The Most Governed Ungoverned Space: Legal and Policy Constraints on Military Operations in Cyberspace

Aaron F. Brantly

SAIS Review of International Affairs, Volume 36, Number 2, Summer-Fall 2016, pp. 29-39 (Article)

Published by Johns Hopkins University Press
DOI: https://doi.org/10.1353/sais.2016.0018

For additional information about this article
https://muse.jhu.edu/article/641158

Access provided by United States Military Academy (26 Sep 2017 16:18 GMT)

The Most Governed Ungoverned Space: Legal and Policy Constraints on Military Operations in Cyberspace

Aaron F. Brantly

Winning wars in cyberspace might sound easy: the click of a mouse or the press of the enter key on a keyboard. Yet, the web of networks that constitutes cyberspace is imbued with challenges. Seemingly every day there is a new story of a government, business, or individual, suffering from a serious hack. These hacks are often attributed to state actors or transnational criminal organizations. Combined, the almost daily revelations of serious incidents compound a common misperception that cyberspace is an ungoverned space. The reality of cyberspace, however, is far different and constitutes a complex environment of overlapping jurisdictions. The overlapping geographic, legal, and technical boundaries affect everything from the freedom of information to the decision to engage in military operations. Technical specifications as well as laws and policies established by local and national governments, international institutions, non-governmental organizations, and corporations form the decision-making framework for national policymakers and military commanders. Understanding how all the elements of cyberspace interact provides context for when, why and how the United States engages in military operations in cyberspace. This paper examines the complexities of the environment and their impact on the decisions of states (with emphasis placed on the United States) to engage in offensive cyber operations, cyber exploitation,[1] and defensive cyber operations against other states and non-state actors. Moreover, it examines the important role that overlapping governmental and non-governmental organizations have in affecting the types of behaviors that occur within cyberspace.[2]

The old adage, "on the internet no one knows you're a dog" is rapidly fading as anonymity fades away.[3] Borders abound on the internet. These borders fall along multiple jurisdictional lines and include everything from the provision of domain names and IP address space allocations to the physical devices that often constitute the edges of national and transnational network infrastructures. To assume that any given user sitting behind their screen is somehow outside of a governed space ignores both technical and geographic reality. The governance of the internet at all levels imposes overlapping legal and policy constraints that profoundly impact the decisions of states to act within this new and evolving area of operations. The internet is a contested space of governance in many ways, yet at its core it constitutes the most governed

Dr. Aaron F. Brantly is Assistant Professor of International Relations and Cyber in the Department of Social Sciences, Cyber Policy Fellow at the Army Cyber Institute and Cyber Fellow at the Combating Terrorism Center. He holds a Ph.D. in Political Science from the University of Georgia and a Master's of Public Policy from American University. His research focuses on national security policy issues in cyberspace including big data, terrorism, intelligence, decision-making and human rights.

ungoverned space in existence. Arguably every single attribute of the internet and its connected services is subject to some form of governance. The decision processes within both international politics and institutional politics from the supranational to the sub-state level govern the capacities and capabilities of all actors to interact.

The governance of the internet at all levels imposes overlapping legal and policy constraints that profoundly impact the decisions of states to act within this new and evolving area of operations.

To understand the legal and policy constraints on military operations resident within what the US military defines as an operational domain, one must start small in scale and historically distant and work up to the large-scale organizational decisions that are temporally present. The governance structures of the internet cannot be examined from a purely realist perspective without taking into consideration the construction of the underlying laws and policies that define the operational environment. While parsimony dictates that one must center any argument in a single level of analysis, such a starting point in the context of internet governance and state action ignores the crucial ontological foundations that govern how state and subs-state actors behave and interact.

At a macro-level of analysis, the internet is best defined as a socio-technical-economic system of systems.[4] At the micro-level, the internet and its connected devices and protocols, which define its operations, are rooted in code and hardware. Code according to Lawrence Lessig constitutes a form of law and establishes a logical structure that defines the basic operation of an environment.[5] In conventional domains of land, sea, air and space the laws of nature define what is and is not possible, but on the internet "code" is defined by programmers. The selection of certain protocols over others at the core of the internet has a historical basis in decisions that evolved from a small working group to a request for comment (RFC) process, and then to a more institutionalized structure of individual, state, corporate, and non-state interests engaging in non-governmental institutional structures. These organizations fall under the umbrella of the Internet Society with its partners the internet Architecture Board (IAB), the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF) and other governance organizations.[6]

Beyond the policies and protocols within the primary technical governance institutions listed above are local and national laws that govern issues such as data privacy, retention, registration of users, filtration of content, surveillance of individuals within a given jurisdiction, and more. Many nations, including the United States, are actively working to develop information sharing organizations to inform others of known vulnerabilities within software and hardware platforms within and across various types of organizations.[7] Where local and national law and policy have failed to fully achieve desired outcomes, states have turned to international working groups, treaties, and agreements on issues of transnational criminal behavior. States have also utilized informal commitments to normative behaviors and even the initial stages of acceptable

state behavior to collaborate. Meetings such as the United Nations Governmental Group of Experts (UN GGE),[8] the Budapest Convention,[9] and others each work towards developing legal, policy and normative frameworks for states and their citizens.

There is no other environment of state interaction where everything from the laws of the basic functioning of the environment to agreements on how individuals should behave within that environment, have been so clearly addressed. There is not a consensus on many of the higher-level normal behaviors that will be examined, yet constraints imposed by lower level agreements confine state actions to areas that are non-random and likely in conformity with the nuances of various aspects of international law.[10] It is not possible here to provide a lengthy analysis of all the governance structures above organizations and their areas of control, yet it is valuable to examine several in more detail in order to provide a measure of context for how and why states do what they do in cyberspace.

There is no other environment of state interaction where everything from the laws of the basic functioning of the environment to agreements on how individuals should behave within that environment, have been so clearly addressed.

The RFC Process and Protocol Design: The Basic Building Blocks of Governance

Despite the prognostications of movies such as *Eagle Eye* or the Bruce Willis Thriller *Live Free or Die Hard*, the underlying rules of the internet are not random, nor is the domain one in which magical strokes on a keyboard can be easily directed to disable an entire country. Rather, the basic functioning of the internet from its early days as a project under the Advanced Research Projects Agency (ARPA) to the present has been rooted in a technical egalitarian process based largely on technical need rather than political expedience or necessity. The process originated in 1969 with Steve Crocker and has been adapted and incorporated by the Internet Society and in particular the Internet Engineering Task Force.[11] RFCs propose actual standards as well specific draft areas for standards, internet standards for shared protocols, informational documents, and historical documentation. The objective of the RFC process is a largely open source technically meritocratic process to advance the best technical solutions. It is a working group focused process with emphasis placed on peer-review, consistency with existing norms, and technical rigor.[12]

One of the more interesting features of the Internet Society and its affiliated partners is its openness to the public at large. While state level actors can be involved in the Internet Society, their voices on any given RFC are no greater than a technical expert in any given field. The Society is open for anyone to become a member.[13] The openness of the structure is contentious in that it

pits state actors against a mixture of non-state actors and individuals in what is best known as a multi stakeholder governance model.[14] The results are technical specifications that might contradict traditional sovereign applications of law, but that facilitate efficiency and interoperability. However, as will be demonstrated, the lack of complete national control over the technical specifications opens doors for actions conducted in and through cyberspace that challenge sovereign state authorities.

Although there is not an overarching state or supranational entity, the Internet Society and its affiliates constitute a robust decentralized governance structure able to solve many of the issues traditionally associated with complex decision-making. In a complex commons in which inter-operative standards are necessary for the operation of the internet, the problem-solving capacity of the RFC process has resulted in much of the underlying technical framework upon which we depend today.

The standards developed through the organizational procedures of the IETF and the IRTF, under the guidance of Internet Architecture Board (IAB), establish the basic laws of nature for any action in cyberspace, including potential military actions. Standards, such as those that increase the security, decrease the openness, improve resilience, or make any number of other potential technical changes could be developed and approved. Any standard developed is likely to affect the potential for states to leverage cyberspace for military needs. Recognizing the important role that non-governmental organizations play in the development of the internet is critically important. Although many of the original members of these organizations had deep relationships with the US government, the trend has been shifting towards more international inclusion with a diversity of interests.[15] These international actors, each with different perspectives and experiences, will challenge the implicit or explicit interests of the United States. This challenge is likely to be minimal in the short term, as the overarching mission of these organizations remains largely centered in the maintenance of a high quality open inter-networked infrastructure.[16] However, as the multi-stakeholder nature of internet governance continues, it may result in outcomes unfavorable to the United States. The potential for undesirable outcomes in governance at the core level of standards development is often rooted in the interests of other state actors. The next section briefly takes up the challenge of an increasing desire by states to become involved in the governance of the internet.

The State in the Governance of the Internet

The internet developed largely outside the control of a single state and as a result its rapid proliferation around the world has challenged the sovereign jurisdictional boundaries of states in ways previously unencountered. The internet provides a vehicle for information distribution and financial transactions to occur outside of traditional state control.[17] In turn, these challenges have provided impetus for nations to focus on wrestling control of the internet into a supranational body better able to represent their policy preferences.

Many states outside of liberal western democracies see the International Telecommunications Union (ITU) as the body best suited for the task. The last major attempt to wrest control occurred in 2012 at the World Conference on Internet Telecommunications (WCIT) in Dubai. At this conference a series of International Telecommunications Regulations were combined into a treaty on the International Telecommunications Regulations (ITRs), which was reviewed and voted upon.

The internet developed largely outside the control of a single state and as a result its rapid proliferation around the world has challenged the sovereign jurisdictional boundaries of states in ways previously unencountered.

The ITRs[18] were designed to provide states with a greater role in overseeing the telecommunications services within their countries. The treaty was supported or opposed largely based on a states political system. Authoritarian leaning regimes were more supportive of the treaty and democratic regimes were more opposed. Within the vote there were a number of non-voting interest groups involved, including Google. Corporate actors are particularly loathe to relinquish their influence to states. A spokeswoman for Google was quoted in a 2012 Wall Street Journal article saying, "We stand with the countries who refuse to sign this treaty and also with the millions of voices who have joined us to support a free and open web."[19]

Actors at all levels disagree on the role of states in the management of the internet.[20] Corporate interests are largely aligned with states that argue against state control over the internet for fear of a fractured internet composed of nationally controlled network infrastructures with divergent rules and regulations or hardware and software standards.[21] While the 2012 failure of WICT appears to have been a body blow to state control of the internet, the 2013 release of classified materials by Edward Snowden seems to have given new life to state efforts at control.[22] Efforts by countries to change the fundamental rules associated with the transit of data have increased in the post-Snowden era.[23] The implementation of state control over the internet under the banner of privacy and sovereignty protections has risen to new heights in both democratic and less-than democratic states, whether with national laws and policies on data localization, internet localization, or a variety of other related issues. A fragmented internet, if it were to develop, would offer new challenges and opportunities to states who wished to leverage cyberspace for state actions.

Bi-lateral Norm Development and State Actions in Cyberspace

Beyond the formal non-governmental, governmental and supranational governmental structures of states are ad hoc agreements or bi-lateral negotiations between states that build on existing legal and normative structures to establish commonly accepted behaviors. Bi-lateral agreements decrease information asymmetries between states, which leads to a reduction in tensions. It is no

secret that over the last decade states such as the United States and China have engaged in increasingly hostile actions against one another in cyberspace.[24] The frustration of the United States over China's aggressive cyber operations against US corporations resulted in high-level talks between US President Barack Obama and Chinese President Xi Jinping in September 2015. During the visit, a mutual understanding on the acceptable use of cyber operations against other states was discussed and a basic framework of behavior was informally agreed upon.[25] Although the informal agreement was subject to significant skepticism, independent analysis by the cybersecurity firm FireEye indicates that the agreement has had a significant positive effect in reducing the number of severe cyber-attacks perpetrated by China against US corporations.[26]

Bi-lateral agreements governing mutual behavior between states can be both beneficial and detrimental to the goals and objectives of the United States. Recent movement in NATO on its role in the cyber domain, specifically a cyber-defense pledge, offers measurable improvements in mutual understanding on how states within the alliance will interpret cyber-attacks against member nations and how they will respond.[27] Conversely, a recent nonaggression pact made between China and Russia potentially increases US fears.[28]

As the brief anecdotes above indicate, there are many layers to internet governance. Each of these layers affects the ability of nations, specifically the United States, to leverage cyberspace for military and intelligence objectives. The next section builds on the understanding that the internet is not devoid of laws which govern it, but that it is a complex environment within which actions carry significant consequences.

When States Decide to Attack

What should be clear is that the complex nature of internet governance highlights that the domain is not an ungoverned space in the traditional sense. Nor is there a lack of effort by actors at almost every level to develop governance structures. It is precisely because of the complex structures of governance that the United States and others are cautious about how they leverage cyberspace to achieve state objectives. States are rational actors in cyberspace.[29] Just because there are laws and governance structures does not necessarily indicate that they will follow said laws. Just as criminals fail to follow laws in perpetrating a crime when they feel they have a reasonable probability of escaping capture, so too will states engage in violations of the laws, policies, and governance structures of the internet when they do not fear reliable attribution or consequence.

The United States expends large amounts of effort to engage at various levels of internet governance. Even in the wake of the Snowden releases, the United States continues to push for an open and interoperable internet. In a speech at the Center for Strategic and International Studies in 2014, Ambassador Daniel A. Sepulveda, Deputy Assistant Secretary and US Coordinator for International Communications and Information Policy, Bureau of Economic and Business Affairs spoke to the US position regarding consistent and reasoned engagement in internet governance and urged listeners not to conflate

issues undertaken for intelligence collection and national security with the core standing of the United States.[30]

The governance of the internet in terms of technical standards, international, and domestic laws and norms weighs heavily on the US decision-calculus of whether to engage in any and all actions in cyberspace. Several well-known examples of attacks attributed[31] to the United States, such as Stuxnet and Flame, would seem to indicate that the attacker followed the letter of international law in a manner mostly consistent with interpretations of the law of armed conflict.[32] To assume that cyberspace is ungoverned would obviate the need for adherence to laws relevant in other domains. This, however, is not the case. Most states based on analyses of data through 2011 largely apply non-cyber specific interpretations of international law to actions conducted in cyberspace.[33]

The governance of the internet in terms of technical standards, international, and domestic laws and norms weighs heavily on the US decision-calculus of whether to engage in any and all actions in cyberspace.

Adherence to non-cyber specific laws in cyberspace is not universal, as recent incidents in Ukraine and New York indicate. Some state actors appear to be testing the limits of acceptable behavior in cyberspace in ways that would be considered clear violations of international law in physical domains of operation.[34] Yet the absence of direct consequence does not reflect the absence of governance. The attack against a minor spillway gate in New York violated numerous state and federal laws, many of which were written well prior to major state cyber-attacks against critical infrastructure.

The Department of Defense is explicit in its adherence to applicable laws with regards to actions conducted in cyberspace. In Joint Publication 3-12, "Cyber Operations," the opening letter to joint doctrine mandates that commanders conform to US laws, regulations, and doctrine.[35] The doctrine document goes further by distributing the functions of cyberspace operations into categorically different unit types, each with specific authorities and responsibilities. The specificity of role and function is not accidental. It is designed simultaneously for efficiency of function and adherence to applicable laws.

Responsibilities are broken down in to primary functions within the DoD into Offensive Cyber Operations (OCO), DoD Information Network Operations (DoDin-Ops), Defensive Cyber Operations (DCO), Defensive Cyber Operations - Response Action (DCO-RA), and Cyber Protection (CPT) Teams.[36] Each of the services has specific field manuals on the roles and responsibilities of operators in leveraging various tools of war. The Army's current unclassified doctrine document on Cyber Electromagnetic Operations (CEMA) is Field Manual 38. Sections 3–38 through 3–42 provide an overview of the roles and responsibilities of operational commanders in engaging in cyber operations. Specifically, commanders must be in compliance with all US laws as well as adhere to the principles of the laws of war.[37]

In documents leaked by Snowden, the rigor with which the United States attempts to adhere to standards of law is clear. Multiple news sites indicate that

only the President or his duly appointed representative may authorize an offensive cyber-attack by the United States against a foreign party.[38] Even then, the application of force through cyberspace is done with caution and an apparent respect for international law.

When the United States wants to engage in offensive cyber operations it must contend with nearly every aspect governing cyberspace, from laws to the technical constraints imposed by standards adopted in many of the organizations highlighted above. Yet, the constraints of law, policy, standards, and technical infrastructure are only part of the overall story. The internet is not an entirely public space. Although some countries have nationalized infrastructure and internet service providers, the United States in particular is heavily dependent on private entities for the provision of its services. For everything from land-based fiber lines that connect military installations within the continental United States, to the trans-oceanic fiber lines and satellites that connect remote bases and operational units, the United States purchases services from private entities.[39] These contracts always entail service level agreements that define acceptable standards of behavior on the networks. Behaviors such as offensive or defensive cyber operations with response actions can violate service agreements, strain network providers, and result in retaliation against networks in unintended ways. These consequences can be severe, resulting in service degradation for other customers beyond the Department of Defense.

When the United States wants to engage in offensive cyber operations it must contend with nearly every aspect governing cyberspace, from laws to the technical constraints imposed by standards adopted in many of the organizations highlighted above.

Decisions to leverage cyberspace by the United States are neither immediate nor without thought towards consequence. The domain is still quite new and its applications for militaries around the world are likely to grow as the number of connected devices increases from 17 billion today to a forecasted 50 billion within the next 10 years.[40] Whereas the kinetic effects of a bomb to a large extent are isolated spatially and temporally (although not psychologically) the effects of a cyber-attack can quickly extend beyond intended spatial, temporal, and psychological confines.[41]

The Painful Reality of Internet Governance and State Cyber Operations

The internet is not, as some might claim, an ungoverned domain. It is a highly governed domain within which states and other actors often violate, both knowingly and unknowingly, the norms, laws, and policies of other states and the international community in order to achieve certain outcomes. All actors operate within the confines of overlapping governance structures that define everything from the physics (code) of the domain to the appropriate behaviors of actors within that domain. Challenges arise when actors disagree on the

roles and responsibilities of states, corporations, and others. As the internet grows and expands from its current penetration of approximately 50% of the global population to the entire population over the next few years[42] and as the number of devices and systems connected globally increases, the challenges of governance are going to grow more acute. The simple yet painful reality is that the world is at the beginning of the digital revolution. The decision-making processes of states will change as the environment evolves.

The current US decision-making process on engaging in cyber operations indicates a deep understanding of the complexities of cyberspace and the overlapping governance structures it entails. Most states similarly recognize these structures. A few actors have been willing to test the limits of acceptable behavior in cyberspace, but these tests have not been without international condemnation.

The histories of governance over land, sea, air and space domains are long compared to that of cyberspace. The interactions of states in these domains still results in pockets lacking effective governance. Cyberspace will continue to resemble an ungoverned space, but the reality is that it is the most governed of ungoverned spaces.

Notes

[1] Cyber exploitation is the penetration of networks for intelligence purposes and constitutes operations conducted under Title 50 in US Code.
[2] The views expressed are those of the author and do not reflect the official policy or position of West Point, the Department of the Army, the Department of Defense, or the US Government.
[3] Peter Steiner, "*On the Internet nobody knows you're a dog,*" Cartoon, *New Yorker*, July 5, 1993.
[4] Chris Demchak, "Hacking the Next War," *The American Interest*, August 10, 2012, http://www.the-american-interest.com/2012/08/10/hacking-the-next-war/.
[5] Lawrence Lessig, *Code and Other Laws of Cyberspace*, (New York: Basic Books, 1999).
[6] Some of these organizations include the Internet Corporation for Assigned Names and Numbers (ICANN), the World Wide Web Consortium (W3C), Regional Internet Registries (RIRs), the International Organization for Standardization (ISO), the Number Resource Organization (NRO), Internet Network Operator's Groups (NOGs), the Internet Governance Forum (IGF) and the International Telecommunications Union (ITU).
[7] See "Information Sharing and Analysis Organizations (ISAOs)," Homeland Security, https://www.dhs.gov/isao (Provides U.S. position on Information Sharing and Analysis Organizations).
[8] General Assembly resolution A/70/174, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, (2015).
[9] Council of Europe, "Convention on Cybercrime," November 23, 2001, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
[10] See Michael N. Schmitt et al., *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence,* (New York: Cambridge University Press, 2013).
[11] Laura DeNardis, *The Global War for Internet Governance*, (New Haven: Yale University Press), 72–74.
[12] Paul Hoffman, "The Tao of IETF: a Novice's Guide to the Internet Engineering Task Force" *Ietf*, https://www.ietf.org/tao.html.
[13] "Become a Member," Internet Society, http://www.internetsociety.org/get-involved/become-member.
[14] The multistakeholder model is expressed as a core feature of ITU conferences on Internet Governance. See "WSIS +10 Outcomes Document," International Telecommunications Union, http://www.itu.int/net/wsis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf.

[15] Kathleen M. Moriarty, "IETF Diversity Update | IETF Blog," *Ietf*, December 4, 2015, https://www.ietf.org/blog/2015/12/ietf-diversity-update/.
[16] See "Mission Statement," Ietf, https://www.ietf.org/about/mission.html; "Internet Architecture Board," IAB, https://www.iab.org.
[17] Note: There has been guidance on behalf of the US Department of Commerce for ICANN and IANNA functions since the 1990s and prior to the establishment of the public Internet there was direct involvement of the US. Government in ARPA and the National Science Foundation.
[18] The text of the treaty can be found here: http://www.itu.int/en/wcit-12/documents/final-acts-wcit-12.pdf.
[19] Rory Jones and Danny Yardon, "U.S.-Led Coalition Refuses to Sign Telecoms Treaty," *The Wall Street Journal*, December 13, 2012, http://www.wsj.com/articles/SB10001424127887324296604578177680798958730.
[20] Tim Maurer and Robert Morgus, "Tipping the Scale: an Analysis of Global Swing States in the Internet Governance Debate," Internet Governance Papers, Paper No. 7, (May 2014): 3, https://www.cigionline.org/sites/default/files/no7_2.pdf.
[21] Kat Lucero, "Tech Companies Flex Influence Abroad at UN Internet Conference," *Sunlight Foundation*, December 3, 2012, http://sunlightfoundation.com/blog/2012/12/03/tech-companies-flex-influence-abroad-wcit/.
[22] Adam Segal, *The Hacked World Order : How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, (New York: Public Affairs, 2016), 221–223.
[23] Yudhistira Nugraha, Kautsarina, and Ashwin Songsoko Sastrosubroto, "Towards Data Sovereignty in Cyberspace," (Paper presented at: 3rd International Conference on Information and Communication Technology (ICoICT) 2015), 465–71; Tatevik Sargsyan, "Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security." *International Journal of Communication* (2016): 2221–37.
[24] Fred H. Cate, "China and Information Security Threats," In *China and Cybersecurity Espionage, Strategy, and Politics in the Digital Domain*, eds., Jon R. Lindsay, Derek S Reveron, and Tai Ming Cheung, (New York: Oxford University Press, 2015), 297–332.
[25] "FACT SHEET: President Xi Jinping's State Visit to the US | Whitehouse.Gov," Whitehouse, September 25, 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.
[26] "Redline Drawn: China Recalculates Its Use of Cyber Espionage," FireEye, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf
[27] "Cyber Defence Pledge," North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/official_texts_133177.htm.
[28] Olga Razumovskaya, "Russia and China Pledge Not to Hack Each Other," *The Wall Street Journal*, May 8, 2015, http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/.
[29] Aaron Franklin Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making*, (Athens: University of Georgia Press, 2016).
[30] Daniel A. Sepulveda, "Internet Governance 2020 - Geopolitics and the Future of the Internet," (presented at the Center for Strategic and International Studies, Washington, DC, January 23, 2014).
[31] The attack has been attributed in various press reports and books but not claimed by the US officially. The most notable reported attribution comes from. David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Pow*er, (New York: Crown Publishers, 2012).
[32] For a robust discussion on Stuxnet and the law of armed conflict See: Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, (New York: Cambridge University Press, 2012).
[33] Brantly, *The Decision to Attack.*
[34] "Cyber-Attack Against Ukrainian Critical Infrastructure | ICS-CERT: IR-ALERT-H-16-056-01." *ICS-CERT*, 2016, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01; Shimon Prokupecz, Tal Kopan, and Sonio Moghe. "Official: Iranians Hacked Into New York Dam," *CNN.com*, December 22, 2015, http://www.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html.

[35] "Joint Publication 3-12 (R), Cyberspace Operations," Department of Defense, (2013): i, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
[36] Ibid.
[37] "FM 3–38, Cyber Electromagnetic Activities," Department of the Army, February 2014, https://www.fas.org/irp/doddir/army/fm3-38.pdf.
[38] James A Lewis, "Truly Damaging Cyberattacks Are Rare," *The Washington Post*, October 10, 2013, https://www.washingtonpost.com/postlive/truly-damaging-cyberattacks-are-rare/2013/10/09/ae628656-2d00-11e3-b139-029811dbb57f_story.html.
[39] Durairajan, Ramakrishnan, Paul Barford, Joel Sommers, and Walter Willinger. "InterTubes: a Study of the US Long-Haul Fiber-Optic Infrastructure." In. SIGCOMM'15, London, 2015, 1–14.
[40] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," CISCO, (2011), https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
[41] See Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, (New York: Crown Publishers, 2014) (Provides a robust discussion on the spillover effects of Stuxnet).
[42] "Internet users in the World by Regions June 2016," Internet World Stats, http://www.internetworldstats.com/stats.htm