prime national security facility does not constitute a cyber attack—because then the Stuxnet operation would have been an illegal action by the United States. On the other hand, the United States has taken to complaining about Chinese espionage, threatening a variety of retaliatory actions—even though espionage is not considered to be prohibited by international law, and the United States is widely assumed (even if never proven) to engage in cyber espionage against China.[27]

During my time in the USCYBERCOM legal office, flying in the face of traditional DoD thinking, we tried to distinguish at the theoretical level between cyber operations that would result in kinetic effects, qualifying them as aggression under traditional definitions, and those activities with no direct effects in the physical world.[28] Our suggestion

[25] The new set of DoD definitions, unclassified but still unpublished at the date of this writing, include "offensive cyberspace operations," defined as "cyberspace operations intended to project power by the application of force in or through cyberspace." Perhaps time and practice will tell what this definition means; the words do not.

[26] *Pentagon Still Grappling with Rules of Cyberwarfare*, ASSOCIATED PRESS (Jul. 25, 2013), http://www.foxnews.com/us/2012/07/25/pentagon-still-grappling-with-rules-cyberwar/.

[27] *US Considers Firmer Action Against Chinese Cyber-espionage,* ASSOCIATED PRESS (Feb. 1, 2013), http://www.telegraph.co.uk/news/worldnews/asia/china/9841385/US-considers-firmer-action-against-Chinese-cyber-espionage.html; John Reed, *Rogers: U.S. Must Confront China on Cyber Theft and Espionage*," FOREIGN POL'Y (Feb. 13, 2013), http://killerapps.foreignpolicy.com/posts/2013/02/13/rogers_us_must_confront_china_on_cyber_espionage_and_theft; *Cyber War of Words: U.S., China Trade Blame for On-Line Security Threats* (Mar. 12, 2013), http://rt.com/usa/us-urges-china-stop-hacking-123/.

[28] It is important to note here that military units plan for and discuss contingencies that are never expected to occur. USCYBERCOM discussions on this point, and my

of the phrase "cyber disruption" to describe activities that are obnoxious but not forceful was met with cool indifference. We just could not think of a better way to say "undesirable cyber action directed against a friendly system that doesn't damage anything physically." We certainly could not think of one that was catchy enough for a headline.[29]

The United States, to date, has answered or, one might say, avoided the question this way.

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.[30]

Even though this statement provides no *definition* of what the United States considers a cyber attack, it does set out a basic understanding that there is a point at which the United States would equate cyber activity hostile enough to merit a response in self-defense. In other words, a cyber event will merit an aggressive response (i.e., will be a cyber attack) when we decide it is. Isn't this good enough? Strategic ambiguity in international relations can further national interests. There really is not a need to define the term. We just have to analyze each event in context, and that really is not much more difficult with cyber events than it is in the kinetic realm.

One example demonstrates the commonality between attacks, regardless of whether the vector is kinetic or cyber. In 2009 at the Shushenskaya dam in Russia, a 1,500 ton piece of equipment blasted through the floor of the dam's power station, shooting 50 feet into the

discussion of the point here, were academic and unrelated to any actual or proposed U.S. cyber operation.

[29] Gary D. Brown & Owen W. Tullos, *On the Spectrum of Cyberspace Operations*, SMALL WARS J. (Dec. 11, 2012), http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations (providing a more complete discussion of the way the USCYBERCOM legal office discussed the issues in this regard).

[30] *International Strategy for Cyberspace* (May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

air. The accident ultimately resulted in the death of 75 people and damaged or destroyed all ten giant turbines in the plant. The accident was *not* the result of a cyber attack, but it was partly due to an automatic control system performing poorly.[31] Such automated systems are vulnerable to cyber attacks, which could result in a catastrophe in the future.[32] If an event like this occurred, there just would not be any doubt about whether it merited a response in self-defense. International lawyers would want to discuss the scope, duration, and intensity of the event; political leaders would want to know if it was "an act of war."[33] No one would care about an academic definition of cyber attack.

The intellectual capital we have spent on this essentially unanswerable issue has been considerable, but it has not been wasted. The discussion has served as a vehicle for discussing larger issues in cyber operations, and the discussion will undoubtedly continue. The academic discussion should not prevent the advancement of practical policy and law in the area.

VI. Do Non-destructive Cyber Activities Violate National Sovereignty?

Both in literature and in policy discussions, this question frequently recurs. It is another question that, unless tied to a specific event, is unanswerable—and even then, it is difficult. The problem is, sovereignty is firmly rooted in geography. There is no universally agreed definition, but considerations of international sovereignty revolve around the recognition of a government's right to exercise exclusive control over territory, and this definition is ill-suited for cyber discussions. For convenience we might refer to "the geography of

[31] Joe P. Hasler, *Investigating Russia's Biggest Dam Explosion: What Went Wrong*, POPULAR MECHS. (Feb. 2, 2010), http://www.popularmechanics.com/technology/engineering/gonzo/4344681.

[32] Video, *Staged Cyber Attack Reveals Vulnerability in Power Grid* (Sep. 27, 2007), http://www.youtube.com/watch?v=fJyWngDco3g.

[33] Although politicians also often ask what constitutes an "act of war," lawyers usually dismiss the question as an archaic reference to pre-United Nations international law. However, as used by politicians today, it really is a shorthand way of combining the questions of whether something is an aggressive act and whether it is serious enough to merit an aggressive response in self-defense. In those terms, it is a perfectly relevant question, but one that cannot be answered in the abstract and is beyond the scope of this article.

cyberspace," but I challenge you to point to cyberspace. Although cyberspace is all around us, when trying to point at it you will be as unable to as the Square in Abbott's *Flatland* was to point at "up."[34] I always found it troubling to hear military commanders talk in terms of seizing the cyber "high ground" or negotiating "cyber terrain." That was language they were comfortable with, but in any meaningful sense of the word, cyber lacks geography.

United Stated officials have articulated some thoughts on the idea of cyber sovereignty. One instance was in Harold Koh's speech at USCYBERCOM. In response to a question he asked himself on the role of State sovereignty, he answered:

> States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict. The physical infrastructure that supports the internet and cyber activities is generally located in sovereign territory and subject to the jurisdiction of the territorial State. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered.[35]

Mr. Koh's statement separated the supporting physical infrastructure from the Internet and cyberspace. This separation allows a discussion to take place within the familiar confines of geography. The assertion that physical infrastructure supports the Internet is certainly true, but fails to ascertain a fresh discussion of sovereignty in the modern world, which we might refer to as cyber sovereignty.

If the physical location of Internet infrastructure constituted the entire subject matter of cyber sovereignty, the discussion would be a

[34] E.A. ABBOTT, FLATLAND: A ROMANCE OF MANY DIMENSIONS (1884).

[35] Harold Koh, State Dep't Legal Adviser, *International Law in Cyberspace* (Sep. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm (comments at the USCYBERCOM Cyber Law Conference).

short one. Activities that had an effect on infrastructure located in a country would quite often impact sovereignty of the host nation. Unfortunately, it is not the cables, routers, servers, etc., that make the Internet what it is. Is the connection of those pieces of physical equipment to the larger enterprise. A Cisco router might cost $100,000, but if it is used to connect a country to the incredible engine of commerce, art, scholarship, science, and growth that we call the Internet, its value is incalculable. However, along with this connection comes some necessary surrender to common use what might otherwise be considered sovereign space. Activating a connection to the Internet requires allowing packets of all sorts from all over the world to flow through equipment; it is simply the way the Internet works.

By contrast, nations do not allow people, planes, ships, etc. unfettered access and transit across their physical territory.[36] Cyber activities are simply different than traditional physical activities and for this reason, cyber sovereignty is by its nature less complete than traditional sovereignty. Countries that desire to retain full sovereignty over the pieces of Internet infrastructure they own can simply unplug them from the Internet. A country can feel fairly confident in exercising full sovereign control over a router sitting in a box in a government office. If it wishes to add the value of an Internet connection to the router, the reality is the quantum of its sovereign control over the device has changed.

A brief explanation of one aspect of how the Internet operates may help bring all this into focus. Information sent over the Internet is divided into pieces called packets, designed as a method to ensure reliable delivery in an efficient manner. The Internet is designed to route these packets individually by the most efficient route at that time (which constantly varies because of many factors, such as volume of traffic) and reassemble them at the destination. Imagine this: you live in Washington, D.C., and you want to send a letter to a friend in Seattle. Would you ever think of writing out the message, then tearing it into little bits with around two dozen words on each piece, copying the address for the destination and origin on each bit of paper, and then sending them off in multiple different directions, including both west

[36] I recognize that although I criticize reasoning by analogy, I do it, too.

across the United States and east across the Atlantic, Europe, Asia and the Pacific Ocean (i.e., the long way around the globe), all to be reassembled at your friend's house so she can read the message? Of course you would not—but your computer would. This is how the Internet handles information. Each message is split up—packetized—and then sent flying about the planet by the most efficient route as determined by Internet algorithms.

Add to this the complexity of cloud services that store "chunks" of data in various places, and it results in a system that quite simply defies geographic definition.

A final word about sovereignty. Traditionally, the limit of sovereignty was considered to be as much territory as a country could protect. This was embodied by the three mile limit of territorial seas; the distance is said to have been chosen because it was the range of a shore-based cannon.[37] That is, three miles from shore was as far as a country could defend, so it was *de facto* the limit of its sovereignty. This is in fact the situation in cyberspace now. Powerful cyber nations do what they can to defend their own Internet infrastructures, with some success. Weaker nations suffer what they must in cyberspace. Victim nations often, undoubtedly, never even know their Internet infrastructure is being used for foreign espionage or as a staging point for cyber criminals, hacktivists, and foreign government actors. In other words, cyber sovereignty extends exactly as far as each country can make it. That answer is unlikely to satisfy diplomats, but it is the best one available at the present—and is a good indication this is not a question that should stop the discussion of cyber strategy in its tracks.

VII. Are We Militarizing Cyberspace?

It is ironic this question is so common. The Internet started as a military communications platform. The Soviet nuclear threat indirectly led to the creation of the Internet. In the wake of Sputnik, the United States was concerned about a space-based nuclear attack. As a result, the

[37] H.S.K. Kent, *The Historical Origins of the Three-Mile Limit*, AM. J. INT'L L. (1954), http://www.jstor.org/discover/10.2307/2195021?uid=3739256&uid=2&uid=4&sid=21102009814067.

Advanced Research Projects Agency (ARPA; now Defense Advanced Research Projects Agency (DARPA)) started designing a nationwide communications network. ARPAnet went live in October 1969, with the first communications between University of California Los Angeles (UCLA) and Stanford. It began as a military project, has always been used by the military and national security infrastructures, and will remain military insofar as it is an essential element of strategic communications until an entirely separate platform is developed, which is farfetched.[38]

Perhaps a better question to ask would be "are we civilianizing military operations?" The increasing United States' use of drones for extraterritorial targeting has generated questions in the public and in Congress about the use of covert authorities to carry out what might be considered military operations. The raid that resulted in the killing of Osama bin Laden serves as an example of how a military operation can be civilianized. That operation was carried out by uniformed military members in the command of a military officer using military equipment, yet it was conducted and characterized as a covert Central Intelligence Agency operation.[39]

One possible reason the Administration used covert authorities for the raid, rather than traditional military authorities, is because there were questions about the propriety of entering Pakistan's sovereign territory, without permission, to kill or capture a terrorist. The same issues might plague proposed cyber operations. As questions surrounding cyber sovereignty and cyber military operations have remained unanswered, it might be appealing to use covert authorities to conduct operations because that will, at least from a United States policy perspective, obviate the need to disclose the legal and policy rationale supporting such operations. Public disclosure of the United States thinking about actual cyber operations would be valuable in the development of international law in the area. However, from a U.S. national perspective, it might be damaging, in that it would allow other countries to employ the same rationale in undertaking actions against the United States.

[38] *A Technical History of the ARPANET*, http://www.cs.utexas.edu/users/chris/nph/ARPANET/ScottR/arpanet/timeline.htm.

[39] Nicholas Schmidle, *Getting Bin Laden*, NEW YORKER (Aug. 8, 2011), http://www.newyorker.com/reporting/2011/08/08/110808fa_fact_schmidle?currentPage=all.

It remains to be seen how the United States will conduct military cyber operations in the future. From covert activities, the public will learn little—until something goes wrong. In traditional military operations, the DoD has disclosed its operations, resulting in taking its share of lumps from the scrutiny of the press, politicians and public.[40] In the end, this has made the DoD stronger. That fire-hardening rarely applies to operations undertaken covertly.

Both because of the increasing intermingling of military and intelligence operations and the military origin and continued use of the Internet, questions about militarizing cyberspace simply miss the point.

There is one question the United States government must answer before it can artfully engage in the cyber game—what is the best way to *organize* for cyber operations? The challenge is there are many government organizations that lay claim to portions of cyber activities, and all of them have an interest in preserving their link to cyber because it's one of the few government areas that continues to grow in people and resources.

The Department of Homeland Security (DHS) tells other agencies to keep their hands off cyber security, and tells the DoD, it can only do cyber defense—even though Congress does not think DHS is up to the task of handling cyber security.[41] The DoD says USCYBERCOM must be co-located with the National Security Agency (NSA) and they will

[40] Noah Schactman, *Military Stats Reveal Epicenter of U.S. Drone War*, Wired (Nov, 9, 2012), http://www.wired.com/dangerroom/2012/11/drones-afghan-air-war/. Unfortunately, however, the U.S. Air Force has recently stopped disclosing statistics about its drone operations, presumably because the scrutiny surrounding the targeted killing program has increased. Reuters, *U.S. Air Force Stops Reporting Data on Afghan Drone Strikes*, Reuters (Mar. 10, 2013), http://www.reuters.com/article/2013/03/10/us-usa-afghanistan-drones-idUSBRE92903520130310.

[41] Homeland Security Presidential Dir.-7, Critical Infrastructure Identification, Prioritization & Protection (Dec. 17, 2003), http://www.dhs.gov/homeland-security-presidential-directive-7; Congressional testimony of DHS Secretary Janet Napolitano (Mar. 7, 2013), http://www.dhs.gov/news/2013/03/07/written-testimony-dhs-secretary-janet-napolitano-senate-committee-homeland-security; William Jackson, *McCain Slams DHS, Wants DoD to Defend Cyberspace*, GCN (Mar. 27, 2012), http://gcn.com/articles/2012/03/27/cyber-defense-hearing-mccain-slams-dhs-favors-dod.aspx. Also, DHS Secretary Napolitano stressed at a *Washington Post*-sponsored cyber event on October 31, 2012, that the DoD's role in cyber *defense* was separate from the DHS role of cyber *security*.

handle cyber defense for the whole nation.[42] The nation tells the NSA to stop reading our e-mail.[43] The Department of State (DoS) says the United States will take action to protect the nation from Chinese cyber threats, although the specified "cyber threats" sound a whole lot like spying, and we all know espionage is not unlawful internationally.[44] Congress says we have to do something about cyber security, but cannot pass a bill.[45] The executive branch has been saying "we've got it" (for three-plus years now), and the President has now issued documents that say, in essence, why can't we all just get along?[46]

President Obama's executive order and policy directive on the cyber security of the nation's critical infrastructure essentially follow the same path of previous government studies and documents, which is a "Whole of Government" approach. This concept may sound appealing, but it disguises a lot of confusion.

During my three years as a cyber legal adviser, when I briefed, I often included a slide on what I called perhaps the most important, and definitely the most boring, part of U.S. cyber warfare: command and control (C2) of military cyber forces.

[42] General Keith Alexander Congressional Testimony (Sep. 23, 2010), http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/House%20Armed%20Services%20Subcommittee%20Cyberspace%20Operations%20Testimony%2020100923.pdf; Secretary of Defense Leon Panetta Remarks (Oct. 11, 2012), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[43] James Risen & Eric Lichtblau, *E-Mail Surveillance Renews Concerns in Congress*, N.Y. TIMES (Jun. 16, 2009), http://www.nytimes.com/2009/06/17/us/17nsa.html?pagewanted=all.

[44] Tom Donilon, Nat'l Security Advisor to the President Remarks, The United States and the Asia-Pacific in 2013 (Mar. 11, 2013), http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

[45] Benjamin Wittes, *Lawfare* blog, http://www.lawfareblog.com/2013/02/allan-friedman-on-why-the-executive-order-on-cyber/ (quoting Allan Friedman and noting, among other things, that Congress has failed to pass a cybersecurity bill since 2001).

[46] Executive Order, Improving Critical Infrastructure Cybersecurity (Feb. 12, 2012), http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity; PRESIDENTIAL POLICY DIRECTIVE 21, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Feb. 12, 2013), http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

The United States established Cyber Command and recently announced it would be growing from about 900 personnel to about 4,900 personnel.[47] Given this, it is clear the United States plans for the military to serve a large role in the nation's cyber security. The question that has not been answered is how the military will organize. Cyberspace operations present two specific challenges for a Defense Department largely organized around geographic combatant commands (e.g., Pacific Command, Southern Command, etc.) and kinetic functionality (e.g., 9th Air Force, 1st Infantry Division, 5th Fleet, etc.): cyber is not geographic and it largely is not kinetic. The third great challenge in organizing the DoD for cyber operations is that such operations have an unclear and sometimes uncomfortable relationship with intelligence. This last point is most clearly illustrated by the DoD's insistence that the commander of U.S. Cyber Command be the same person who directs the National Security Agency, which was followed by congressional expressions of concern over that very relationship.[48]

At a minimum, any laydown of cyber military forces must do two things. It must clearly identify precisely who is in charge of all the forces and it must carve out specific mission space for the military forces. In my opinion, the structures proposed do precisely the opposite of these, both obfuscating who is charge and attempting to divide the mission into artificial service functionalities. Illustrations of the USCYBERCOM chain of command include overlapping lines of authority, dual—and even triple-hatted positions, and unclear divisions between military and intelligence operations, among many other issues. The U.S. Government Accountability Office (GAO) made similar observations about the lack of clarity in the cyber command chain in 2010 and 2011.[49]

[47] Jason Healey, *Cyber Command Expanding Five Fold*, NEW ATLANTICIST (Jan. 29, 2013), http://www.acus.org/new_atlanticist/cyber-command-expanding-five-fold.

[48] Defense Authorizations Act, Fiscal Year 2013, Pub. L. No. 112-705 § 940 (Jan. 3, 2012), http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112jr4310enr.pdf (discussing "Sense of Congress on the United States Cybe Command).

[49] *See* U.S. GOVERNMENT ACCOUNTABILITY OFFICE, GAO-10-338, PROGRESS MADE BUT CHALLENGES REMAIN IN DEFINING & COORDINATING THE COMPREHENSIVE NATIONAL INITIATIVE (Mar. 2010), http://www.gao.gov/new.items/d10338.pdf; U.S. GOVERNMENT ACCOUNTABILITY OFFICE, GAO-11-75, DOD FACES CHALLENGES IN ITS CYBER ACTIVITIES (Jul. 2011), http://www.gao.gov/new.items/d1175.pdf. The cleverly designed mock three-dimensional graph on page 18 of the latter

VIII. Conclusion

A frequently heard complaint at cyber law conferences is that presenters continually point out the same thorny questions, but rarely provide any answers. In that regard, I must apologize for, at least on one level, contributing to that problem.

On the other hand, I hope that by noting the wrong questions that are being asked, I may have furthered the debate a bit. That is, if the wrong questions are being asked, even the correct answers to them will get us nowhere.

Some of the right questions suggested here are: How should the United States organize for cyber warfare? What cyber actions by an adversary would justify and demand an aggressive response from the United States—and what U.S. cyber actions would result in aggressive responses from the victim?

Finally, perhaps sweeping the wrong questions from the table will open debate on the most important question of all. The promise of cyber warfare has always been a more precise, less lethal way to wage war. When nations engage in armed conflict in the future, use of cyber warfare techniques might make the struggle less devastating to the civilian population. Far too little intellectual capital has been spent on this aspect of cyber capabilities, and I will end by asking one final question: How can this new capability best be leveraged to wage war more humanely?

reference does not shed much light on how things actually work, but does provide a good illustration of just how confused the organization of cyber forces and leadership is.