Sovereignty and Cyberspace

Bryan Nakayama
DRAFT

ABSTRACT

Most studies of the relationship between Cyberspace and sovereignty have focused on the question of infrastructural control and technological shaping. Inspired by John Herz's 1958 study of the changing nature of sovereignty in the face of the missile and jet age this paper begins from a different starting point: whether cyberspace alters the state's ability to provide a protective and defensible frontier. Militaries across the world have increasingly declared and operated within cyberspace as a distinct arena or domain of warfare. I argue in this paper that the rapid integration of the information and communication technologies that compose cyberspace into all aspects of everyday life suggests that there is a deeper challenge to the basic function of sovereignty than mere control.

TO BE DONE:

- Integrate explicit comparisons with approaches of EU, China, and Russia
- Expanded discussion of role of cyber-security industry

1 Introduction

During the late 1990s John Perry Barlow, an internet activist, published the "Declaration of the Independence of Cyberspace." In the first graf Barlow, addressing governments, declared that "you have no sovereignty where we gather." Barlow's warning flows from his understanding of where cyberspace is—continuing to address states he says "cyberspace does not lie within your borders. Do not think that you can build it, as though it were a construction project…it is an act of nature…" For Barlow, cyberspace is a space of social interaction that exceeds the territorial and material basis of the state and thereby vesting it with a form of sovereignty which demands non-interference by states.[1] However, the condition of possibility for these social interactions was irreducibly material and constructed by states; in 1996, when Barlow penned the declaration, the United States National Science Foundation completed its privatization of internet infrastructure.[2] While Barlow's declaration may seem naive several decades later, it is emblematic of a deeper problem with understanding the relationship cyberspace and sovereignty—a reification of a "cyberspace," a spatial metaphor to describe the existence of globe-spanning information infrastructure, that distinguishes it from its material basis. This means that discussions of the relationship between sovereignty and cyberspace tend to take the sovereignty of cyberspace as a given, states come to "control" cyberspace by seeking to enclose, filter, or censor it. Hence, a dominant perspective is that states are imposing Westphalian principles of sovereignty on *their* cyberspace through the interposition of rule into the operation of a distinct social world.[3] In this

[1] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, 1996, accessed October 15, 2016, `https://projects.eff.org/%7B~%7Dbarlow/Declaration-Final.html`; Cf. Timothy Wu, "Cyberspace Sovereignty?—The Internet and the International System," *Harvard Journal of Law & Technology* 10, no. 3 (1997): 647–666

[2] Jane Abbate, *Inventing the Internet*, Inside Technology (Cambridge, MA: MIT Press, 2000), 212

[3] Chris C. Demchak and Adam B. Lowther, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (2011): 32–62; Ronald Deibert, "The geopolitics of internet control," in *Routledge Handbook of Internet Politics*, ed. Andrew Chadwick and Philip Howard (London, UK: Routledge, 2008), 323–336; Ronald J. Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (New york, New York: Penguin, 2013); Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton, NJ: Princeton University Press, 2018). The Tallinn Manual 2.0 embodies this dynamic as well, for example that states may interpose control on cyber-infrastructure and activities. **CITE

paper, instead of continuing this tendency to oppose cyberspace and the territorial state when grappling with the nature of sovereignty I begin by treating cyberspace as always already an element of a state's sovereignty and explore how cyberspace, as constituted by states, alters the functional role of sovereignty. I argue that state management of cyberspace infrastructure is fundamentally changing the core protective role of sovereignty by generating what I term the "cyber in/security paradox"—the use of cyberspace as infrastructure by states for security purposes is premised on the maintenance of insecurity.

For example, over the course of late 2016 and 2017 a series of malware attacks—WannaCry and NotPetya—propagated across the world holding at ransom the data of individuals and organizations. Both of these attacks utilized a computer exploit called "EternalBlue" developed by the National Security Agency (NSA), which enabled malicious actors to gain control of the popular Windows operating system. The proliferation of this Windows exploit was the consequence of a leak of NSA hacking tools by a group, allegedly affiliated with the Russian government, called Shadow Brokers.[4] While the NSA eventually contacted Microsoft which issued a security update to stop the exploit, the damage was still done as hundreds of thousands of computers were affected. Reflecting on the impact of the Shadow Broker's leak of EternalBlue and the tension between disclosing computer vulnerabilities and retaining them faced by the NSA, a former White House official remarked that "the fact that a vulnerability is widely used and therefore the harm could be broad should be a significant factor. At the end of the day, it's a balancing act."[5] This "balancing act" has significant and little-discussed implications, the United States government had already hardened many of its

[4]Mark Galeotti, *Putin is Waging Information Warfare. Here's How to Fight Back*, 2016, accessed December 14, 2016, http://www.nytimes.com/2016/12/14/opinion/putin-is-waging-information-warfare-heres-how-to-fight-back.html; Ellen Nakashima and Craig Timberg, *NSA officials worried about the day its potent hacking tool would get loose. Then it did.*, The Washington Post, [Online; accessed 11/03/2018], May 2017, https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html?utm_term=.37e8379279ad

[5]ibid.

systems against the EternalBlue vulnerability while simultaneously using it against adversaries. However, in order to ensure the utility of EternalBlue, the underlying vulnerability that it exploited could not be publicly disclosed. This lack of disclosure combined with the fact that computer vulnerabilities are generally exploitable by anyone with skill and knowledge of them meant the NSA contributed to maintaining a state of vulnerability for computer systems used by a variety actors from adversaries, international organizations, educational institutions, corporations, and civilians. Therefore, the pursuit of security through the activities of the NSA was premised on the maintenance of insecurity.

The core of this paradox is that the sovereign territorial state generally arranges for a layer of protection against attacks through a variety of dimensions or domains. Most states will at the very least maintain a security architecture defending against attacks on land and through the air with a combination of military and police forces. Moreover, sovereign territorial states enjoy a high degree of jurisdictional exclusivity and equality thereby enabling the generation of internal juridical orders that stabilize social and economic interaction. In other words, sovereign states provide protection to their inhabitants both through internal order and by generating what Jon Herz calls a "hard shell of defensibility" over a territory.[6] Sovereignty is typically understood as a capacity—a government is able to exert sovereignty over a territory—-or as a quality that appertains to a political formation—a state's right to non-interference—but in this paper, I seek to advance an understanding of sovereignty as a functional relationship.[7] This similar but distinct from the Weberian aphorism that the "state is a human community that (successfully) claims the *monopoly of the legitimate use of physical force* within a given territory" which is about the legitimation of violence within a territory but not how that violence functions.[8] Cyberspace alters

[6]John H. Herz, "Rise and Demise of the Territorial State," *World Politics* 9, no. 4 (1957): 473–493

[7]Krasner provides a useful summary of the main ways in which sovereignty is characterized. Larry Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, NJ: Princeton University Press, 1999)

[8]A tendency to focus on this pithy formulation has the consequence that many tend to ignore that Weber is arguing about a monopoloy on legitimation. He goes on to argue "the right to use physical force is ascribed to other institutions or to individuals only to the extend to which the state permits it. The state is considered the sole source of the 'right' to use violence." Max Weber, *Politics as a Vocation* (New York, NY: Oxford University Press, 1946), 4

the functional relationship embedded in the sovereignty of territorial states because in providing attempting to provision cybersecurity states become involved in the management of and tampering with infrastructure that is becoming increasingly embedded in the most intimate aspects of human life. As opposed to the "hard shell" of protection that cleanly divides the inside and the outside of a sovereign territorial state, the inter-connectivity of cyberspace as a material infrastructure that enables action at distance spreads the locus of cyber-protection across infrastructure on the interior of a state. Therefore, protection is interposed within and through infrastructure and the methods by which states seek to provide protection require that the security of that infrastructure be continuously mediated in accordance with the security needs of a state.

In this paper, I unpack this paradox and explore its implications across these two interlinked areas—sovereignty and the function of the state in provisioning security. I argue that the security uses of cyberspace by states transforms sovereignty and the provisioning of security by states for three reasons. First, the territorial nature of sovereignty places the state at the center of mediating external threats through the maintenance of defensible frontiers. Cyberspace, for states that use it as a medium of belligerent action, enables the production of effects at a distance through nominally civilian infrastructure. The penetration of cyberspace infrastructure into everyday life means that the defensible frontier becomes generalized across the space of the state, the state defends or controls some networks while leaving others vulnerable. Second, this fundamentally alters the protective relationship between a state and its citizens. Nominally, one of the core functions of the modern state is to distribute security within the territory over which it holds sovereignty in order to provide protection.[9] The security uses of cyberspace by states substantially alters this relationship as states, in peacetime, extend security to their institutions while ensuring vulnerability for their populations and all other users of targeted systems. Finally, the maintenance of this insecurity is unprecedented in scale and scope—as the most intimate details of everyday life become interlaced with Internet connectivity the range of potential attacks

[9]Of course, this is not to take the naive view that states protect all citizens or inhabitants equally.

against individuals, corporations, and others actors multiply. This enables unprecedented specificity in targeting during peacetime and war, a consequence of the conscious maintenance of infrastructural insecurity.

The remainder of the paper will unfold in the following fashion: first, I will provide a methodological note and definition of what I term "cyberspace." I argue that to fully appreciate the security implications of cyberspace, scholars of international relations need to pay substantially more attention to how states manipulate or otherwise interact with cyberspace infrastructure beyond the creation and deployment of "cyber-weapons" or attempts to control infrastructure. Next, I review the literature on cyberspace and sovereignty wherein I outline the major existing approaches and claims. Following this, I outline how I understand sovereignty as a security relationship—that territorial sovereignty can be understood as a legitimate claim to distribute security within a state. Then, I unpack the two major ways in which cyberspace transforms the functional nature of sovereignty that I outlined in the previous paragraph. I conclude the paper with a discussion of substantive implications.

2 Cyberspace

There is a common view that the security challenges of cyberspace are a natural property that flows from its unique status as information infrastructure.[10] In this paper, I take the opposite view, that the security challenges of cyberspace are the consequence of historically contingent choices in the formation of the underlying material infrastructure. That is, cyberspace is not an alien force

[10]Many of these features were the consequences of choices made during its development. See Abbate, *Inventing the Internet*; Barry M Leiner et al., *Brief History of the Internet*, Internet Society, [Online; accessed June 20, 2015], 1997, `http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet`; S. Lukasik, "Why the Arpanet Was Built," *IEEE Annals of the History of Computing* 33, no. 3 (March 2011): 4–21. This naturalization of cyberspace most often manifests in the proclamations and statements by governmental officials and commentators. For example, see: TBD: CYBER-PEARL HARBOR, CLARKE AND KNAKE, ETC For scholarly literature that attributes metaphysical properties to cyberspace/the Internet see: Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, Massachusetts: MIT Press, 2012), 320; Lucas Kello, *The Virtual Weapon and International Order* (New Haven, Ct: Yale University Press, 2017); TBD ++

that challenges states but rather is actively modified, used, and produced through state action. Cyberspace is not a space on which control is imposed but rather an infrastructure that can enable. What this view suggests is that studies of the implications of cyberspace need to pay substantially more attention to how states manipulate the underlying technologies of cyberspace for their own purposes. I take this view not just to satisfy a methodological quibble over the relationship of technology and human politics but because it has substantial consequences for the study of cyberspace and international politics. Whereas a nuclear weapon is the consequence of a bounded set of technologies marshaled for a clear outcome—a device that creates a massive explosion and/or radiological effects—"cyber-weapons" and other security uses of cyberspace are highly variable in their content and purpose.[11] Inattention to how the security conditions of cyberspace are shaped and produced by states means flattening or reifying cyberspace in a way that effaces the role that states play in creating the (in)security conditions of cyberspace. Given that cyberspace is increasingly being treated as a new "domain of warfare" equivalent to air, land, sea, and space, being attentive to the consequences of the choice to treat cyberspace as a medium of conflict is crucial because it aids in demystifying the current and future consequences of cyberspace.[12] The movement to a "military domain" framework is also representative of another form of contingency—that cyberspace, due to its technical nature, can only be understood through human interpretation.[13] Air, land, sea, and orbital space have distinctive geophysical

[11] Brandon Valeriano and Ryan C Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York, NY: Oxford University Press, 2015), Chapter 1; Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157, no. 1 (2012): 6–13

[12] For seminal statements of the domain status of cyberspace see: Michael V. Hayden, "The Future of Things "Cyber"," *Strategic Studies Quarterly*, 2011, 3–7; William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (2010): 97–108

[13] On the social interpretations of cyberspace see: Vincent Mosco, *The Digital Sublime: Myth, Power, and Cyberspace* (Cambridge, MA: MIT Press, 2005); There is a long-running literature on securitization and cyberspace that has largely been little discussed in American security studies. However, this literature does not make explicit the linkage between interpretation and material interventions into cyberspace. Myriam Dunn Cavelty, *Cyber-security and threat politics: US efforts to secure the information age* (London, UK: Routledge, 2007); Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, no. 53 (2009): 1155–1175; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-threats," *Journal of Information Technology and Politics* 10, no. 1 (2013): 86–103

manifestations, cyberspace is a metaphorical concept premised on human-built information infrastructure. That cyberspace must be secured through the logic of war was a conscious choice with deep implications for the nature of security and sovereignty.[14] At a conceptual level, I argue that within international relationship scholarship cyberspace should be endogenized. States do not confront cyberspace, states create, enable, and use cyberspace.

In this paper, I operate with an understanding of cyberspace as a contingent, mutable, and fundamentally material space/set of technologies. To bound what is meant by "cyberspace" I adopt the U.S. Department of Defense's layer model for decomposing cyberspace into three components: (1) physical network which refers to the material components; (2) logical network which are the code or data components that enable information networking; and (3) cyber-persona which refers to representations of entities operating in cyberspace.[15] I use this definition for two reasons: first, it provides a useful abstraction, based on the actual design of the underlying technologies of cyberspace, that makes the heterogeneity of cyberspace interpretable.[16] Moreover, it enables analytical claims about what aspects of cyberspace states are choosing to intervene on or tamper with. Second, the account in the following pages is largely focused on actions taken by the United States military and computer security industry. I acknowledge the limits of centering the United States, but I choose explore the paradox through the United States because of its central role in developing the technologies of cyberspace.[17] Moreover, the corporations that create the two most dominant computer operating systems—Microsoft and Apple—are based within the United States and a substantial portion of the work and funding for the Linux operating system comes from U.S. based companies and developers.[18] Core technical governance institutions such

[14]Demchak and Lowther, "Rise of a Cybered Westphalian Age"; Martin Libicki, "Cyberspace is a not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 1 (2012): 321–336; Martin Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly* 7, no. 4 (Spring 2014): 23–45; Martin Libicki, *Cyberspace in Peace and War* (Annapolis, Maryland: Naval Institute Press, 2016)

[15]Joint Chiefs of Staff, *JP 3-12 Cyberspace Operations* (Chairman of the Joint Chiefs of Staff, 2018), I-3, I-4

[16]For a discussion of the technical and social origins of layering see: Abbate, *Inventing the Internet*, Chapter 4

[17]See: ibid.; Yasha Levine, *Surveillance Valley: The Secret Military History of the Internet* (New York, NY: Public Affairs, 2018)

[18]Cite on Linux

as the International Corporation for Assigned Names and Numbers and the Internet Engineering Task Force were formed in the United States. The concentration of core institutions and users of cyberspace in the United States means that it has a unique ability to exploit the infrastructure—for example, the PRISM surveillance program revealed by Edward Snowden enables the United States to directly access data held by top Internet corporations such as Microsoft, Yahoo, Facebook, and Google.[19] Altogether, this means that the United States is both a first mover and has substantial formal and informal influence over the design, governance, and promulgation of Internet infrastructure.[20]

3 Sovereignty

As seen in Barlow's declaration, during the 1990s a dominant theme of public promotion and engagement with cyberspace and the Internet was a form of cyber-utopianism—that cyberspace would bring about the obsolescence or the very least decrease the relevance of the nation-state as a mode of social and political organization. The core reasons advanced for this decline of state sovereignty were three-fold: first, new forms of community would emerge on the Internet which would erode the nation-state as a primary source of identification for individuals. Second, cryptography would enable the formation of new virtual communities and render attempts to control information flows moot. And finally, that corporations and individuals would be substantially empowered by the near limitless mutability of information substantially reducing the

[19] Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8, no. 2 (2014): 121–144, doi:10.1111/ips.12048, https://doi.org/10.1111/ips.12048

[20] A telling example is the case of TOR—an application that promises to help evade government monitoring—which is largely funded by the United States government and is reported to have at least in one case privately disclosed a vulnerability that would unmask users to the NSA. Levine, *Surveillance Valley: The Secret Military History of the Internet*, 238. McCarthy has argued that the United States has used the Internet as part of its foreign policy by institutionalizing western values in the technical design. Daniel R McCarthy, *Power, information technology, and international relations theory: The power and politics of US Foreign policy and internet* (London, UK: Palgrave Macmillan, 2015)

relative power of states vis-a-vis the economy and civil society.[21] From the perspective of 2018, these views may seem naive but they formed the foundation of the "liberation technology" thesis that dominated the early part of the 21st century—that cyberspace enabled activities could escape state control thereby enabling resistance to authoritarian regimes. This had the consequence that the United States and other western countries saw the diffusion of applications and technologies, such as TOR or mesh networking, as a tool of democracy promotion.[22] Overall, the utopian premise was part of a broader belief that cyberspace as a feature of globalization would lead to a de-concentration of state power, transnational networks would obviate the potency of and need for state sovereignty.

However, the empirical record seems to have indicated that authoritarian regimes have become highly adept at using cyberspace to impose censorship, target political enemies, and intervene in the operation of western liberal democracies.[23] The increasing state control over

[21] Some prominent examples: Barlow, *A Declaration of the Independence of Cyberspace*; E. Dyson, *Release 2.0: A Design for Living in the Digital Age* (New York, NY: Viking, 1997); Timothy May, "The Crypto Anarchist Manifesto," in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, ed. Peter Ludlow (Cambridge, MA: MIT Press, 2001), 61–65; Timothy May, "Crypto Anarchy and Virtual Communties," in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, ed. Peter Ludlow (Cambridge, MA: MIT Press, 2001), 65–81

[22] Hillary Clinton, *The prepared text of U.S. of Secretary of State Hillary Rodham Clinton's speech, delivered at the Newseum in Washington, D.C.*, [Online; accessed 10-May-2017], January 21, 2010, http://foreignpolicy.com/2010/01/21/internet-freedom/; Hillary Clinton, *SECRETARY OF STATE HILLARY RODHAM CLINTON REMARKS ON INTERNET FREEDOM*, [Online; accessed 10-May-2017], February 15, 2011, https://www.eff.org/files/filenode/clinton_internet_rights_wrongs_20110215.pdf; Pamina Firchow, "A Cuban Spring? The Use of the Internet as a Tool of Democracy Promotion by United States Agency for International Development in Cuba.," *Information Technology for Development* 19, no. 4 (2013): 347–356, ISSN: 02681102; Larry Diamond, "Liberation Technology," *Journal of Democracy* 21, no. 3 (2010): 69–83, doi:10.1353/jod.0.0190, https://doi.org/10.1353/jod.0.0190; Shanthi Kalathil and Taylor C. Boas, *Open Networks Closed Regimes* (Washington, D.C.: Carnegie Endowment, 2003); Levine, *Surveillance Valley: The Secret Military History of the Internet*, 101-138; McCarthy, *Power, information technology, and international relations theory: The power and politics of US Foreign policy and internet*, 101-121; Mosco, *The Digital Sublime: Myth, Power, and Cyberspace*, 55-84; Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York, New York: Perseus, 2011)

[23] Yochai Benkler, Robert Faris, and Hal Roberts, *Network Propaganda* (New York, NY: Oxford University Press, 2018); Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*; United Nations Human Rights Council, *Report of the independent international fact-finding mission on Myanmar*, United Nations Human Rights Council, (Online; accessed 11/04/2018), 2018, 14, %5Curl%7Bhttps://www.ohchr.org/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.docx%7D; Morozov, *The Net Delusion: The Dark Side of Internet Freedom*; Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*; P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York, NY: Houghton Mifflin Harcourt, 2018)

Internet infrastructure is seen as part of a "cyber-Westphalian" process, whereby the inter-connectivity of cyberspace infrastructure between states is modulated by state interventions into the underlying infrastructure. The process is meant to invoke the concept of Westphalian sovereignty—that states mediate cyberspace interconnectivity in order to extend control over domestic infrastructure to enable jurisdictional exclusivity and repel external attacks. This process has also been described as "balkanization" as individual or like-minded groups of states carve up the physical and logical network in response to security threats.[24] While states such as Iran and China are clearly erecting barriers within cyberspace, most western states have not intervened into the Internet infrastructure in the same way.[25] Some, such as Demchak and Dombrowksi see the 2009 creation of U.S. Cyber Command and the concomitant extension of the logic of warfare to cyberspace as representative of a key trend towards a western cyber-Westphalia.[26] While approaches to the overt control of cyberspace infrastructure vary cross-nationally, the construction of cyberspace infrastructure is becoming an increasing aspect of strategic competition. Disputes in 2018-2019 between the United States and its allies with China over the manufacture of 5G network infrastructure go beyond the grammar of technological competition of the Cold War Space Race—it is not just about achievement but also the ability to secure and control infrastructure shared with allies and adversaries.[27]

Whether the United States and other western states will fully embrace overt forms of

[24]For example, a former CEO of Google, Eric Schmidt, has predicted that the Internet will bifurcate into Chinese and U.S. led orders. Lora Kolodny, *Eric Schmidt, ex-Google CEO, predicts internet bifurcation with China*, CNBC, (Accessed on 11/04/2018), September 2018, `https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html`; See also: David Betz and Tim Stevens, *Cyberspace and the State: Towards a Strategy for Cyber-Power* (Abingdon, United Kingdom: Routledge, 2011), Chapter 2; Nazli Choucri and D D Clark, "Who controls cyberspace?," 69, no. 5 (2013): 21–31; Demchak and Lowther, "Rise of a Cybered Westphalian Age," Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (2010): 15–32; Rex Hughes, "A treaty for cyberspace," *International Affairs* 86, no. 2 (2010): 523–541. Though, others such Mueller challenge this process by highlighting the ways in which meaningful infrastructural governance is conducted by technicians. Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010)

[25]Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*, Chapter 1; + IRAN Cite

[26]Demchak and Lowther, "Rise of a Cybered Westphalian Age"

[27]CITE TBD

control like China or Iran has yet to be seen. For the present, Bauman et al, have suggested that rather than cyber-Westphalia the scale and scope of surveillance revealed by Snowden demonstrate that the United States and it's intelligence partners has turned sovereignty into a "mobius-strip." For them, the weak distinctions between foreign/domestic collection and analysis as well as the widespread harnessing of Internet infrastructure for the purpose of surveillance have eroded any distinctions between domestic and international security policy. Overall, they claim, mass surveillance in cyberspace is fundamentally altering the security relationship between the United States and its intelligence partners with their domestic populations, calling into question *who* is being secured.[28] While Bauman et al suggest an interesting way of interpreting the nature of sovereignty and security in the age of mass surveillance, their argument does not consider the hoarding of exploits/vulnerabilities and is largely focused on other matters.

3.1 What is sovereignty for?

In this section, I seek to explore how cyberspace has transformed the functional relationship embedded within the status of sovereignty. What I mean by "functional relationship" is that sovereignty, as a political relationship between territory and authority, has a function beyond legal status, preventing non-interference by other sovereign entities, control over domestic affairs, or control of borders.[29] Instead, I aver that cyberspace challenges to sovereignty flow from the transformation in how states distribute security within a territory.

In utilizing this conception of sovereignty, I am retrieving John Herz's 1957 argument over the relationship between technologies of warfare and the territorial state. For Herz, the rise

[28] Bauman et al., "After Snowden: Rethinking the Impact of Surveillance"

[29] To use Krasner's four-fold typology of sovereignty. Krasner, *Sovereignty: Organized Hypocrisy*. There is another interesting line of exploration that looks at the topology of control that exists through network structures. Galloway and Thacker argue that distributed networks, such as the Internet, are able to express their own form of sovereignty through two means: first, the creation of protocols that mediate the edges of networks. And, second, the existence of "exceptional topologies" that generate power through their dissimilar operation from the overall network. While interesting and at times insightful, Galloway and Thacker's argument is not useful at the moment. Alexander R. Galloway and Eugene Thacker, *The Exploit: A Theory of Networks* (Minneapolis, MN: University of Minnesota Press, 2007)

of air and atomic warfare during World War II had created a condition wherein "utmost strength now coincides in the same unit with utmost vulnerability, absolute power with utter impotence."[30] This is because the modern territorial state, he argued, was premised on a functional relationship between territorial space and the state—the creation of a "hard shell" to thwart external attacks. New technologies, such as aircraft, meant that the interior of states became de-facto integrated into the process of inter-state warfare by granting a means to ignore frontiers and by legitimizing the destruction of the interior of territorially sovereign states. This quality of territorially sovereign states for Herz was not a question of borders as such but rather the state's ability to spatially defend itself by providing a thick interface between its political community and attacks by other states. This is because borders serve two functions—first, they provide an administrative distinction between political jurisdictions and as such do not only exist on the edges of a territorially sovereign state. Second, borders serve to permit or restrict flows in and out of a political unit, a condition that does not necessarily coincide with territorial sovereignty. Therefore, the key insight is the survival of territorial states is founded on an ability to spatially interpose itself between its society and invasion or atttack. While Herz's prediction that the system of territorially-bound sovereignty that under-girds the international system would degrade and be eventually replaced by some form of world government, his questioning over the relationship between technology, territoriality, and the security relationship between a sovereign state and its territory is useful for understanding the consequences of cyberspace.[31]

I seek to extend and modify Herz's functional conceptualization of sovereignty—that sovereignty is the ability for a state/political formation to make defensible a unit of territory—by understanding the functional relationship of sovereignty as the exclusive distribution of security within a territorial unit by a state or other political formation. I extend Herz's argument on the basis of the following two claims about states, territory, and security: first: that the main reason

[30] Herz, "Rise and Demise of the Territorial State," 474
[31] ibid.

that sovereign states exist is to provide security for their inhabitants. Scholars of international relations have long gestured toward the Hobbesian State of Nature as a metaphor for the nature of (international) anarchy, the resolution of the State of Nature at the meso-level is accomplished for Hobbes by humans creating sovereign political formations that provide physical security and regularize social interactions through the imposition of morality. Citizens give up some of their individual wills to create a corporate political formation that stabilizes conditions by wielding coercive force.[32] However, this is not to make a claim that sovereignty in this sense flows from popular consent, even a kleptocracy needs to protect its populations and provide a framework for social and economic interaction.

Second and consequently, outside of providing stability within a territorial unit, states under the permissive condition of anarchy will seek to reduce the condition of insecurity through internal or external means.[33] I emphasize the reduction of insecurity because not all other states or neighbors are perceived as generating the condition of insecurity, for example, the United States spends substantially fewer resources on its northern border than its southern border. Or, that the United States built the Distant Early Warning series of radar installations in Canada and its northern frontier because it expected Soviet nuclear bombers to overfly the North Pole. States choose to secure different parts of their territory against external threats due to political, technological, or geographical reasons. However, this uneven reduction of insecurity/distribution of security is not exclusive to the edges or frontiers of states, security is distributed unevenly within states by variable investment, economic distribution, allocation of rights, or exercise of police powers. Therefore, in/security is a spatially uneven condition because states make choices about how to distribute security across their sovereign territory.

However, one might wonder why this functional understanding of sovereignty as the

[32]Thomas Hobbes, *Leviathan*, ed. C.B. MacPherson (New York, NY: Penguin, 1982)

[33]This is not to make a claim that either of these conditions hold true for territorial units such as "failed-states," see: Arjun Chowdhury and Raymond Duvall, "Sovereignty and Sovereign Power," *International Theory* 6, no. 2 (2014): 191–223

distribution of security by states across a territorial unit is preferable or useful for unpacking the relationship between cyberspace and security. The first reason is methodological—I aver that cyberspace should not be treated as an exogenous feature of international politics. When one examines the actual history and contemporary development of the technologies/infrastructure of cyberspace it becomes clear that it does not exist outside of the realm of human politics.[34] By utilizing a functional definition of sovereignty it forces analysts to consider not just how challenging or revolutionary qualities of cyberspace confront states but how they are produced by states. For example, the fact that much of the material and logical infrastructure of cyberspace is run by private corporations was a choice made during the late 1980s and early 1990s to privatize the U.S. Internet's immediate precursor which was owned and managed by the National Science Foundation.[35] That much of this infrastructure is held in private hands was a political choice. Likewise, limited regulation of cryptography within the United States began with the high-profile failure of the "Clipper-Chip" private-key escrow proposal during the mid-1990s which would have enabled the federal government exclusive ability to decrypt communications through a mandated backdoor.[36] Analyzing the consequences of cyberspace for sovereignty through this lens enables a consideration of the ways in which cybersecurity is differentially constituted for governments, militaries, corporations, and publics.

Second, this conceptualization of sovereignty unites security, territoriality, and the state in a fashion that draws attention to important dynamics. One could claim that either control over domestic affairs and/or Westphalian sovereignty is a useful tool for explaining the security relationship a sovereign state has with its territory. However, these forms of sovereignty draw

[34] cf. Laura Denardis, *Internet Architecture as a Proxy for State Power*, [Online; accessed 10-May-2017], August 2015, `http://www.ipjustice.org/wp-content/uploads/2015/08/IPJustice_Journal_DeNardis_Internet_Architecture.pdf`; Laura Denardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge, Massachussetts: MIT Press, 2009)

[35] Abbate, *Inventing the Internet*, Chapter 6

[36] Sean Gallagher, "What the government should've learned about backdoors from the Clipper Chip," *Ars Technica*, December 14, 2015, `https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/`

analytical focus to either the control of domestic threats (domestic sovereignty) or the negative right to non-interference (Westphalian), they treat as analytically separate interior/external threats. This Moreover, they do not conceptually account for the fact that security mechanisms are intentionally unevenly distributed across territorial space. A more recent trend in the study of sovereignty is the retrieval of the work of Carl Schmitt, which focuses on how sovereign power is produced through a suspension or withdrawal of the normal legal order within a state in a time of crisis. For Schmitt, sovereignty thereby flows from the sovereign who is able to suspend but not transgress the law.[37] Because the cyber in/security paradox I outlined earlier hinges on the differential protection afforded by states through withholding knowledge of vulnerabilities and exploits one could make the case that this is a form of sovereign exception, however, this dynamic does not appertain to cybersecurity because, for example, there is no legal order within the United States that effectively governs the disclosure of computer and networking vulnerabilities. Furthermore, this situation is partly a product of routine legal obeisance, during the late 1990s when the United States stood up its first cyberspace defense unit—Joint Task Force–Computer Network Defense—their ability to defend U.S. networks was constrained by posse comitatus.[38] Likewise, during the late 1980s, there was an attempt to bring all U.S. information infrastructure under the umbrella of the National Security Agency for the purpose of network defense but this proposal was defeated due to civil liberties concerns.[39] Thus, the expression of a sovereign power that withholds security is regularized or otherwise unconstrained. Withholding vulnerabilities and the maintenance of insecurity that it generates is therefore fully compatible with a regularized legal order. This conception of sovereignty is useful because it captures the constitution of

[37] Carl Schmitt, *Political Theology: Four Essays on the Concept of Sovereignty* (Chicago, IL: University of Chicago Press, 2005)

[38] Jason Healey, *A Fierce Domain: Conflict in Cyberspace 1986-2012* (Baltimore, Maryland: The Atlantic Council, 2013), Chapter 2

[39] Fred Kaplan, *Dark Territory: The Secret History of Cyberwar* (New York, NY: Simon / Schuster, 2016), 1-4; Michael Warner, "Notes on the Evolution of Computer Security Policy in the US Government 1965-2003," *IEEE Annals of the History of Computing* 37, no. 2 (April 2015): 10-12; The White House, *National Security Decision Directive Number 145: National Policy on Telecommunications and Automated Information Systems Security*, Federation of American Scientists, [Online; accessed June 12, 2017], 9-17-1984, `https://fas.org/irp/offdocs/nsdd145.htm`

sovereignty in-motion as opposed to a steady-state—sovereignty as a functional relationship exposes new and crucial dynamics for understanding cyber in/security.

3.2 Cyber In/security

The core of the cyber in/security paradox, that provisioning cybersecurity necessitates maintaining widespread vulnerability, fundamentally changes the nature of territorial sovereignty as the distribution of security by inverting the terms. Rather, for the United States to "secure" cyberspace requires the maintenance and distribution of insecurity, because vulnerabilities and exploits serve a core role in the fashioning of cyber-weapons. This core dynamic is exacerbated and maintained in two ways: first, states and private cyber-security firms "stockpile" exploits and vulnerabilities because their utility depends on maintaining private knowledge. Whereas a gun, bomb, or missile has a physical manifestation that enables possessive control over their circulation, an exploit or vulnerability is a latent condition in material objects and logical/code constructs. This is due to the imprecision of the process of creation, heterogeneity of elements within a computer or information network, and a series of design choices that enabled the creation of heterogeneous federated information networks.[40] Thus, the problem of security is not addressed merely by careful use of a computer or the application of security utilities such as an anti-virus program as exploitable vectors are latent to systems and not an imposed condition.[41] The first two features of exploits and vulnerabilities mean that once revealed to the public or a manufacturer, they can be addressed. This has the consequence that the utility of vulnerabilities potentially decays over time, and that this decay can only be staunched by refusing disclosure.[42] Furthermore, vulnerabilities are fundamentally agnostic as to their users—control over a nuclear

[40] One could conceivably argue that a gun exploits the vulnerability of the human body to high velocity impacts but this vulnerability is not a choice.

[41] Gary McGraw, "Cyber War is Inevitable (Unless We Build Security In)," *Journal of Strategic Studies*, 2013, 1–11

[42] In a 2017 report RAND researchers estimated that the average life of a zero-day exploit is 6.9 years. Lillian Albon and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and the Their Exploits* (Santa Monica, CA: RAND Corporation, 2017)

weapon can be achieved by introducing a locking mechanism that prevents the operation of a warhead whereas a vulnerability can only be controlled through non-disclosure or an engineering fix that removes its utility. Corporations that create the physical and logical technologies of cyberspace are cognizant of these vulnerabilities and have "bug bounty" programs whereby they pay researchers who disclose vulnerabilities. However, given the value of these vulnerabilities there exist extensive markets for actors who seek to exploit them.[43]

The condition of in/security vis-a-vis vulnerabilities is exacerbated by fact that there is little legal accountability within the United States for corporations that fail to secure their systems even when vulnerabilities have been discovered and resolved. For example, the 2017 Equifax breach which exposed the data of approximately 146 million Americans, British, and Canadian citizens was the consequence of two factors: first, that Equifax failed to renew a security certificate for a network monitoring apparatus that would have detected the attack; and second that they failed to segment their databases which allowed hackers access to a large trove of data. This happened despite an advisory from the US–Computer Emergency Response Team to monitor for the vulnerability. Despite widespread public outcry, Equifax has faced little consequences and legislation to create a legal regime for imposing sanctions on companies with data breaches fizzled out.[44] Despite Equifax facing few consequences for this breach, those whose data was exposed in the breach will continue to be at risk for identity theft for the foreseeable future. This dynamic is revelatory of the incentive structure faced by corporations that heavily depend on cyberspace infrastructure—there are few non-reputational consequences for producers of these technologies and holders of data while users and data-subjects bear the burden of risk.[45] This is only exacerbated

[43]FireEye, *What is a Zero-Day Exploit?*, FireEye, [Online; accessed 11/02/2018], n.d. https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html; n.a., *Why the market for zero-day vulnerabilities on the dark web is vanishing*, Fifth Domain, [Online; accessed 11/02/2018], 2018, https://www.fifthdomain.com/industry/2018/09/25/why-the-market-for-zero-day-vulnerabilities-on-the-dark-web-is-vanishing/

[44]Catalin Cimpanu, *US government releases post-mortem report on Equifax hack*, ZDNet, (Accessed on 11/03/2018), 9/7/2018, https://www.zdnet.com/article/us-government-releases-post-mortem-report-on-equifax-hack/

[45]Council on Foreign Relations, *Reforming the U.S. Approach to Data Protection and Privacy*,

by the fact that resolving vulnerabilities is not an instantaneous process, it requires users to monitor and update their physical and logical systems. That the United States has largely failed to create a system to punish poorly designed or managed systems while simultaneously stock-piling exploits unevenly distributes security across the network structure of cyberspace, and thereby across the United States as a territorial entity. Altogether, this means that while cyber in/security is both an engineering problem and a question of legal accountability the way in which the United States pursues cybersecurity generates incentives for leaving unresolved computer vulnerabilities.

The second way in which the cyber in/security paradox is exacerbated is through the method by which the United States and other states pursue security within cyberspace. The primary mode of security seeking with cyberspace is applying the logic of warfare through the instantiation of cyberspace as a military domain. While there has been some controversy over this designation, little has been done to stem the tide as the development of formal military cyber units continues apace.[46] This is not to suggest that states do not face cybersecurity risks from other political actors, rather, that there was nothing natural or inevitable about cyberspace being treated as a military domain. Debates and doctrine in the United States during the 1990s over what would be understood today as cyberspace operations centered on either the destruction or manipulation of command and control systems by any means or manipulating enemy epistemology through mass media and information control systems.[47] Likewise, the probable origin of the term

https://www.cfr.org/report/reforming-us-approach-data-protection, [Online; accessed 11/05/2018], 1/30/2018

[46]For example, there was a brief public debate whene U.S. Cyber Command was first created, see: Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy"; Jane Holl Lute and Bruce McConnell, "OP-ED: A CIVIL PERSPECTIVE ON CYBERSECURITY," [Online; accessed March 20, 2017], *Wired Magazine*, 2-14-2011, `https://www.wired.com/2011/02/dhs-op-ed/`. There has also been a long-running debate between RAND analyst Martin Libicki and General Michael Hayden. See: Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York, NY: Penguin, 2016); Hayden, "The Future of Things "Cyber""; Libicki, "Cyberspace is a not a Warfighting Domain"; Martin Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly* 14, no. 1 (Spring 2014): 23–39; Libicki, *Cyberspace in Peace and War*. + CITE ON US CYBER UNITS REACHING OPERATIONAL CAPACITY

[47]Doctrine: Air Force Office of the Chief of Staff, *Cornerstones of Information Warfare*, http://www.c4i.org, [Online; accessed May 25, 2017], 1995, `http://www.c4i.org/cornerstones.html`; Atwood, Donald J, *TS 3600.1*, DOD FOIA Online Reading Room, 12-21-1992, `http://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/14-F-0492_doc_01_Directive_TS-3600-1.pdf`; Colin Powell, *Chairman of the Joint Chiefs of Staff Memorandum of Policy No. 30 (CMOP); Command and*

"cyberwar"—"Cyberwar is Coming!" by John Arquilla and David Ronfeldt—focused on the conduct of warfare utilizing cybernetic principles and not the creation of military effects through infrastructure.[48] None of these conceptions treated information infrastructure as a medium, but instead as a target for activities during wartime. That the United States and other states came to understand cyberspace as a domain of warfare is not a natural outcome but rather a choice that enabled states to apply the logic of warfare and all that that implies.

Rather, there was a deliberate choice to extend the logic of warfare to fighting through a shared global infrastructure. As I argued previously, the problem of cybersecurity is at its base an engineering problem—the first order effects of a cyber-attack are disruption of a logical system that produces consequential knock-on effects.[49] This is substantially different from the explosion of a bomb or the impact of a bullet, both of which directly produces consequential kinetic effects. The creation of U.S. Cyber Command and the reification of cyberspace as a domain in doctrine represents the triumph of a view that an engineering challenge is best met through the application of military logics and force.[50] Which is to say, it was contingent, the United States could have centered Information Assurance as the primary response to cyber-threats instead, which would have changed the framework by which problems and solutions were offered.[51]

Control Warfare, Defense Technical Information Center, [Online; accessed June 11, 2017], 1993-3-8, `http://www.dtic.mil/docs/citations/ADA389344`. Debates: R. L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," *Airpower Journal* IX, no. 4 (Winter 1995): 69–79; Chris Morris, Janet Morris, and Thomas Baines, "Weapons of Mass Protection: Nonlethality, InformationWarfare, and Airpower in the Age of Chaos," *Airpower Journal* IX, no. 1 (Spring 1994): 15–29; Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal* IX, no. 1 (Spring 1995): 56–65; George J. Stein, "Information Warfare," *Airpower Journal* IX, no. 1 (Spring 1995): 30–55; Alvin Toffler and Heidi Toffler, *War and Anti-War* (New York, NY: Grand Central Publishing, 1995); YuLin Whitehead, "Information as a Weapon: Reality versus Promises," *Airpower Journal* XI, no. 3 (Fall 1997): 40–54;

[48] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy* 12, no. 2 (Spring 1993): 141–165

[49] Thomas Rid, *Cyber War Will Not Take Place* (New York, NY: Oxford University Press, 2013), Chapter 1

[50] General Michael Hayden in memoir argues that "domain" is a perceptual schema that extends military logics. "Actually, when you convince a GI that something is a domain, a lot of things click. He doesn't clutter his mind with extraneous concepts like networks, bandwidth, and the like. It's a domain, an operational environment, and—just like all other domains—it has its own characteristics." Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, 128

[51] Demchak and Lowther, "Rise of a Cybered Westphalian Age," 44. Martin Libicki in his most recent book argues that cyber should not be given the primacy symbolized by U.S. Cyber Command, preferring to see it as a support function. *passim* Libicki, *Cyberspace in Peace and War*

This application of military logics and the extension of the status of "domain" has two main consequences for the distribution of security by states across their sovereign territory. First, it privileges the "stuff" of cyberwarfare—exploits, and vulnerabilities—as a resource for the pursuit of national security. Given that exploits and vulnerabilities impact commonly used civilian and commercial systems this means that the logic of war demands keeping systems insecure so as to ensure a "strategic reserve." Certainly, there are threats from adversaries through cyberspace, however, it is not clear "who" is being protected through this approach. In the case of the EternalBlue exploit used in NotPetya and WannaCry, the Department of Defense resolved vulnerabilities in their systems without informing the public. That cybersecurity is only distributed to state organs through the stabilization of technical insecurity suggests that there is an inversion in the distribution of security—that the state engages in the distribution of in-security of information networks and computer systems. The second consequence is that it leaves civilian and commercial actors open to attacks from belligerents who exploit vulnerabilities known only to security services, ironically state systems are hardened against belligerents while the inhabitants of a states' territory are left vulnerable. The deterrent effects of having an airbase near a border distributes security both to vulnerable military assets further in the interior as well as civilian populations who could be attacked from the air, whereas the development of cyber-capabilities does not extend the same type of protection to civilian populations.

One could object to the uniqueness of this dynamic by highlighting the fact that weapons production, testing, and use frequently imposes negative externalities on domestic populations. For example, industrial processes may pollute or the air or water which poisons a civilian population, thereby exposing them to a health risk. Likewise, a similar argument is made that the very existence of atomic weapons, because of the magnitude of their power, places the entire world at risk. While these certainly expose the unevenness of security and the maintenance of the well-being of populations; the cyber in/security paradox is substantially different because the existence of vulnerabilities across a wide range of information and computer systems while

unavoidable is also resolvable. The vulnerability of a human body to radiological effects or pollution is a consequence of the biological nature of human life, thereby this vulnerability is an unavoidable feature of human existence. The problem of cyber in/security is that cyber-vulnerabilities are fundamentally engineering problems and therefore can be resolved, the choice not to resolve them for the sake of creating cyber-weapons is how insecurity is distributed throughout sovereign territory by states.

4 Conclusion

Overall, what is novel about cyberspace and sovereignty is that that states are utilizing cyberspace for security purposes in such a manner as to stabilize insecurity across cyber infrastructure. The fact that states are turning towards the weaponization of cyber infrastructure by exploiting rather than resolving latent flaws within the infrastructure challenges the traditional functional relationship of sovereignty. This distribution and maintenance of vulnerability across infrastructure signals a transformation of kind and not scale—it calls into question who is the subject of state security practices and the relationship between a state and its sovereign territory. While at the moment the individual consequences of this distribution of vulnerability are largely limited to financial crimes or invasions of privacy, the potential for much greater effects is rapidly expanding as ever more-mundane or private aspects of human life come to be accessible through cyberspace. The rise of the "Internet of Things" promises to extend network connectivity to everything from cars to personal massagers, this integration into everyday life creates a great potential for uncontrollable cascading effects and great mishap.[52] Critically, the core problem of the cyber in/security paradox is not about the decline of the state, but rather about an increasing distance between the security functions of the state and the safety of domestic populations.

On a methodological level, this paper made the case for greater attention to the built and

[52] ex.: car being remotely disabled, leak of telemetry data collected by personal massagers

infrastructural basis of cyberspace. Rather than treating cyberspace as an exogenous or emergent factor of the international system that states control or instrumentalizes, more attention needs to be paid as to how states constitute infrastructure as a security threat and instrument. In the case of sovereignty, reifying cyberspace as a challenge to state sovereignty ignores the power strategies that states employ when managing infrastructure and their implications. Scholarship in international relations and in particular security studies needs to be far more sensitive to the interaction between human politics and technology. Outside of the study of nuclear weapons, technology is largely treated as either deterministic or plastic—both of these perspectives miss the way in which technology and human politics are intertwined.[53] The rapid deepening and widening of the role of cyber infrastructure and digital information technology into the fabric of political life necessitates paying closer attention to how states articulate security by, within, and through cyberspace.

[53]Geoffrey Herrera, *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change* (Albany, New York, 2006); McCarthy, *Power, information technology, and international relations theory: The power and politics of US Foreign policy and internet*; Langdon Winner, "Do Artifacts Have Politics?," *Daedalus* 109, no. 1 (1980): 121–136

References

Abbate, Jane. *Inventing the Internet*. Inside Technology. Cambridge, MA: MIT Press, 2000.

Air Force Office of the Chief of Staff. *Cornerstones of Information Warfare*. http://www.c4i.org. [Online; accessed May 25, 2017], 1995. http://www.c4i.org/cornerstones.html.

Albon, Lillian, and Andy Bogart. *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and the Their Exploits*. Santa Monica, CA: RAND Corporation, 2017.

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (Spring 1993): 141–165.

Atwood, Donald J. *TS 3600.1*. DOD FOIA Online Reading Room, 12-21-1992. http://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Other/14-F-0492_doc_01_Directive_TS-3600-1.pdf.

Barlow, John Perry. *A Declaration of the Independence of Cyberspace*, 1996. Accessed October 15, 2016. https://projects.eff.org/%7B~%7Dbarlow/Declaration-Final.html.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8, no. 2 (2014): 121–144. doi:10.1111/ips.12048. https://doi.org/10.1111/ips.12048.

Benkler, Yochai, Robert Faris, and Hal Roberts. *Network Propaganda*. New York, NY: Oxford University Press, 2018.

Betz, David, and Tim Stevens. *Cyberspace and the State: Towards a Strategy for Cyber-Power*. Abingdon, United Kingdom: Routledge, 2011.

Cavelty, Myriam Dunn. *Cyber-security and threat politics: US efforts to secure the information age*. London, UK: Routledge, 2007.

Choucri, Nazli. *Cyberpolitics in International Relations*. 320. Cambridge, Massachusetts: MIT Press, 2012.

Choucri, Nazli, and D D Clark. "Who controls cyberspace?" 69, no. 5 (2013): 21–31.

Chowdhury, Arjun, and Raymond Duvall. "Sovereignty and Sovereign Power." *International Theory* 6, no. 2 (2014): 191–223.

Cimpanu, Catalin. *US government releases post-mortem report on Equifax hack*. ZDNet. (Accessed on 11/03/2018), 9/7/2018. https://www.zdnet.com/article/us-government-releases-post-mortem-report-on-equifax-hack/.

Clinton, Hillary. *SECRETARY OF STATE HILLARY RODHAM CLINTON REMARKS ON INTERNET FREEDOM*. [Online; accessed 10-May-2017], February 15, 2011. https://www.eff.org/files/filenode/clinton_internet_rights_wrongs_20110215.pdf.

———. *The prepared text of U.S. of Secretary of State Hillary Rodham Clinton's speech, delivered at the Newseum in Washington, D.C.* [Online; accessed 10-May-2017], January 21, 2010. http://foreignpolicy.com/2010/01/21/internet-freedom/.

Council on Foreign Relations. *Reforming the U.S. Approach to Data Protection and Privacy*. https://www.cfr.org/report/reforming-us-approach-data-protection. [Online; accessed 11/05/2018], 1/30/2018.

Deibert, Ronald. "The geopolitics of internet control." In *Routledge Handbook of Internet Politics*, edited by Andrew Chadwick and Philip Howard, 323–336. London, UK: Routledge, 2008.

Deibert, Ronald J. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. New york, New York: Penguin, 2013.

Deibert, Ronald J., and Rafal Rohozinski. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology* 4, no. 1 (2010): 15–32.

Demchak, Chris C., and Adam B. Lowther. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5, no. 1 (2011): 32–62.

Denardis, Laura. *Internet Architecture as a Proxy for State Power*. [Online; accessed 10-May-2017], August 2015. http://www.ipjustice.org/wp-content/uploads/2015/08/IPJustice_Journal_DeNardis_Internet_Architecture.pdf.

———. *Protocol Politics: The Globalization of Internet Governance*. Cambridge, Massachussetts: MIT Press, 2009.

Diamond, Larry. "Liberation Technology." *Journal of Democracy* 21, no. 3 (2010): 69–83. doi:10.1353/jod.0.0190. https://doi.org/10.1353/jod.0.0190.

DiNardo, R. L., and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." *Airpower Journal* IX, no. 4 (Winter 1995): 69–79.

Dyson, E. *Release 2.0: A Design for Living in the Digital Age*. New York, NY: Viking, 1997.

Firchow, Pamina. "A Cuban Spring? The Use of the Internet as a Tool of Democracy Promotion by United States Agency for International Development in Cuba." *Information Technology for Development* 19, no. 4 (2013): 347–356. ISSN: 02681102.

FireEye. *What is a Zero-Day Exploit?* FireEye. [Online; accessed 11/02/2018], n.d. https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html.

Galeotti, Mark. *Putin is Waging Information Warfare. Here's How to Fight Back*, 2016. Accessed December 14, 2016. http://www.nytimes.com/2016/12/14/opinion/putin-is-waging-information-warfare-heres-how-to-fight-back.html.

Gallagher, Sean. "What the government should've learned about backdoors from the Clipper Chip." *Ars Technica*, December 14, 2015. https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/.

Galloway, Alexander R., and Eugene Thacker. *The Exploit: A Theory of Networks*. Minneapolis, MN: University of Minnesota Press, 2007.

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly*, no. 53 (2009): 1155–1175.

Hayden, Michael V. *Playing to the Edge: American Intelligence in the Age of Terror*. New York, NY: Penguin, 2016.

———. "The Future of Things "Cyber"." *Strategic Studies Quarterly*, 2011, 3–7.

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace 1986-2012*. Baltimore, Maryland: The Atlantic Council, 2013.

Herrera, Geoffrey. *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*. Albany, New York, 2006.

Herz, John H. "Rise and Demise of the Territorial State." *World Politics* 9, no. 4 (1957): 473–493.

Hobbes, Thomas. *Leviathan*. Edited by C.B. MacPherson. New York, NY: Penguin, 1982.

Hughes, Rex. "A treaty for cyberspace." *International Affairs* 86, no. 2 (2010): 523–541.

Joint Chiefs of Staff. *JP 3-12 Cyberspace Operations*. Chairman of the Joint Chiefs of Staff, 2018.

Kalathil, Shanthi, and Taylor C. Boas. *Open Networks Closed Regimes*. Washington, D.C.: Carnegie Endowment, 2003.

Kaplan, Fred. *Dark Territory: The Secret History of Cyberwar*. New York, NY: Simon / Schuster, 2016.

Kello, Lucas. *The Virtual Weapon and International Order*. New Haven, Ct: Yale University Press, 2017.

Kolodny, Lora. *Eric Schmidt, ex-Google CEO, predicts internet bifurcation with China*. CNBC. (Accessed on 11/04/2018), September 2018. https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html.

Krasner, Larry. *Sovereignty: Organized Hypocrisy*. Princeton, NJ: Princeton University Press, 1999.

Lawson, Sean. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-threats." *Journal of Information Technology and Politics* 10, no. 1 (2013): 86–103.

Leiner, Barry M, Vincent G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen P. Wolff. *Brief History of the Internet*. Internet Society. [Online; accessed June 20, 2015], 1997. `http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet`.

Levine, Yasha. *Surveillance Valley: The Secret Military History of the Internet*. New York, NY: Public Affairs, 2018.

Libicki, Martin. *Cyberspace in Peace and War*. Annapolis, Maryland: Naval Institute Press, 2016.

———. "Cyberspace is a not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* 8, no. 1 (2012): 321–336.

———. "Why Cyber War Will Not and Should Not Have Its Grand Strategist." *Strategic Studies Quarterly* 7, no. 4 (Spring 2014): 23–45.

———. "Why Cyber War Will Not and Should Not Have Its Grand Strategist." *Strategic Studies Quarterly* 14, no. 1 (Spring 2014): 23–39.

Lukasik, S. "Why the Arpanet Was Built." *IEEE Annals of the History of Computing* 33, no. 3 (March 2011): 4–21.

Lute, Jane Holl, and Bruce McConnell. "OP-ED: A CIVIL PERSPECTIVE ON CYBERSECURITY." [Online; accessed March 20, 2017], *Wired Magazine*, 2-14-2011. `https://www.wired.com/2011/02/dhs-op-ed/`.

Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (2010): 97–108.

May, Timothy. "Crypto Anarchy and Virtual Communties." In *Crypto Anarchy, Cyberstates, and Pirate Utopias*, edited by Peter Ludlow, 65–81. Cambridge, MA: MIT Press, 2001.

———. "The Crypto Anarchist Manifesto." In *Crypto Anarchy, Cyberstates, and Pirate Utopias*, edited by Peter Ludlow, 61–65. Cambridge, MA: MIT Press, 2001.

McCarthy, Daniel R. *Power, information technology, and international relations theory: The power and politics of US Foreign policy and internet*. London, UK: Palgrave Macmillan, 2015.

McGraw, Gary. "Cyber War is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies*, 2013, 1–11.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York, New York: Perseus, 2011.

Morris, Chris, Janet Morris, and Thomas Baines. "Weapons of Mass Protection: Nonlethality, InformationWarfare, and Airpower in the Age of Chaos." *Airpower Journal* IX, no. 1 (Spring 1994): 15–29.

Mosco, Vincent. *The Digital Sublime: Myth, Power, and Cyberspace*. Cambridge, MA: MIT Press, 2005.

Mueller, Milton. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010.

n.a. *Why the market for zero-day vulnerabilities on the dark web is vanishing*. Fifth Domain. [Online; accessed 11/02/2018], 2018. https://www.fifthdomain.com/industry/2018/09/25/why-the-market-for-zero-day-vulnerabilities-on-the-dark-web-is-vanishing/.

Nakashima, Ellen, and Craig Timberg. *NSA officials worried about the day its potent hacking tool would get loose. Then it did.* The Washington Post. [Online; accessed 11/03/2018], May 2017. https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html?utm_term=.37e8379279ad.

Powell, Colin. *Chairman of the Joint Chiefs of Staff Memorandum of Policy No. 30 (CMOP); Command and Control Warfare*. Defense Technical Information Center. [Online; accessed June 11, 2017], 1993-3-8. http://www.dtic.mil/docs/citations/ADA389344.

Rid, Thomas. *Cyber War Will Not Take Place*. New York, NY: Oxford University Press, 2013.

Rid, Thomas, and Peter McBurney. "Cyber-Weapons." *The RUSI Journal* 157, no. 1 (2012): 6–13.

Roberts, Margaret E. *Censored: Distraction and Diversion Inside China's Great Firewall*. Princeton, NJ: Princeton University Press, 2018.

Schmitt, Carl. *Political Theology: Four Essays on the Concept of Sovereignty*. Chicago, IL: University of Chicago Press, 2005.

Singer, P.W., and Emerson T. Brooking. *LikeWar: The Weaponization of Social Media*. New York, NY: Houghton Mifflin Harcourt, 2018.

Stein, George J. "Information Warfare." *Airpower Journal* IX, no. 1 (Spring 1995): 30–55.

Szafranski, Richard. "A Theory of Information Warfare: Preparing for 2020." *Airpower Journal* IX, no. 1 (Spring 1995): 56–65.

The White House. *National Security Decision Directive Number 145: National Policy on Telecommunications and Automated Information Systems Security*. Federation of American Scientists. [Online; accessed June 12, 2017], 9-17-1984. https://fas.org/irp/offdocs/nsdd145.htm.

Toffler, Alvin, and Heidi Toffler. *War and Anti-War*. New York, NY: Grand Central Publishing, 1995.

United Nations Human Rights Council. *Report of the independent international fact-finding mission on Myanmar*. United Nations Human Rights Council. (Online; accessed 11/04/2018), 2018. %5Curl % 7Bhttps : / / www . ohchr . org / Documents / HRBodies / HRCouncil / FFM - Myanmar/A_HRC_39_64.docx%7D.

Valeriano, Brandon, and Ryan C Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press, 2015.

Warner, Michael. "Notes on the Evolution of Computer Security Policy in the US Government 1965-2003." *IEEE Annals of the History of Computing* 37, no. 2 (April 2015).

Weber, Max. *Politics as a Vocation*. New York, NY: Oxford University Press, 1946.

Whitehead, YuLin. "Information as a Weapon: Reality versus Promises." *Airpower Journal* XI, no. 3 (Fall 1997): 40–54.

Winner, Langdon. "Do Artifacts Have Politics?" *Daedalus* 109, no. 1 (1980): 121–136.

Wu, Timothy. "Cyberspace Sovereignty?—The Internet and the International System." *Harvard Journal of Law & Technology* 10, no. 3 (1997): 647–666.