Mutually Assured Vulnerability: An Ecological Approach to the Study of Coercion and Power in Cyberspace

By Hans-Inge Langø, August 22nd, 2018

Despite years of debate and a growing body of scholarship, the future of cyber conflict remains unclear. The discussion has hinged on the arrival (or lack thereof) of some kind of cyber war, but the almost exclusive focus on a very specific phenomenon has stymied efforts to understand the actual object of analysis: cyberspace. This paper proposes a new study to cyber security where cyberspace is conceived of as an ecological system where the actors and the structure interact. By identifying the defining characteristics of cyberspace itself we can better understand the sources of cyber power, and thus how actors can achieve their political goals. Because cyberspace is a malleable system, the implication is that actors will attempt to change the structure itself in order to achieve strategic advantages. Coupled with asymmetric information and offensive advantage, this causes severe collective action problems between states and the deterioration of the viability of cyberspace as open system.

INTRODUCTION

For over twenty years we have waited for the arrival of cyber war, yet none have come.[1] Despite the spread and ubiquity of information communications technology (ICT) throughout society, and increased militarization of cyberspace, there are but a handful of examples of serious and complex cyber attacks.[2] The absence of cyber war has not tempered debate on cyber security, but the political and strategic implications of the information revolution on international security remain underexplained and undertheorized. By focusing on large-scale, complex attacks the debate has failed to highlight the practical and theoretical implications of the information revolution. This has been exacerbated by disagreements about the conceptual and empirical nature of cyberspace.[3] The result is that we are far away from any conclusive thoughts on how ICT affects international relations and conflict.[4]

[1] The initial, or most famous, proclamation of how the information revolution would lead to an age of cyberwar came from RAND researchers John Arquilla and David Ronfeldt. See: John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (1993): 141–65.

[2] The most prominent examples are Stuxnet, cyber attacks against the Estonian government in 2007, and cyber attacks during the Russo-Georgian war. A larger study counted 110 cyber incidents and 45 cyber disputes in the period 2001-2011, though many of those were minor events. See: Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11," *Journal of Peace Research* 51, no. 3 (2014): 347–60.

[3] For a broader review of the various schools of thought on cyber security and the disagreements between the camps, see: Hans-Inge Langø, "Competing Academic Approaches to Cyber Security," in *Conflict in*

This paper seeks to chart a new way forward by theorizing the coercive power of cyberspace from a bottom-up perspective, rather than focusing on parochial questions or science-fiction scenarios.[5] I do so because we cannot explain behavior in and through cyberspace without identifying the sources and origins of cyber power. Power helps explain behavior, which in turn allows us to draw clear implications for conflict and cooperation between actors, and particularly states, in cyberspace. In short, I argue that the defining characteristics of cyberspace exacerbate both domestic cooperation problems and international commitment problems. These factors suggest that low-level conflict in cyberspace is likely to continue for the foreseeable future.

To explain how cyberspace affects international conflict, I propose a novel approach to the study of cyber security and cyber power based on a new conceptualization of this amorphous system. Instead of considering cyber security as merely a new set of technologies, the paper takes a holistic approach to cyberspace. If we assume that cyber power is derived from cyberspace itself and how an actor uses or manipulates it, the first step to defining cyber power is to describe cyberspace. The paper conceptualizes cyberspace as an ecological system where the actors and the structure interact, and the former can and will affect the latter. By focusing on cyberspace, rather than particular implications or events, and defining cyber power more broadly, the approach here will produce a general framework for future research.

This paper posits that cyberspace has four defining characteristics: it is malleable, a hybrid of physical and virtual layers, networked and software-centric. All of these characteristics carry security implications, some of which feature prominently in the cyber security debate, for

---

Cyber Space, ed. Karsten Friis and Jens Ringsmose (London: Routledge, 2016). For discussions on the militarization of cyberspace, see: Ronald J. Deibert, "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace," *Millennium-Journal of International Studies* 32, no. 3 (2003): 501–30; Panayotis Alexander Yannakogeorgos, *Technogeopolitics of Militarization and Security in Cyberspace* (ProQuest, 2009); Sean Lawson, "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History," Working paper (Fairfax, VA: Mercatus Center, January 2011).

[4] The one issue that does seem clear by now is that cyber war will not happen. Cyber war implies a military conflict that exists solely or primarily in cyberspace. Many have criticized the term for being both theoretically and empirically inappropriate for the type of conflict we see or are likely to see in regards to cyberspace. See: Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013); Erik Gartzke, "The Myth of Cyberwar," *International Security* 38, no. 2 (Fall 2013): 41–73; Lucas Kello, "The Meaning of the Cyber Revolution," *International Security* 38, no. 2 (Fall 2013): 7–40.

[5] I use Joseph Nye, Jr.'s definition of cyber power and David J. Betz and Tim Stevens' definition of compulsory cyber power for this paper. Cyber power is defined behaviorally as "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain. Cyberpower can be used to produce preferred outcomes *within* cyberspace, or it can use cyberinstruments to produce preferred outcomes in other domains *outside* cyberspace." Compulsory cyber power is "direct coercion by one cyberspace actor in an attempt to modify the behaviour and conditions of existence of another." See: Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011), 123; David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (New York: Routledge, 2011), 45. Betz and Stevens' framework for cyber power is based on an existing framework of power in international relations. See: Michael Barnett and Raymond Duvall, "Power in International Politics," *International Organization* 59, no. 01 (2005): 39–75.

instance the difficulty of attributing hostile actions to actors in cyberspace. This is a pervasive feature of cyber conflict, but it is not a defining characteristic. Rather, it is the product of the idiosyncratic nature of the Internet made possible by the malleability of cyberspace, coupled with its decentralized, networked nature. The defining characteristics presented here should outline what behavior is encouraged in cyberspace and what behavior is not encouraged. In other words, we assume that the characteristics of cyberspace, to a certain extent, influence actor behavior.[6] This is not to say that the nature of cyberspace will or will not encourage conflict, but it might favor some types of operations over others.

I argue that the characteristics of cyberspace affect actor behavior because they are the source of cyber power. Many scholars focus primarily on compulsory cyber power, as defined by David J. Betz and Tim Stevens as "the use of direct coercion by one cyberspace actor in an attempt to modify the behaviour and conditions of existence of another."[7] However, by systematically studying cyberspace itself, and thus the source of cyber power in its various forms, we get a broader understanding of cyber conflict. In this paper I argue specifically that the potential for compulsory cyber power is in large part affected by control or influence over cyberspace, and particularly the structure (i.e. structural cyber power).[8] Because cyberspace is malleable, the future of cyber conflict is dependent on how actors attempt to shape cyberspace going forward, and not just how they exploit it today. Thus, to paraphrase Alexander Wendt, cyber conflict is to a certain extent what states choose to make of it.[9]

Whether states seek conflict or cooperation depend on several factors, but cyberspace's defining characteristics exacerbate both domestic cooperation problems and international commitment problems. At home, governments have to balance economic (defensive) concerns with national security (offensive) issues. Because offense and defense are two sides of the same coin, the two objectives are at odds, leading states to pursue at times contradictory policies. In the international sphere, the ability to affect the structure of cyberspace itself encourages defection and prohibits cooperation. If states seek to pursue offensive capabilities, this affects other states, thus potentially leading to a death spiral. Furthermore, states cannot know for sure whether others are abiding by agreements or, worse, preparing or committing hostile actions. Information asymmetries and monitoring problems thus cause serious commitment problems.

The first section of the paper will give a brief overview of the relevant literature on strategic cyber security. It will show what are some of the prevailing ideas and concepts, but also

---

[6] I focus primarily on states as the wielders of power, but the analysis shows how non-state actors, such as private companies, are important parts of the system, and as such distinguishes cyber security from other realms of security.

[7] Betz and Stevens, *Cyberspace and the State*, 45.

[8] Betz and Stevens use the term structural cyber power to define how cyberspace shapes the structural positions of actors, but this paper is more interested in how actors work to shape the structure. There is some overlap here with compulsory and institutional cyber power, as defined by Betz and Stevens, but through which avenues actors shape the structure is secondary to this discussion.

[9] Alexander Wendt, "Anarchy Is What States Make of It: The Social Construction of Power Politics," *International Organization* 46, no. 2 (1992): 391–425.

demonstrate shortcomings in the academic literature. In the next section, I will present my own analytical framework for understanding cyberspace and cyber power. This section will define the four defining characteristics and the resulting implications that are the most relevant for international security. The last section will discuss the theoretical and practical implications of using an ecological approach to cyber security. It will do so by examining the relationship between the defining characteristics and cyber power and the numerous obstacles to cooperation. The section will conclude by offering up policy implications and future avenues of research.

EVOLVING IDEAS

In this paper I define the practice of cyber security as the effort to protect or compromise the integrity of ICT systems and their data and functions. From an academic perspective, the study of cyber security is still evolving, in part because cyber security itself is in its nascent stage. We can trace discussions of information warfare, a broader term that encompasses much of the ideas of computer network operations (CNO) prevalent today, at least back to the 1970s. However, most of the significant academic contributions to the field have been published in the past two decades.[10] While there is much written now on cyber security, it remains a fragmented field of disparate approaches and conceptual thinking.[11] These approaches can offer significant elucidation of certain questions, but are often narrow in focus or based on concepts of other forms of power. For instance, the foundational writings of John Arquilla and David Ronfeldt in the 1990s articulated the impact the information revolution could have on warfare and even societal conflict. [12] More specifically, information was treated as a material asset, and they posited that information dominance through organizational superiority could be translated into battlefield victory. [13] However, their work does not sufficiently describe how actors can exploit cyberspace vulnerabilities, especially in a civilian setting. Their work is as much about organization and doctrine as it is about cyberspace as a strategic environment. As such, it is more appropriate for military planning than for examining cyber power in a larger setting encompassing the private sector and civil society.

Another important component of the cyber security literature is the work surrounding strategic information warfare (SIW). SIW is defined as a way of waging cyber warfare on the

[10] For an early example of Pentagon thinking on information warfare, see Thomas P. Rona, "Weapon Systems and Information War" (Office of the Secretary of Defense, July 1, 1976). For an historical overview of information warfare in the U.S. military, see Bruce D. Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century* (New York, NY: Free Press, 2003), chap. 4 and 6.

[11] For a broader discussion on the literature of cyber security, see: Langø, "Competing Academic Approaches to Cyber Security."

[12] Arquilla and Ronfeldt's concept of 'netwar', information-based conflict on a societal level, will be discussed towards the end of this paper. A collection of their most important works can be found in John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997).

[13] Libicki has written similarly on using information superiority through the use of sensors to control the battlefield. See Martin C. Libicki, "The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon" (Washington, DC: National Defense University, March 1994), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA278484&Location=U2&doc=GetTRDoc.pdf.

strategic level, causing independently decisive effects on a target through the use of CNO.[14] The most likely manifestation of this type of warfare would be large-scale, complex attacks against critical national infrastructure (CNI). As an idea, SIW has laid the foundation for many scholars' take on cyber power. Usually this has come in the form of comparative analyses, comparing cyberspace with other domains or powers, such as air power or even nuclear power. While the use of analogies can be helpful in highlighting differences, too often it is used to show how cyber power can resemble air power or why cyberspace is similar to the maritime domain because they share some commonalities; for instance, they both have chokepoints of sorts.[15] This approach is problematic since it inevitably runs the risk of shoehorning something new into an old analytical framework.[16] It also leads to conceptual and terminological confusion since there is no consensus on key terms and definitions related to cyberspace. Furthermore, such a top-down approach to the study of cyberspace is not conducive to examining the nature of the environment as it means studying particular trends or transient phenomena observed at the time of the analysis rather than the defining characteristics of cyberspace.

More recent work on cyber security has focused on studying the empirical and conceptual character of cyber conflict as it stands today. Scholars have made persuasive arguments that delineate the limits of compulsory cyber power.[17] Thomas Rid argues that cyberspace is not conducive to fighting wars, but more appropriate for sabotage, espionage and subversion.[18] Other scholars of international relations have reached similar conclusions.[19] Erik Gartzke argues that cyber tools have limited coercive or compellent power, while Lucas Kello says that they are

---

[14] For a broader discussion on SIW, see: Roger C. Molander, Andrew Riddile, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War" (Santa Monica, CA: RAND Corporation, 1996), http://www.rand.org/pubs/monograph_reports/MR661.html; Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001).

[15] For examples of scholarly use of analogies in regards to cyber security, see: Rattray, *Strategic Warfare in Cyberspace*; Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 253–74; Andrew F. Krepinevich, "'Cyber Warfare: A "Nuclear Option"?'" (Washington, DC: Center for Strategic and Budgetary Assessments, August 24, 2012), http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/; Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 24–42.

[16] Jean-Loup Samaan, "Cyber Command: The Rift in US Military Cyber-Strategy," *The RUSI Journal* 155, no. 6 (2010): 16–21; David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue* 44, no. 2 (2013): 147–64.

[17] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32; David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York: Frank Cass, 2004).

[18] Rid, "Cyber War Will Not Take Place," 2012.

[19] For recent scholarship on the limits of cyber operations as a coercive tool, see: Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, USA, 2015); Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford University Press, 2018).

more appropriate for social or economic destabilization.[20] Furthermore, Jon R. Lindsay argues that cyberspace favors strong states, rather than leveling the playing field.[21]

This new scholarship has helped cool the cyber hype, but it has limitations for studying cyber power in a more systematic fashion. First, it is overly focused on violence as a necessary component of warfare, understating the disruptive potential of cyber warfare.[22] As societies grow more dependent on ICT, so does the number of vulnerabilities, thus potentially making compulsory cyber power more tenable than scholars claim. Second, the available data is simply insufficient to generalize about the security implications of cyberspace. While the lack of large-scale cyber attacks so far could be used as an argument against SIW, it must be noted that most actors are still grappling with the security implications of cyberspace. Third, much of the current scholarship assumes implicitly that cyberspace is a static environment. As such, they rightly point out the limitations of compulsory cyber power today, but do not consider how the source of that power can change structurally, either through concerted effort by actors or through complex market dynamics. Furthermore, the relationship between compulsory cyber power and other forms of cyber power are not sufficiently considered.

Other scholars have attempted a more systematic and holistic approach to the study of cyberspace. Appropriately, these scholars often focus on power, but their work is better defined by its analytical approach, namely the environmental analysis of cyberspace. The 'environmentalist' approach entails examining cyberspace as a whole, be it an environment or a domain, to define its key characteristics or strategic features.[23] For instance, when Joseph Nye, Jr. attempts to define cyber power, he uses an environmental analysis to describe its character.[24] Nye's main focus is the diffusion of power occurring in cyberspace, while others focus on different characteristics. Libicki indirectly addresses compulsory cyber power in his work on deterrence and conquest in cyberspace, while Gregory R. Rattray approximates a systematic analysis of cyberspace's "strategic features" in a 2009 book chapter appropriately called "An Environmental Approach to Understanding Cyberpower."[25] All of these works inform our discussion about particular characteristics or phenomena, but do not necessarily account for the

[20] Gartzke, "The Myth of Cyberwar"; Kello, "The Meaning of the Cyber Revolution."
[21] Jon R. Lindsay, "Stuxnet and the Limits of Cyberwarfare," *Security Studies* 22, no. 3 (2013): 365–404.
[22] While Rid defines violence as a requirement for war, other scholars argue that states can use force without bloodshed and still achieve political goals. Whether such behavior qualifies as war might be a question of semantics, so this paper primarily uses the term cyber conflict. See: Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld & Nicolson, 2005), 293–94; Phillip S. Meilinger, "The Mutable Nature of War," *Air & Space Power Journal* 24, no. 4 (2010): 24–30; John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies* 36, no. 1 (2013): 101–8.
[23] There are various terms used in the literature, but they mean essentially the same thing. This discussion will use the former term, whereas Gregory J. Rattray uses the latter in his writing.
[24] Nye, *The Future of Power*, chap. 5.
[25] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007); Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009); Rattray, "An Environmental Approach to Understanding Cyberpower."

relationship between the actors and the structure. I therefore synthesize their insights into a more general ecological understanding of cyberspace.

AN ECOLOGICAL APPROACH

An ecological approach to cyberspace means mapping the terrain of cyberspace and describing what actions cyberspace either encourages or restrains. The approach used in this paper borrows from several of these texts.[26] However, the approach used here is different from previous work in two respects. First, this paper considers the relationship between the technological environment and the actors participating in it with the assumption that the actors' behavior can and will affect the landscape. As such, cyberspace is better understood as a dynamic ecological system than as a static landscape.[27] Second, it distinguishes between the defining characteristics of cyberspace and its security implications. Implications are the result of the defining characteristics, and so the former can, hypothetically, only change if the latter changes first. This distinction also makes it easier to explain which issues are merely fleeting, based on a particular technology or standard, and which are more likely to be enduring features of cyber conflict. Much of the existing literature either conflates or confuses the two, so establishing these causal relationships has significant importance for both future analysis and policy prescriptions.

What is unique about cyberspace, and this will be discussed below in more detail, is that it is a non-hierarchical system. There are numerous examples of literature from both the social sciences and other disciplines that examine the relationship between actors and structures in these types of systems, and how interaction between the various parts causes systemic changes.[28] This paper is not an attempt to settle the agency-structure debate, but instead uses the basic

---

[26] Several scholars have done environmental studies of cyberspace, either explicitly or implicitly through the study of cyber power. For examples, see Joseph S. Nye, *The Future of Power* (New York: Public Affairs, 2011); Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 253–274; Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009), 24–42; David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a strategy for cyber-power* (New York: Routledge, 2011); Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007).

[27] "Cyberspace as 'EcoSpace,'" SENDS, November 5, 2010, http://sendsonline.org/2010/11/05/cyberspace-as-ecospace/; Carl Hunt, "The Blogging Luddite: The Two-and-a-Half Faces of Cyberspace Security," SENDS, April 25, 2011, http://sendsonline.org/2011/04/30/the-blogging-luddite-the-two-and-a-half-faces-of-cyberspace-security/.

[28] Network theory is often used in the study of international political economy, but similar approaches to security and conflict could be beneficial. For instance, Aaron Frank has used evolutionary theory to explain how revolutions in military affairs affect the international system. See Aaron Frank, "Military Revolutions, Evolution, and International Relations Theory" (American Political Science Association Annual Convention 2010, Washington, D.C., 2010).

concept as a heuristic device for understanding cyberspace and its actors. There are no directly applicable models to the subject of cyber security, but the paper draws on certain interdisciplinary research. Social-ecological system (SES) theory attempts to model the relationship between social actors and the natural environment in order to understand environmental issues such as pollution and deforestation. This ecological approach is taken to account for temporal and spatial variation, in addition to large degrees of uncertainty and complexity.[29] It is a useful analogy to cyberspace, with the caveat that unlike nature, cyberspace does not have the capacity to change itself—barring any introduction of artificial intelligence, which is beyond the scope of this paper. The similarity between the SES approach and an ecological approach to cyberspace is that the structure of cyberspace is defined not only by its existing properties but by its relationship with actors—another variable that is not static, as more actors join in the ecosystem.[30] Because a large part of what constitutes cyberspace today is manmade, and can therefore be changed, the claim that cyberspace is an ecological system should not be a difficult notion to accept. The more important question is: how does this approach benefit our understanding of cyber power, especially as it relates to the use of force, or threats thereof?

Scholars often list a number of characteristics that shape the threat environment, but these lists differ from scholar to scholar as some focus on a particular aspect of cyberspace while others focus on a specific threat or method. There is no authoritative list of the features of cyberspace, but based on an extensive reading of the literature, in addition to conversations with a wide range of scholars and practitioners, a comprehensive list of commonly accepted features would include: collapse of space and time, no conquerable ground, lack of warning of attacks, the difficulty in attributing actions to actors, a constantly changing and evolving battlefield, democratization of technology, and a low cost of entry.[31]

---

[29] For examples of how SES is used to study change and governance, see: Ian Scoones, "New Ecology and the Social Sciences: What Prospects for a Fruitful Engagement?," *Annual Review of Anthropology* 28, no. 1 (1999): 479–507; Carl Folke et al., "Adaptive Governance of Social-Ecological Systems," *Annu. Rev. Environ. Resour.* 30 (2005): 441–73; Brian Walker et al., "Resilience, Adaptability and Transformability in Social--Ecological Systems," *Ecology and Society* 9, no. 2 (2004): 5; Thomas Dietz, Elinor Ostrom, and Paul C. Stern, "The Struggle to Govern the Commons," *Science* 302, no. 5652 (2003): 1907–12.

[30] There are examples of agent-based modeling used to model interactions in cyberspace, but these are narrow models based on specific events, such as Denial of Service attacks between adversaries, and do not take into account the long-term effect actors have on the structure. For example, see: Igor Kotenko, "Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet," in *19th European Simulation Multiconference "Simulation in Wider Europe*, 2005; Azzedine Boukerche et al., "An Agent Based and Biological Inspired Real-Time Intrusion Detection and Security Model for Computer Network Operations," *Computer Communications* 30, no. 13 (2007): 2649–60.

[31] Conversations with scholars and practitioners have taken place primarily through the work with Multinational Experiment 7, a multinational concept development and experimentation campaign led by the U.S. Joint Staff with participants from 16 other countries and NATO ACT, focused on access to the global commons, of which cyberspace was a subject of study. The author represented Norway in this campaign from March 2011 to December 2012.

All of these so-called features can have an impact on security and actor behavior, but calling them characteristics or properties of cyberspace is imprecise. They are the implications of more fundamental characteristics of cyberspace. In other words, they are dependent variables. This paper proposes that there are, roughly speaking, four defining characteristics of cyberspace, and each of these has a set of security implications, with all of the above included. Making this distinction between characteristics and implications is important, because it means the latter can and most likely will change if the former changes. The four defining characteristics of cyberspace are those of being malleable, virtual, networked, and software-centric.

The characteristics interact; in some instances they reinforce each other's effects on behavior, while other times they have countervailing effects. However, I argue that malleability is the key, underlying characteristic of cyberspace because it defines the scope of the system and can affect, but not cause, the other characteristics. For example, malleability can make cyberspace more complex by expanding the use of ICT to new areas, but it cannot change the fact that the structure is networked to begin with. Similarly, cyberspace is characterized by the merger of physical and virtual layers. Malleability means that we can observe changes within these layers, but it cannot abolish the distinction between hardware and software.

A Malleable Terrain

Cyberspace is a manmade environment. While the electromagnetic spectrum is not, cyberspace as it exists today consists of hardware and software designed and built by people. Martin C. Libicki has divided cyberspace into three layers. The physical layer consists of tangible objects like wires, routers and servers, while the syntactic layer, often referred to as the logical layer, reflects the formation of information and "how the various information systems from which cyberspace is built are instructed and controlled."[32] The semantic layer "contains the information meaningful to humans or connected devices."[33] It is perhaps best understood as the cognitive function of cyberspace, bridging man and machine, or man and information. It is how information is conveyed to users, but it also has a social function when multiple users plug in at each end of the network.

The different layers of cyberspace are a result of decades of construction, be it deliberate or through a form of natural selection where some inventions become standard while others fall by the wayside. This means that the content and character of the various layers can be altered. New technologies to transmit signals might be invented, while new protocols and software for the syntactic layer are constantly amended or replaced. The layers of cyberspace, however, are seemingly set. While the protocols of the syntactic layer might change, there will always be a physical layer underneath it and a semantic layer above it. This is not to say that technical changes in cyberspace are themselves unlikely, merely that there are some 'laws of physics' governing the development in this environment. I call this feature 'vertical malleability.'

[32] Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 8.
[33] Libicki, 9.

Attributing malicious behavior in cyberspace, especially on the Internet, to specific actors is a widely referenced problem area in cyber security. The problem exists because of the way the Internet is built. It is easy to conceal the origin of a CNO because of the lack of a robust verification system and the ease with which one can reroute traffic through unsuspecting servers elsewhere. The attribution issue in cyberspace is an idiosyncratic property of the Internet, and as such a result of vertical malleability.

Furthermore, efforts to 'fix' the attribution problem show that security implications do not remain static. The Internet Engineering Task Force (IETF), which develops and promotes Internet standards, has developed IPv6, a new communications protocol that will replace the existing and dominating IPv4. IPv6 purports to fix the problem with attribution, or at least reduce it, by making packets of data easier to trace back to their origins. Whether this will actually happen is uncertain. In fact, the implementation of IPv6 might instead lead to new vulnerabilities.[34] Nonetheless, it is an example of how vertical malleability can impact security.

If vertical malleability concerns the character of cyberspace itself and its technologies, the other kind, 'horizontal malleability,' implies a change in how humans and society relate to cyberspace.[35] The two features may interact, but for the sake of clarity it is best to address them separately in this discussion. Horizontal malleability refers first and foremost to two processes: increased integration of ICT in society (quantity), and technology being used in new ways (quality), even changing the users themselves in the process. In short, this means that individuals, organizations and society are becoming increasingly dependent on cyberspace, for both existing and new functions.

Horizontal malleability is characterized by increased dependence on cyberspace. Given the nature of cyberspace, this almost inevitably means increased vulnerabilities. New software often means new vulnerabilities, and expanded use of ICT means new vulnerabilities in new places. From a defensive perspective, particularly for states, the battleground is in flux and the perimeter is in constant expansion. This process is happening on multiple levels. With the ubiquity of smart phones, there has been a significant proliferation of malware designed to compromise mobile operating systems. There are also concerns that medical devices in government officials could be hacked.[36] More significant attacks could be aimed at government structures or critical national infrastructure. This has lead to numerous initiatives aimed at improving public-private cooperation, for instance with several cross-sectoral cyber security exercises.[37]

---

[34] Atik Pilihanto, "A Complete Guide on IPv6 Attack and Defense" (Bethesda, Maryland: SANS Institute, November 14, 2011).

[35] Society is meant to include not just the public and private sector, but civil society as well.

[36] Andrea Peterson, "Yes, Terrorists Could Have Hacked Dick Cheney's Heart," Washington Post, October 21, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/.

[37] For example, see: "Quantum Dawn After Action Report" (New York: Security Industry and Financial Markets Association, March 5, 2012); "Quantum Dawn 2: A Simulation to Exercise Cyber Resilience and

The increased focus on critical infrastructure protection amongst many states suggests that governments and officials share this perception of uncertainty, though not all cyberspace-dependent functions in society are included in critical infrastructure protection. Uncertainty in matters of vulnerability and dependence lies at the heart of cyber policy efforts in the United States, the EU and other countries, so much so that the traditional risk and threat analysis approach is being at least partially replaced by a focus on resilience.[38] This new approach does not set aside calculations of risk or threats, but is based on the assumption that conducting a proper risk assessment is near impossible because it is not feasible to assess the full scope of one's vulnerabilities. They are so plentiful and unpredictable that both states and organizations base their cyber defense on the assumption that their networks will be penetrated or attacked. This acquiescence of risk is then coupled with an effort to build up resilience, which, simply put, means the ability to absorb malicious actions and recover.

By definition, the malleability of cyberspace is the most amenable of the defining characteristics. Both the vertical and horizontal dimensions are constantly changing, and so it is also the most influential of the four characteristics. It can change the other defining characteristics, and also dictate what cyber security means by its ability to change or expand cyberspace as an ecological system. The most obvious implication for policy is the persistent presence of uncertainty; vulnerabilities are by definition unknown and the threat landscape is dynamic. This is not to say that threats are unknown, as cyberspace does not create new hostile actors, but introduces new ways for them to assert power.

It is in this particular characteristic that we see the similarities between cyberspace and social-ecological systems. Malleability offers uncertainty, but also opportunity. If these characteristics are the source of cyber power, we can also see how affecting the characteristics affect power. For instance, the malleability of cyberspace means that actors can affect the structure of cyberspace. If certain actors have significant structural cyber power, they can use that to change their compulsory cyber power. As such, malleability is the foundation on which this paper's analysis is built on and essential to understanding cyber power.

A hybrid realm

Crisis Management Capabilities" (New York: Deloitte, October 21, 2013), http://www.sifma.org/uploadedfiles/services/bcp/after-actionreport2013.pdf?n=40439; "Cyber Storm Exercise Report" (Washington, D.C.: Department of Homeland Security National Cyber Security Division, September 12, 2006), http://www.dhs.gov/sites/default/files/publications/nppd/CSC/Cyber%20Storm%20I%20After%20Action%20Report.pdf; "Cyber Storm II Final Report" (Washington, D.C.: Department of Homeland Security National Cyber Security Division, July 2009), http://www.dhs.gov/xlibrary/assets/csc_ncsd_cyber_stormII_final09.pdf; "Cyber Storm III Final Report" (Washington, D.C.: Department of Homeland Security National Cyber Security Division, July 2011), http://www.dhs.gov/sites/default/files/publications/nppd/CyberStorm%20III%20FINAL%20Report.pdf.

[38] This observation is based on the work developing a threats and vulnerabilities methodology for cyberspace through MNE7.

Cyberspace is often described as a virtual or non-physical domain, because data is created, managed, and manipulated through the use of software. This is not entirely accurate. A significant part of what constitutes cyberspace is virtual, but it is dependent on a physical layer to function. The physical assets of cyberspace, like processors, wires and routers, permit the storage, modification, exchange and exploitation of information, but these processes are governed by what is commonly referred to as the syntactic or logical layer. The resulting information then exists in the semantic layer where users, human or otherwise, can access it.[39] We can thus say that one of the defining characteristics of cyberspace is that a significant part of its functions are done virtually, but enabled by a physical structure. This dualism is essential for understanding both the possibilities and limitations of cyber network operations.

The reason why these layers and processes are usually referred to as 'virtual' is a question of scale. The information in cyberspace is physical. It is stored on physical devices and exchanged through signaling, a process which involves real electrons. But because of the dramatic development in computer technology over the past half-decade, information can be stored or transmitted at remarkable speeds and in vast quantities. Gordon E. Moore predicted in 1965 that the number of transistors on integrated circuits would double approximately every two years, and this has turned out to be a prophetic statement of significant accuracy.[40] The processing speed of computers has increased exponentially for quite some time, and aided by fiber optics, networked environments like the Internet, communication has reached previously unimagined velocity in creating and sending information.

The immediate security implication of this virtual realm is the collapse of space and time. The collapse of space is only meant metaphorically; increased computing power and fast transfer methods mean that physical distance between the attacker and the defender is close to irrelevant as an operational issue. This is obvious with Chinese individuals or organizations penetrating U.S. government networks and U.S. agencies conducting large-scale computer network exploitation (CNE) in the Middle East, but these countries already possessed the ability to project force or assets across large distances before the advent of cyberspace. It is the equivalent of dropping paratroopers behind enemy lines, except that you are using commercial airplanes to do it, at network speed. Cyberspace makes this easier, but in reference to Nye's focus on power diffusion, the substantive change is that more actors can do it, and not just states. The rise of hacktivist groups such as Anonymous illustrates the borderlessness of cyberspace by being able to launch DDoS attacks against a wide range of targets from thousands of computers spread across several continents.[41]

---

[39] Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, chap. 10.

[40] Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics* 38, no. 8 (April 19, 1965).

[41] Saki Knafo, "Anonymous And The War Over The Internet," Huffington Post, January 30, 2012, http://www.huffingtonpost.com/2012/01/30/anonymous-internet-war_n_1233977.html; Saki Knafo, "Anonymous And The War Over The Internet (Part II)," Huffington Post, January 31, 2012, http://www.huffingtonpost.com/2012/01/31/anonymous-war-over-internet_n_1237058.html?ncid=edlinkusaolp00000003; Quinn Norton, "How Anonymous Picks Targets,

The strategic implication of the collapse of space is similar. Geography matters less than with conventional coercive tools, and it is easier to hold a distant opponent's assets at risk. Whereas traditional force projection or covert operations would run the risk of alerting an opponent beforehand, offensive cyber operations can leap across the map. This means most states can potentially have new coercive tools. Today, the United States is the only state with significant force-projection capability, but depending on the coercive utility of cyberspace, more states will be capable of limited force-projection. What impact such a development—a development that is contingent on more sophisticated cyber weapons and continued societal vulnerability related to cyberspace—will have on international security is unclear, but this will be further discussed in the final section of this paper.

Collapsing both speed and time means that CNOs seem to happen instantaneously. Targeted states or organizations are usually given little or no advance warning, enabling sneak attacks. Rapid attacks in cyberspace have been compared to the German blitzkrieg doctrine, but setting aside the discussion over the destructive potential of cyber weapons, there are important distinctions between tank warfare and cyber warfare. Arquilla and Ronfeldt argue that cyber warfare depends less on geographic terrain and having to rapidly penetrate an opponent's defensive line, and more on controlling the cyberspace environment. They write, "Cyberwar may require speedy flows of information and communications, but not necessarily a speedy or heavily armed offense like blitzkrieg. If the opponent is blinded, it can do little against even a slow-moving adversary."[42] This is similar to the idea of blitzkrieg serving as a form of strategic penetration, finding a weak point in the defensive line to strike at the nervous system of the opponent's military.[43]

The difference highlighted is important, but Arquilla and Ronfeldt inaccurately infer from this an advantage over blitzkrieg because cyberspace is not a purely virtual environment. Whereas tanks can advance after taking out a target, cyber weapons do not work that way. Cyber weapons by design exploit vulnerabilities in an opponent's network. Once that vulnerability has been exploited to gain access to or cripple a system, that weapon has been spent. Instead of being like a tank, a cyber weapon is like a single-shot rifle.[44] Furthermore, if the CNA does not destroy or adequately degrade the targeted network, system administrators will eventually be able to reboot the network, meaning the attacker will have to keep firing. Cyber attacks simply cannot dislodge an opponent.

Launches Attacks, and Takes Powerful Organizations Down," Threat Level, July 3, 2012, http://www.wired.com/threatlevel/2012/07/ff_anonymous/all/; Quinn Norton, "Anonymous 101: Introduction to the Lulz," Threat Level, November 8, 2011, http://www.wired.com/threatlevel/2011/11/anonymous-101/all/1.

[42] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 1997), 44.

[43] John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983), 36.

[44] Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal* 157, no. 1 (2012): 9.

As such, cyber weapons are better suited for cumulative effects, rather than sequential effects. Instead of utilizing "force in discrete, linear packages," a cumulative strategy using cyber weapons will "build gradual and nonlinear pressure on an opponent."[45] A cumulative strategy would then negate the possible gains from a surprise attack, alerting the opponent to the attack and enabling them to respond without a crippling first strike.

The limitations on surprise attacks mean the increase in speed only yields a limited first-move advantage.[46] On a strategic level, this has certain implications. Theoretically, states can mobilize without detection and attack faster than with kinetic strikes, but a digital blitzkrieg would necessitate cyber weapons much more sophisticated than what has been demonstrated today, in addition to a much larger organizational capacity for cyber warfare. Several states are seeking to increase their capacity, though little is known about their actual capabilities, particularly those related to offensive operations.[47]

We can thus say that while cyber operations offer some advantages in terms of temporal and spatial restraints, the effects are usually ephemeral. However, targets in cyberspace are not necessarily discreet, but rather connected and interdependent, even with physical processes. Therefore, the next subsection discusses the structure of cyberspace and how the defining characteristics discussed so far accumulate to a very complex picture of cyber power, and particularly coercive cyber power.

A Networked Space

Calling cyberspace a networked space has several meanings and implications. It means the environment is open and connectable. Be it the Internet or cyberspace, just about anyone can

[45] Adam Elkus, "Cyber Warfare...Brought To You By J.C. Wylie," Information Dissemination, May 31, 2012, http://www.informationdissemination.net/2012/05/cyber-warfarebrought-to-you-by-jc-wylie.html.
[46] For a broader discussion of first-move advantage in international relations theory, see Stephen Van Evera, *Causes of War: Power and the Roots of Conflict* (Ithaca: Cornell University Press, 1999).
[47] The conclusion that little is made public about states' offensive capabilities is based on the author's own observations following developments in cyber security over the past two years. For examples of countries actively pursuing offensive capabilities, see Gerard O'Dwyer, "Finland To Develop Cyber Defense 'Counterpunch,'" DefenseNews, October 20, 2011, http://www.defensenews.com/article/20111020/DEFSECT04/110200306/Finland-Develop-Cyber-Defense-Counterpunch-; Michael Fischer, Joerg Blank, and Christoph Dernbach, "Germany Confirms Existence of Operational Cyberwarfare Unit," Deutsche Presse-Agentur, June 5, 2012, http://www.stripes.com/news/germany-confirms-existence-of-operational-cyberwarfare-unit-1.179655; Nick Hopkins, "UK Developing Cyber-Weapons Programme to Counter Cyber War Threat," Guardian, May 30, 2011, http://www.guardian.co.uk/uk/2011/may/30/military-cyberwar-offensive; Scott Shane, "U.S. Officials Opening Up on Cyberwarfare," New York Times, September 26, 2012, http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html?pagewanted=all; Kim Eun-jung, "S. Korea to Upgrade Preparedness against North's Cyber, Nuclear Attacks," Yonhap News Agency, August 29, 2012, http://english.yonhapnews.co.kr/national/2012/08/29/18/0301000000AEN20120829008600315F.HTML.

connect using readily available technology. This also means cyberspace is decentralized. With the exception of some organizations that govern standards and protocols, there is no central authority that controls entry or usage. It is a network of networks. Combined, this means cyberspace is complex, with a large number of users ungoverned and largely unchecked. The implication of this networked complexity and interdependence is that it is practically difficult to limit the effects of cyber incidents to one particular country or region. Defining the exact structure of cyberspace is seemingly impossible, as it is more a concept than a cohesive, coherent structure, but some attempts have been made at examining the Internet, which can serve as an example for how networks within cyberspace work.

A 2007 study of the nodes that make up the Internet found that there are three subcomponents of the Internet: at the core is a small nucleus consisting of around 100 nodes, and around it is a fractal subcomponent consisting of around 15,000 nodes that can connect to the bulk of the Internet without congesting the nucleus.[48] The third subcomponent consists of around 5,000 isolated nodes that connect directly to the nucleus. By mapping and testing the relationship between the nodes and subcomponents, the researchers found that without the nucleus around 70% of the peer-connected nodes (the second subcomponent) remained connected. This suggests that while the nucleus is important for achieving full connectivity, the Internet is decentralized and robust.

Despite its decentralized nature, the Internet is not devoid of weak points. As opposed to scaled networks, where each node has roughly the same amount of connections, nodes in scale-free networks have a varying number of connections. Some have only one, like the third subcomponent discussed above, while others have many, like the Internet nucleus. The Internet is a scale-free network, and this has an impact on security. Studies of Internet resilience have shown that scale-free networks are more resilient to errors and failure than scaled networks. However, this robustness comes at a cost. Because some nodes have significantly more connections than others (i.e. the nucleus), intentional attacks aimed at those nodes can fragment and impair the network, making the Internet vulnerable to actors seeking to disrupt or degrade the network.[49]

The notion of weak points in cyberspace has obvious parallels to other subfields within international security. While sea power can mean the ability to control sea lanes and chokepoints, a comparable analogy in cyberspace would be the control of key points in the ICT infrastructure. Cyber power, like sea power, is about controlling the terrain to produce preferred outcomes.[50] The chokepoints in terms of cyberspace, according to Gregory J. Rattray, "include the physical

---

[48] Shai Carmi et al., "A Model of Internet Topology Using K-Shell Decomposition," *Proceedings of the National Academy of Sciences of the United States of America* 104, no. 27 (July 3, 2007): 11150–11154.
[49] Réka Albert, Hawoong Jeong, and Albert-László Barabási, "Error and Attack Tolerance of Complex Networks," *Nature* 406 (July 27, 2000): 378–82; Reuven Cohen et al., "Resilience of the Internet to Random Breakdowns," *Physical Review Letters* 85, no. 21 (November 20, 2000): 4626–28; Reuven Cohen et al., "Breakdown of the Internet under Intentional Attack," *Physical Review Letters* 86, no. 16 (April 16, 2001): 3682–85.
[50] Nye, *The Future of Power*, 123.

infrastructures that enable communications, such as undersea fiber optic cables and communications satellites, and major interconnection points for large global networks."[51] However, the analogy to sea power is flawed. These key bits of infrastructure, given their relatively small number, are chokepoints but cannot be controlled in the same way a fleet controls a narrow strait. Undersea cables cannot be the subjects of a blockade, and while satellites and key nodes can be controlled or destroyed, the issue of interdependence is difficult to circumvent. While technically feasible, it appears difficult to limit the effects of a chokepoint operation to a given geographical area. Cyberspace is not divided into regions; its parts are interwoven across borders and not easily disentangled.[52] An actor could decide to destroy a chokepoint, but the internal costs would likely be substantial. Shutting off the Internet in one target country would likely mean affecting Internet access in neighboring countries, perhaps even including the attacking country. This high level of interdependence makes any strike on the key parts of the physical layer of the Internet risky.

Another implication of cyberspace's networked nature is that attacks can have cascading effects. The spread of complex malware, such as Flame and Duqu, suggests that these cyber tools are not accurate or easily contained.[53] While this can be inferred to be based on flaws in the programming of the malware, it is not inconceivable that the nature of cyberspace and modern computing is so complex that unintended consequences are inevitable. The lack of predictability might be the best explanation as to why there have been so few CNAs like Stuxnet and no attacks on physical ICT infrastructure. The uncertainty is not limited to cyberspace either. Before the 2003 invasion of Iraq, the U.S. military debated launching CNOs against the Iraqi banking system. Causing an economic crisis and panic could soften the battlefield, but the United States eventually decided against the idea due to fears that the effects could spread throughout the region and even to Europe.[54] Similarly, the spread of Stuxnet and other malware has led to concerns over cyber proliferation, with some noting that cyber weapons used by the United States can potentially be adopted and used against the United States.[55] The problem of proliferation can be further exacerbated by the development of malware kits, possibly with a

---

[51] Rattray, "An Environmental Approach to Understanding Cyberpower," 268.

[52] States can, however, choose to isolate themselves, as the Egyptian government did in early 2011. Internet Service Providers (ISP) were forced to withdraw information for the border gateway protocol (BGP), a core routing protocol for the Internet, which basically meant no networks outside Egypt could find the route to Egyptian servers. See: Gregg Keizer, "How Egypt Pulled Its Internet Plug," Computerworld, January 28, 2011, http://www.computerworld.com/s/article/9207040/How_Egypt_pulled_its_Internet_plug.

[53] Cyber weapons are not inherently indiscriminate, but they require a high level of technical expertise and knowledge about the target to be discriminating. See: Steven M. Bellovin, Susan Landau, and Herbert S. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity* 3, no. 1 (2017): 59–68.

[54] Eric Schmitt and Thom Shanker, *Counterstrike: The Untold Story of America's Secret Campaign against Al Qaeda* (New York: Times Books, 2011), 132.

[55] Jason Healey, "Stuxnets Are Not in the US National Interest: An Arsonist Calling for Better Fire Codes," New Atlanticist, June 1, 2012, http://www.acus.org/new_atlanticist/stuxnets-are-not-us-national-interest-arsonist-calling-better-fire-codes.

modular design, that automate CNE. The U.S. military is developing such capabilities with the aim of further integrating cyber components into military operations.[56]

Whatever uncertainty may arise from specific pieces of programming, the networked nature of cyberspace suggests an inherently interdependent environment where actions are neither easily contained nor predicted. As such, the networked nature of cyberspace means it is difficult to achieve precise, contained attacks, but it also means that there are inherent challenges to obtaining comprehensive situational awareness of the system. In the same way it requires effort to ensure that a cyber attack fulfills its intended purpose, it is also, to an even larger degree, difficult to defend a system that is non-hierarchical. Without the cyber equivalent of a high ground, actors are reliant on intimate knowledge of their own networks as well as intelligence, surveillance and reconnaissance (ISR) capabilities in other networks.

If we consider the networked nature of cyberspace in conjunction with the previous defining characteristics, we get a sense of the challenges facing states when exerting cyber power. Malleability implies an ever-changing landscape, since the networks keep changing and growing, which means that actors require a certain level of resources to both defend and attack. In other words, there are more potential targets available, but also more assets to secure. If we couple this fact with the collapse of time and space as implied by cyberspace's virtual nature, then we have a high degree of complexity requiring both precision and quick responses.

As discussed above, cyberspace's virtual nature also implies that it cannot be conquered or occupied in any meaningful way, thus lessening the utility of traditional military strategy. However, its networked nature opens up attack vectors to other processes and structures that are not primarily ICT functions. Though CNOs cannot conquer a network, they can use it to 'jump' into other facilities. This gap is usually a significant hurdle to clear, but the possibility of generating kinetic effects is still there and dependent on the processes related to malleability. If we compare military air campaigns to cyber operations, it is quite clear that air strikes, given sufficient capabilities, can reach more targets than a cyber attack, but do not offer cascade effects. The appeal of cyber attacks is that the high degree of networked interdependence, coupled with the connection between virtual and physical processes, can trigger cascade effects that are harder to predict and prevent.

Taken together, these characteristics imply that both cyber defense and offense are demanding tasks for actors. There are more targets and more vectors of attack, but the effects might be unpredictable or even counterproductive. Since offense and defense are two sides of the same coin in cyberspace, the same challenges hold for defending against attacks and intrusions. This is important to keep in mind for the next subsection, which deals with the significant democratization of ICT over the past two decades or so.

[56] Ellen Nakashima, "With Plan X, Pentagon Seeks to Spread U.S. Military Might to Cyberspace," Washington Post, May 30, 2012, http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_print.html.

Software and Power Diffusion

The explosive growth in computing power has not just collapsed speed and distance; these technological advances, coupled with economies of scale, have made computing power cheaper. This, in turn, has made personal computers practically ubiquitous, at least in the developed world, enabling access to computing power that just a few decades ago was reserved for governments and corporations. Something similar has happened in terms of speed of communication. Nye argues that, "[t]he key characteristic of this Information Revolution is not the *speed* of communications between the wealthy and powerful: for more than 130 years, instantaneous communication by telegraph has been possible between Europe and North America. The crucial change is the enormous reduction in the cost of transmitting information."[57] This characteristic of cyberspace is the one that most closely, and most visibly, bridges technology and society. Therefore, this discussion focuses more on the utilization of technology than it does on conceptual analysis of cyberspace.

While there have been enormous technological breakthroughs, as discussed earlier, the societal impact would likely not have been possible without the economy-of-scale effect that ensured diffusion of personal computing technology. This is what Nye refers to when he talks about power diffusion in cyberspace, and it is often characterized by cyber security scholars as enabling a relatively low barrier to entry for state and non-state actors. In short, this means that obtaining power in cyberspace is comparably cheaper than in traditional domains, such as air and sea. It is much cheaper to design malware and launch CNOs than acquire physical assets like fighter jets and destroyers that come with substantial costs and require access to highly advanced technology. The security implication of this has been portrayed as that of making rogue nations, or even individuals, capable of waging cyberwar with very low costs, but this is incorrect and misses the genuine character and limitations of the technological diffusion.[58]

The diffusion of personal computer technology, enabled by reduced cost and technological advances, has turned cyberspace into a more software-centric environment. In other words, whereas purchasing hardware constituted a significant threshold for entry into cyberspace before, that threshold is now significantly lower. Developing malware is mostly an

[57] Nye, *The Future of Power*, 115.

[58] The myth of individual hackers launching large-scale, complex cyber attacks is primarily the product of popular culture, seen in movies such as *Sneakers* (1992), *Live Free or Die Hard* (2007) and *Skyfall* (2012). However, the U.S. government has warned that the barrier to entry is lower in cyberspace, allowing more states and even non-state actors to conduct advances cyber attacks. See: U.S. Department of Homeland Security, "The National Strategy to Secure Cyberspace," February 2003; U.S. Department of Defense, "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense," January 2012; Keith B. Alexander (Commander of United States Cyber Command), "Oversight: U.S. Strategic Command and U.S. Cyber Command," § Senate Committee on Armed Services (2013). For examples of scholarly work that discusses the lower barrier to entry, see Dorothy E. Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?," *IO Journal* 1, no. 1 (2009); Lawson, "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History"; Diego Rafael Canabarro and Thiago Borne, "Reflections on The Fog of (Cyber)War," NCDG Policy Working Paper (Amherst, Massachusetts, March 1, 2013).

issue of finding vulnerabilities and programming effective exploits—which can be done with regular laptops. There are three caveats to this observation. First, while expensive hardware might not be necessary to perform most tasks, the need for brain power (i.e., human capital) is so central to CNO that it constitutes a significant requirement for cyber power—a requirement that is based on a limited resource. Recruiting competent individuals is a problem for both the public and private sector, because increase in demand is outstripping the supply of IT professionals in general, and cyber security experts specifically.[59] Moreover, there are a limited number of individuals who can do the sophisticated kind of programming necessary for malware such as Stuxnet or Flame.[60] Second, hardware is not irrelevant, as some CNOs necessitate access to significant computing power to perform complex tasks.[61] Nye mentions several technological trends that favor powerful states. "Space-based sensors, direct broadcasting, high-speed computers, and complex software provide the ability to gather, sort, process, transfer, and disseminate information about complex events that occur over wide geographic areas. This networking of military systems produces a powerful advantage (as well as a potential vulnerability)."[62] Third, some CNOs require assets outside cyberspace, such as intelligence, to target or gain access to certain networks. As mentioned earlier, the Stuxnet operation was made possible by jumping the air gap. This can be done with an agent or by planting malware on equipment used by an unknowing insider. Furthermore, the development of Stuxnet necessitated access to the physical infrastructure used at Natanz, specifically the centrifuges, to test out and

[59] Anecdotal evidence and surveys suggest not enough people are being trained as cyber security to meet market demand. The U.S. Bureau of Labor Statistics predict a significant increase in IT jobs, including security-related positions this decade. See Jaikumar Vijayan, "Demand for IT Security Experts Outstrips Supply," Computerworld, March 7, 2013, http://www.computerworld.com/s/article/9237394/Demand_for_IT_security_experts_outstrips_supply; Sandrine Rastello and Jeanna Smialek, "Cybersecurity Starts in High School with Tomorrow's Hires," Bloomberg, May 16, 2013, http://www.bloomberg.com/news/2013-05-16/cybersecurity-starts-in-high-school-with-tomorrow-s-hires.html; Bureau of Labor Statistics, U.S. Department of Labor, "Network and Computer Systems Administrators," in *Occupational Outlook Handbook*, 2012th-2013 Edition ed., accessed May 23, 2013, http://www.bls.gov/ooh/Computer-and-Information-Technology/Network-and-computer-systems-administrators.htm; Bureau of Labor Statistics, U.S. Department of Labor, "Information Security Analysts, Web Developers, and Computer Network Architects," in *Occupational Outlook Handbook*, 2012th-13 Edition ed., accessed May 23, 2013, http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts-web-developers-and-computer-network-architects.htm.

[60] Some have argued that Stuxnet's sophistication has been exaggerated, and actually relies on off-the-shelf code and possibly outsourcing. This was done in order to save money and obscure the origins of the malware. See: James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (2011): 23–40.

[61] According to one estimate, the spread of the malware known as Flame needed as much as $200,000 worth of computing time. While not a tremendous amount of money for organizations, it shows that some cryptographic operations require more than individual computers. See Dan Goodin, "Flame's Crypto Attack May Have Needed $200,000 Worth of Compute Power," Ars Technica, June 12, 2012, http://arstechnica.com/security/2012/06/flame-crypto-attack-may-have-needed-massive-compute-power/.

[62] Nye, *The Future of Power*, 118.

properly calibrate the malware.[63] If Stuxnet is indicative of the resources necessary for such complex operations, then cyberspace should favor stronger actors who have extensive resources and intelligence capabilities.[64]

All three caveats impose limitations on which actors can do what. The lack of human capital is a supply problem that affects states' potential abilities to conduct large and complex operations. For states, overcoming this problem requires investing in education, as they cannot simply poach talent from other states, and this is a long process. While the supply issue does not appear to significantly hamper states at the present time, it is not unrealistic to assume that the demand will increase as cyber operations gain more relevance in military operations. Foreseeing this issue, many states, including potentially hostile actors, are investing heavily in education and in the training of cyber security experts.[65] The necessity for hardware in some operations is unlikely to prove an obstacle to most states, but it is a caveat on Nye's "diffusion of power" concept, as non-state actors might find it difficult to acquire or gain access to significant ICT infrastructure. Intelligence and other resources outside cyberspace also favor states, and especially states with significant intelligence and covert operations capabilities. In sum, the barrier to entry in cyberspace is lower relative to other domains, but the requirements for certain resources still favor states when it comes to complex operations.

A second security implication of the software-centric nature of cyberspace is the ease with which malware and methods of exploitation can spread. Similarly to the diffusion of hardware technology, the proliferation of software means a leveling of the playing field. The distinction between the two phenomena is that malware proliferation has more direct and specific effects. Whereas hardware diffusion is a long-term process that affects the power balance, malware proliferation in most cases means the spread of a specific tool designed for a specific, and often limited, purpose. The spread of such tools therefore has little strategic impact, because once an exploit has been used, the vulnerability can be detected and fixed.[66] The more serious security implication of proliferation occurs when these tools are reengineered for broader or different purposes. Such is the fear with Stuxnet, as parts or translations of its source code have been made public on the Internet, which can then be redesigned for other targets.[67] The U.S.

---

[63] William J. Broad, John Markoff, and David E. Sanger, "Stuxnet Worm Used Against Iran Was Tested in Israel," New York Times, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

[64] Lindsay, "Stuxnet and the Limits of Cyberwarfare."

[65] Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage" (Washington, D.C.: Northrop Grumman Corp, March 7, 2012); Tony Capaccio, "North Korea Improves Cyber Warfare Capacity, U.S. Says - Businessweek," Bloomberg Businessweek, October 22, 2012, http://www.businessweek.com/news/2012-10-22/north-korea-improves-cyber-warfare-capacity-u-dot-s-dot-says.

[66] There are exceptions to this rule. Some well-known vulnerabilities such as buffer overflows are still an issue, years after first being discovered.

[67] Joel Langill, "Want the Source Code to Stuxnet? Come and Get It," Infosec Island, October 21, 2011, http://infosecisland.com/blogview/17613-Want-the-Source-Code-to-Stuxnet-Come-and-Get-It.html.

Department of Homeland Security said in a congressional testimony in 2011 that "attackers could use the increasingly public information about [Stuxnet] to develop variants targeted at broader installations of programmable equipment in control systems."[68]

Given these developments, the diffusion of technology in relation to cyber security has several security implications. It can potentially affect the power balance between states, enable greater participation by non-state actors and make it easier for belligerent actors to launch attacks on other actors. However, the caveats discussed earlier indicate that states, and particularly powerful states, are still favored in cyberspace.[69] While smaller states can repurpose part of the Stuxnet code to launch attacks against U.S. critical national infrastructure, they will probably lack the intelligence capacity to launch accurate attacks and the human resources needed to sustain a prolonged campaign.[70] These are significant hurdles and would suggest that after a certain point (somewhere after DDoS attacks and simple CNE), the complexity of an operation or campaign is proportional to a state's traditional power. However, this proposition needs to be further tested as there is currently insufficient data on state cyber warfare.

The diffusion of software and hardware may not rebalance compulsory cyber power, but it should affect other forms of cyber power. If the networked nature of cyberspace enables the dissemination of power, the diffusion of technology enables the production of ideas. However, if productive cyber power is the result of malleability, networks, and technology diffusion, state actors do not easily control it. It is reasonable to assume that governments might affect the adoption of ICT in various sectors through legislation and regulation, and it can also work to influence standards and governing institutions, but the chief driver of innovation is the private sector. We can therefore argue that the public sector has primarily, but not exclusively, negative power, whereas the private sector has positive, or productive, power. In other words, the defining characteristics of cyberspace might favor productive power, but while states can exploit this, they do not control the processes of diffusion and networking that enable such power. This is a simplification of highly complex market and governance processes, but it is nonetheless useful to distinguish between not just different forms of cyber power, but also the various types of actors involved. In the next section we will discuss further the implication of defining characteristics on cyber power in part to illustrate what states can expect to influence and what it can merely exploit. This should tell us how compulsory cyber power can be achieved and how it related to particularly structural cyber power.

Behavior in an ecological system

[68] Roberta Stempfley and Sean P. McGurk, "Statement for the Record," § Committee on Energy and Commerce, Subcommittee on Oversight and Investigations (2011).

[69] Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?"; Rid and McBurney, "Cyber-Weapons."

[70] Loch K. Johnson has argued that national wealth is the key factor in enabling effective collection and analysis of intelligence. See Loch K. Johnson, "Bricks and Mortar for a Theory of Intelligence," *Comparative Strategy* 22, no. 1 (2003): 1–28.

The ecological framework suggests a picture of conflict that closely resembles what has actually transpired in the past decade. We have seen very few examples of outright attacks, particularly against critical infrastructure, and most malicious activities are either espionage or reconnaissance. These features of cyber conflict today conform closely to the theoretical implications of cyberspace's defining characteristics. The primary characteristic, affecting all the others, is malleability. In terms of security implications, it means there is a wide and increasing range of targets to attack, so a state would pursue new or unknown vulnerabilities to surprise its opponent. We have already seen some examples of simplistic CNAs, such as North Korean DDoS attacks on South Korea and Russia's alleged DDoS attacks on Estonian and Georgian websites in 2007 and 2008, respectively.[71] These are relatively crude operations aimed at disrupting communications, and as such the threshold for conducting them might be relatively low.

More advanced operations are more likely to manifest themselves in attacks on critical national infrastructure, such as power grids, stock exchanges and telecommunications infrastructure. This is where we see the virtual nature of cyberspace become significant, as actors attempt to leap from networks to physical processes. While DDoS attacks merely floods servers with requests to suspend ICT service, these operations involve infiltrating networks and creating major disruption and possibly degradation or destruction outside cyberspace. Stuxnet showed that critical infrastructure attacks are possible, and there have been other, examples of attacks or so-called proofs of concepts of attacks on critical national infrastructure.[72] For instance, hackers took down a significant part of the Ukrainian power grid in 2015. The attack was sophisticated; it skirted security measures that are unusual for many infrastructure systems, but the hacking was also coordinated with a Denial-of-Service attack against customer call centers to prevent people from reporting the outage.[73] The details of these incidents reveal the challenges of implementing such operations. We might then expect them to be rare, but the experimental use of CNI probings and attacks also suggest that actors are actively developing such attack vectors.

The networked nature of cyberspace, in conjunction with its malleability, means that there is significant difficulty in attributing actions to actors. This would suggest a low threshold for malicious activity, but we must also consider other characteristics to get a more complete picture of behavior in cyberspace. For instance, the uncertain accuracy and effects of attacks, not to mention the single-shot nature of most tools, means it is more likely that states would be

---

[71] "Ten Days of Rain: Expert Analysis of Distributed Denial-of-Service Attacks Targeting" (Santa Clara, California: McAfee, July 2011), https://secure.mcafee.com/us/resources/white-papers/wp-10-days-of-rain.pdf.

[72] Chloe Albanesius, "Illinois Water Utility Pump Destroyed After Hack," PC Magazine, November 18, 2011, http://www.pcmag.com/article2/0,2817,2396632,00.asp; Dan Goodin, "Second Water Utility Reportedly Hit by Hack Attack," The Register, November 18, 2011, http://www.theregister.co.uk/2011/11/18/second_water_utility_hack/print.html.

[73] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; Andy Greenberg, "How An Entire Nation Became Russia's Test Lab for Cyberwar," *Wired*, June 20, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/.

hesitant about launching attacks. Therefore, assessing the threshold for malicious activity is probably more complex and dependent on the types of operations and targets. Given the risks of retaliation and escalation, my framework suggests that states would be more inclined to use their cyber resources on espionage, at least in peacetime. Whereas attacks are dependent on achieving relatively swift and precise effects, espionage operations can be done piecemeal and adjusted over time.

Regarding how the collapse of space and time affects offensive behavior, it would be reasonable to expect that states would utilize cyber attacks to achieve a form of first-move advantage. Given the single-shot nature of cyber weapons, however, states could be hesitant about using their tools and exposing their capabilities. We have seen examples of both. During both the Estonian-Russian conflict in 2007 and the Georgian-Russian war in 2008, the Russian government or its agents allegedly launched DDoS attacks to paralyze communications in the target countries. In the case of the former, Russia appears to have used the attacks to coerce the Estonian government into reversing its decision regarding the Bronze Soldier of Tallinn statue.[74] The cyber attacks on Georgia were part of a military campaign, attempting to disrupt communications, albeit in limited ways, during fighting.[75] However, the operational value of the attacks was quite small as Georgian authorities were able to reroute traffic and move servers abroad, illustrating both the resilience of the networked space and the inefficiency of blunt tools such as DDoS.

The software-centric nature of cyberspace suggests a leveling of the playing field, but as we see in the examples discussed here, and supported by the framework, practically all of the notable cyber incidents have been perpetrated by powerful, or at least very capable, states. There also appears to be a significant power disparity between the attacker and defender, though we would need more data before concluding on this. Nonetheless, it seems that on diffusion of technology the effect is asymmetrical, with smaller states becoming relatively more powerful in some areas, while powerful states maintain their advantage in other areas (i.e. complex CNO). While it is possible that less powerful states can build up sufficient capabilities to launch sophisticated cyber attacks, it is unlikely that this would affect a broader power balance between those states and great powers. Diffusion of technology may enable more states to conduct CNOs, but more powerful states would still have superior kinetic capabilities. Therefore, there would have to be a significant increase in cyber power for smaller states to successfully use cyber capabilities as a credible deterrent. Given the findings presented here, powerful states still hold the advantage, despite the information revolution.

The above discussion conforms to a large extent with what we see in cyber security today. While states worry about the potential threat against CNI, there have been few examples

---

[74] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," Guardian, May 17, 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

[75] Independent International Fact-Finding Mission on the Conflict in Georgia, "Report: Volume II" (Brussels: Independent International Fact-Finding Mission on the Conflict in Georgia, September 2009), http://www.ceiig.ch/pdf/IIFFMCG_Volume_II.pdf.

of cyber conflict, and those we have seen have been primarily regional.[76] What little attacks have happened in war or intense conflict have either been of entirely auxiliary nature (Estonia, Georgia), harassment (Korea) or sabotage as part of a covert operation (Stuxnet). In fact, some of the most telling examples of cyber conflict have been those that did not happen. The decision not to attack the Iraqi bank system in 2003 illustrates how hard it might be to contain the effects of attacks, while the decision not to use cyber warfare in Libya reveals a hesitance on the part of the United States to show its hand.[77]

Cyber security today, on a state level, is mostly about espionage. As a list compiled by the Center for Strategic and International Studies of all major cyber incidents since 2006 shows that the vast majority of incidents are CNE operations.[78] The targets range from governments to corporations, with some operations including a mixture of both. The information gathered may vary greatly, but they mostly appear to be of strategic purpose, as would be expected during peacetime, and not for immediate operational utility. These campaigns have gathered information about state secrets and military technology (Byzantine Hades), corporate secrets, or both (Operation Shady RAT).[79] Information about dissidents has also been a part of at least one campaign, Operation Aurora.[80] Other campaigns appear to be part of reconnaissance operations, for instance Duqu and Flame. Both malwares appear to be designed for gathering information in the Middle East. Duqu, the oldest of the two, arguably shares similarities with Stuxnet, and thus might have related purposes in regards to the Iranian nuclear program.[81] According to some

[76] Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11."
[77] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare Against Libya," New York Times, October 17, 2011, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=2.
[78] James A. Lewis, "Significant Cyber Incidents Since 2006" (Center for Strategic and International Studies, April 2018), https://csis-prod.s3.amazonaws.com/s3fs-public/180425_Significant_Cyber_Events_List.pdf?pqetcWcwV7mvAo33_lAZFlQVQz7.E0qh.
[79] Brian Grow and Mark Hosenball, "Special Report: In Cyberspy vs. Cyberspy, China Has the Edge," Reuters, April 14, 2011, http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414; Dmitri Alperovitch, "Revealed: Operation Shady RAT" (Santa Clara, California: McAfee, August 3, 2011); Eugene Kaspersky, "Shady RAT: Shoddy RAT.," Nota Bene, August 18, 2011, http://eugene.kaspersky.com/2011/08/18/shady-rat-shoddy-rat/.
[80] George Kurtz, "Operation 'Aurora' Hit Google, Others by George Kurtz," CTO, January 14, 2010, http://blogs.mcafee.com/corporate/cto/operation-aurora-hit-google-others; David Drummond, "A New Approach to China," Google Official Blog, January 13, 2010, http://googleblog.blogspot.no/2010/01/new-approach-to-china.html.
[81] Boldizsár Bencsáth et al., "Duqu: A Stuxnet-like Malware Found in the Wild" (Budapest: Laboratory of Cryptography and System Security at Budapest University of Technology and Economics, October 14, 2011); SecureWorks Counter Threat Unit Research Team, "Duqu Trojan Questions and Answers," Dell SecureWorks, October 26, 2011, http://www.secureworks.com/research/threats/duqu/; "Iran Says It Has Detected Duqu Computer Virus," Reuters, November 13, 2011, http://www.msnbc.msn.com/id/45278589#.Ts6rqUohMXh.

reports, Flame, discovered in 2012, is also aimed at Iran, designed to gather information in preparation for cyber sabotage.[82]

It should be noted that behavior during war, or intensified conflict, could be different. While there is not sufficient data to make proper predictions, the ecological framework suggest that some behavior is more likely than others during open conflict. Signaling would be a significant motivation for launching attacks during a declared conflict, making the possibility of plausible deniability largely irrelevant. Operations like Stuxnet and Duqu are likely to be part of operations during or leading up to conflict, given their operational value, while campaigns such as Byzantine Hades and Operation Shady Rat have more long-term, and possibly economic, aims. We might therefore see, despite the reservations discussed above, that attacks could transpire rather quickly. Given the lower threshold for espionage, actors are likely to build up knowledge of opponents' networks during peacetime, with the expectation that once conflict breaks out, they have a form of turnkey capability to affect CNI and other capabilities. However, the high degree of complexity combined with efforts of deception on part of the belligerents means that any conflict in cyberspace could become rather unpredictable and contingent on the actors being able to adjust course and pivot to new targets.[83] As such, there might be significant divergence between expectations and reality, but that is beyond the scope of this paper.

IMPLICATIONS

The findings presented here suggest that states have limited coercive power in cyberspace. These limitations can, however, change, and we must examine not just the defining characteristics, but also how they relate to cyber power writ large. While this article cannot account for all iterations of relationships between the characteristics and the various forms of cyber powers, we can examine one specific example. Structural cyber power is best understood as the relationship actors and the structure of cyberspace (contrary to Betz and Stevens' conceptualization, this paper focuses on how the former affects the latter). Put in simple terms, we can argue that changing the structure can affect the potential for compulsory cyber power, but whether states pursue conflict or cooperation depend on domestic and international politics and cyberspace itself.

Structural cyber power is complex as it depends on several, if not all, of the defining characteristics of cyberspace. Malleability, both in its vertical and horizontal form, determines the use of ICT. New uses of ICT (horizontal malleability) mean new vulnerabilities, and changes in protocols or standards (vertical malleability) can either strengthen or weaken security. The former is primarily driven by market dynamics, while the latter is a mix of government regulation and Internet governance—which states can influence through their institutional cyber

[82] Ellen Nakashima, Greg Miller, and Julie Tate, "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," Washington Post, June 19, 2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_print.html.

[83] Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48.

power. As such, a state's ability to affect the structure of cyberspace depends on other actors, and in particular on private actors.

The role of the private sector requires further elaboration. State actors are not the only ones influencing the defining characteristics supporting coercion. Malleability and diffusion are the product of interaction between governmental action and market dynamics. Many changes in cyberspace are primarily driven non-state actors, and besides military research and development, innovations in hardware and software reach the open market through private companies. This is also where vulnerabilities appear, for instance in operating systems that run the gamut through private, corporate and industrial systems. Governments can regulate and set requirements through outsourcing, but they are not necessarily the primary source of innovation. Related to this, the diffusion of technology is driven in large part by the private sector, so adoption of new technologies takes place through the marketplace. We can therefore say that the malleable and software-centric characteristics are not something states can affect directly, or at least only to a limited extent, but the increased use of ICT by government agencies mean they do affect the extent of their vulnerabilities.

A state's ability to wield structural power thus depends on its own capacities and that of others. We should expect larger states with a thriving private sector to have more structural power, as it can both set standards and affect demand. However, power can be wielded in different ways, and states might choose to purse either cooperation or conflict, which depends on domestic politics.

Domestic obstacles to cooperation

While government cyber policies and strategies fall on a spectrum, we can distinguish between two extremes. States can regulate security requirements and create mechanisms to encourage certain behaviors, such as information sharing and cross-sectoral cooperation, in order to improve cyber security. As such, they can be the producers of a public good. Or, states can undermine the robustness of cyberspace by maintaining or encouraging weaker security standards in order to seek competitive advantages. This can be done with the aim of increasing a state's compulsory cyber power. The two behaviors may seem in conflict, and they most likely are, but that does not mean states do not actively pursue both avenues of cyber policy. States can seek to shore up its critical national infrastructure, while at the same time developing capabilities designed to exploit others' vulnerabilities. Taken to its logical extreme, states can seek to undermine the security of cyberspace itself by ensuring that the structure remains inherently vulnerable, if not actively working to degrade cyberspace's robustness. While this may increase their compulsory cyber power, it may have problematic effects down the line as it decreases the general solidity of cyberspace.

Developments in cyber policy over the past few years suggest that some states pursue both policy tracks, in some form or another. The case of U.S. cyber policy is instructive in this discussion. While too much of the cyber security literature has relied on Stuxnet to explain most things, it is useful in this context to illustrate how within a state there can be multiple efforts working against each other. Stuxnet, or Operation Olympic Games as it was part of, was

ostensibly a covert operation conducted by the United States and Israel to sabotage the Iranian nuclear program. However, its use also undermined efforts elsewhere in the U.S. government. The Department of Homeland Security (DHS) is tasked with coordinating civilian cyber security, but the potential proliferation of such malware, not to mention the precedent set in using them against CNI, runs the risk of digital blowback affecting the very institutions and sectors DHS is trying to help secure.

A less obvious, but possible more damaging, example of this policy contradiction is the case of the serious Internet vulnerability known as Heartbleed. The bug exposed secure communication protocols for years, and millions of users were affected. The U.S. National Security Agency is alleged to have known about the vulnerability for quite some time. Though the allegations have not been corroborated, and the NSA deny them, Heartbleed illustrates the dilemma a state can face when choosing between maintaining specific capabilities and preventing potential exploitation. The state can choose to strengthen the structure of the Internet, or it can passively or actively maintain its vulnerabilities. The economic costs of the latter can be substantial because of direct losses through fraud and opportunity costs in lost productivity.[84]

We can think of this dilemma as a form of domestic cooperation problem, as different parts of the government have different missions. DHS might be concerned with protecting the domestic economy, while the NSA is primarily concerned with foreign threats (though it does have a separate information assurance mission, making even their own purpose at times contradictory).

International conflict and cooperation

Domestic obstacles are not the only ones preventing cooperation and encouraging conflict. Any given state might find it worthwhile to devote its resources to building more robust standards and cyber defenses. However, the effort is likely to be futile without the cooperation of many other states. One way of thinking about cooperation on cyber security is to think in terms of international regimes and treaties. Enhancing security depends in part on improving software standards and protocols. However, a standard is not a standard unless adopted by a sufficient number of actors. Cyber security is particularly difficult for achieving cooperation because it involves a complex set of issues and multitude of actors, both public and private. Existing research on climate change shows that these factors can prevent international agreement.[85]

Beyond cooperation and coordination, states also face commitment problems in cyberspace. Existing theories of international conflict argue that if other actors can renege on

[84] Jim Finkle, "Big Tech Companies Offer Millions after Heartbleed Crisis," Reuters, April 24, 2014, http://www.reuters.com/article/2014/04/24/us-cybercrime-heartbleed-idUSBREA3N13E20140424; Brian Fung, "Heartbleed Is about to Get Worse, and It Will Slow the Internet to a Crawl," Washington Post, April 14, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/14/heartbleed-is-about-to-get-worse-and-it-will-slow-the-internet-to-a-crawl/.

[85] Robert O. Keohane and David G. Victor, "The Regime Complex for Climate Change," *Perspectives on Politics* 9, no. 01 (2011): 7–23.

agreements, it becomes harder for states to reach peaceful agreements and avoid conflict.[86] Furthermore, if states cannot observe malicious actions, such as interventions, conflicts can escalate.[87] The defining characteristics of cyberspace exacerbate these concerns in several ways, which in turn encourage states to use structural power to achieve coercive power.

First, its malleability means that actors can affect the system, thus affecting other actors. If offense and defense are two sides of the same coin, being able to design new malware means increasing ones' offensive capabilities at the expense of another's defensive capabilities. In a bilateral setting in the absence of external enforcement, these dynamics can then introduce a commitment problem because neither state can credibly promise not to develop offensive cyber capabilities.

In this regard, the notion of an offense-defense balance is both critical to understanding cyber power, but also problematic because it works differently here compared to how it is used in the existing international relations literature. With traditional military conflict, the balance is defined by "the ratio of the cost of the forces that the attacker requires to take territory to the cost of the defender's forces."[88] This implies that states can compensate for a strong offense by investing in defense, because the two are distinct processes. However, in cyberspace, the two sides are the same, which changes how offense and defense relate. Imagine that instead of your opponent building a rocket to fire at your defenses, he builds a rocket that fits the rocket-sized hole in your wall.

Another issue with directly adopting the offense-defense balance for discussing cyber power is the concept of dual-use technology. Kinetic or physical technologies can be used for both defensive and offensive purposes, and sometimes the distinction is quite blurry.[89] A cyber weapon cannot be used for cyber defense, and vice-versa.

If we were to adopt Biddle's conceptualization of the offense-defense balance, the application becomes harder still.[90] He argues that force employment is also significant for assessing the balance, but cyberspace's malleability means that the actors can change the structure. Compulsory power in cyberspace therefore stands apart from traditional land power, in the sense that actors can change the environment, or system, to achieve tactical or operational advantages.[91]

---

[86] James D. Fearon, "Rationalist Explanations for War," *International Organization* 49 (1995): 379–379.
[87] Kenneth A. Schultz, "The Enforcement Problem in Coercive Bargaining: Interstate Conflict over Rebel Support in Civil Wars," *International Organization* 64, no. 02 (2010): 281–312.
[88] Charles L. Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?," *International Security* 22, no. 4 (Spring 1998): 46.
[89] Kier A. Lieber, *War and the Engineers : The Primacy of Politics over Technology* (Ithaca: Cornell University Press, 2005).
[90] Stephen Biddle, "Rebuilding the Foundations of Offense-Defense Theory," *The Journal of Politics* 63, no. 3 (2001): 741–74.
[91] Stephen D. Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton University Press, 2004).

Instead, we can think of the offense-defense balance in cyberspace as a mechanism encouraging defection from cooperation. If vulnerabilities are plenty, then offensive opportunities increase. States may then become increasingly tempted to invest in offensive capabilities, rather than try to coordinate defensive policies, such as information sharing across borders.

Second, cyberspace's virtual and networked nature means that states cannot directly observe if other states are cooperating or shirking. The monitoring problem of international relations is thus particularly acute in this area. A state might claim it is working towards strengthening Internet security, but secretly developing tools and strategies to attack others. It might not share information about vulnerabilities, and others would have no way of knowing that information was being withheld. This issue is exacerbated by the attribution problem in cyberspace. States cannot necessarily observe other actors investing in offensive capabilities, and it might also not be able to hold an actor responsible if it were to use those capabilities.

Cyberspace therefore creates an inherent problem of asymmetric information. This unobservability can prevent states from reaching agreements, such as treaties on the offensive use of cyber weapons, and it also encourages investment in the offense. An otherwise benign state might choose to purse conflict because it cannot trust that others will abide by agreements, and it cannot trust that others will not exploit vulnerabilities it might not even know exists.

Opportunities

The implications articulated above suggest a future of sustained, low-level conflict. However, it does not necessarily follow that the Internet is doomed. The cost of escalating cyber conflict might become too high and prompt cooperation. For instance, an increased offensive advantage could make the cost of an insecure Internet prohibitively high, incentivizing cooperation. A death spiral of cyber attacks and exploitations could have a significant negative impact on the economy, prompting a change in government policy towards more information sharing and international regimes.

Furthermore, the domestic politics of cyberspace could be instrumental in developing future policies. While this paper has not discussed this dimension at length, a wide range of industries relies on the Internet either directly or indirectly. These companies are stakeholders in domestic politics and they might demand government action. Some of them are also providers of cyber power. Technology giants such as Google provide services to governments, while also having a significant effect on socioecological system. They are therefore not only passive objects to be protected, but actors with agency. We might therefore be wise to integrate the private sector into our theories of cyber power and cyber conflict.

CONCLUSION AND FUTURE RESEARCH

The ecological approach to cyber power helps to understand current and future behavior in cyberspace because it accounts for the relationship between cyberspace itself and powers actors

can derive from it. It can also explain how cyber conflict might change in the future, but more research is required. The implications the information revolution has had and will continue to have on international security remain largely unexplored. One important question is whether the development of more sophisticated cyber weapons and continued societal vulnerability related to cyberspace will increase the risk of international conflict.[92] This is not to say that cyberspace will create conflict, but proliferation and digital arms races can trigger escalation in diplomatic conflicts or cause security dilemmas.

Related to this is the question of posture and policy-formulation. This paper has not directly addressed the issue of actors' threat perception, but an informal reading of many states' strategies in cyberspace suggests that there is a disconnect between what the model presented here suggests about cyber conflict and what states are preparing for in cyberspace. This gap can be explained by a flawed understanding of cyberspace as a strategic ecological system, or it can be the result of threat inflation. Constructivists and securitization scholars have done some work already on the formulation of cyber policy and threat inflation.[93] Examining how states perceive threats in and through cyberspace can inform our understanding of cyber security, but it also offers direct policy relevance. Like with warnings of a "cyber Pearl Harbor," too much of the discourse on cyber security is rooted in science fiction rather than fact.

Future research should focus on the collective action problems promoting escalation in cyberspace. While the system might be ill suited for large-scale coercive attacks, the continued focus on such conflict risks undermining the system because the actors can to a certain extent change the structure itself. This can lead to efforts to secure the Internet through fragmentation and stronger governmental control, but it can also lead to digital arms races where the actors purposefully undermine the existing security layers. If the latter scenario takes place, we might see a convergence of perception and reality, but to the detriment of the Internet as a source and avenue of economic growth. Erosion of trust in the Internet might also damage it as an avenue for information and stifle democratic discourse. These potential political implications should be further explored, and hopefully the analytical framework presented in this paper can lay the foundation for such analyses.

Bibliography

[92] There is a large body of literature on the relationship between conflict and technology, particularly with the discussion on the offense-defense balance. See: Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167–214; Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security* 22, no. 4 (Spring 1998): 5–43; Van Evera, *Causes of War: Power and the Roots of Conflict*; Glaser and Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" For criticism of offense-defense theory, see Lieber, *War and the Engineers : The Primacy of Politics over Technology*. For a response to Lieber's work, see Jack Snyder, "Correspondence: Defensive Realism and the 'New' History of World War I," *International Security* 33, no. 1 (Summer 2008): 174–94.

[93] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (December 2009): 1155–75; Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Abingdon: Routledge, 2008).

Albanesius, Chloe. “Illinois Water Utility Pump Destroyed After Hack.” PC Magazine, November 18, 2011. http://www.pcmag.com/article2/0,2817,2396632,00.asp.
Albert, Réka, Hawoong Jeong, and Albert-László Barabási. “Error and Attack Tolerance of Complex Networks.” *Nature* 406 (July 27, 2000): 378–82.
Alperovitch, Dmitri. “Revealed: Operation Shady RAT.” Santa Clara, California: McAfee, August 3, 2011.
Arquilla, John, and David Ronfeldt. “Cyberwar Is Coming!” *Comparative Strategy* 12, no. 2 (1993): 141–65.
———. “Cyberwar Is Coming!” In *In Athena’s Camp: Preparing for Conflict in the Information Age*, edited by John Arquilla and David Ronfeldt, 23–60. Santa Monica, CA: RAND Corporation, 1997.
———, eds. *In Athena’s Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND Corporation, 1997.
Barnett, Michael, and Raymond Duvall. “Power in International Politics.” *International Organization* 59, no. 01 (2005): 39–75.
Bellovin, Steven M., Susan Landau, and Herbert S. Lin. “Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications.” *Journal of Cybersecurity* 3, no. 1 (2017): 59–68.
Bencsáth, Boldizsár, Gábor Pék, Levente Buttyán, and Márk Félegyházi. “Duqu: A Stuxnet-like Malware Found in the Wild.” Budapest: Laboratory of Cryptography and System Security at Budapest University of Technology and Economics, October 14, 2011.
Berkowitz, Bruce D. *The New Face of War: How War Will Be Fought in the 21st Century*. New York, NY: Free Press, 2003.
Betz, David J., and Tim Stevens. “Analogical Reasoning and Cyber Security.” *Security Dialogue* 44, no. 2 (2013): 147–64.
———. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. New York: Routledge, 2011.
Biddle, Stephen. “Rebuilding the Foundations of Offense-Defense Theory.” *The Journal of Politics* 63, no. 3 (2001): 741–74.
Biddle, Stephen D. *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton University Press, 2004.
Boukerche, Azzedine, Renato B. Machado, Kathia RL Jucá, João Bosco M. Sobral, and Mirela SMA Notare. “An Agent Based and Biological Inspired Real-Time Intrusion Detection and Security Model for Computer Network Operations.” *Computer Communications* 30, no. 13 (2007): 2649–60.
Broad, William J., John Markoff, and David E. Sanger. “Stuxnet Worm Used Against Iran Was Tested in Israel.” New York Times, January 15, 2011. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.
Bureau of Labor Statistics, U.S. Department of Labor. “Information Security Analysts, Web Developers, and Computer Network Architects.” In *Occupational Outlook Handbook*, 2012th-13 Edition ed. Accessed May 23, 2013. http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts-web-developers-and-computer-network-architects.htm.

———. “Network and Computer Systems Administrators.” In *Occupational Outlook Handbook*, 2012th-2013 Edition ed. Accessed May 23, 2013. http://www.bls.gov/ooh/Computer-and-Information-Technology/Network-and-computer-systems-administrators.htm.
Canabarro, Diego Rafael, and Thiago Borne. “Reflections on The Fog of (Cyber)War.” NCDG Policy Working Paper. Amherst, Massachusetts, March 1, 2013.
Capaccio, Tony. “North Korea Improves Cyber Warfare Capacity, U.S. Says - Businessweek.” Bloomberg Businessweek, October 22, 2012. http://www.businessweek.com/news/2012-10-22/north-korea-improves-cyber-warfare-capacity-u-dot-s-dot-says.
Carmi, Shai, Shlomo Havlin, Scott Kirkpatrick, Yuval Shavitt, and Eran Shir. “A Model of Internet Topology Using K-Shell Decomposition.” *Proceedings of the National Academy of Sciences of the United States of America* 104, no. 27 (July 3, 2007): 11150–11154.
Cavelty, Myriam Dunn. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Abingdon: Routledge, 2008.
Cohen, Reuven, Keren Erez, Daniel ben-Avraham, and Shlomo Havlin. “Breakdown of the Internet under Intentional Attack.” *Physical Review Letters* 86, no. 16 (April 16, 2001): 3682–85.
———. “Resilience of the Internet to Random Breakdowns.” *Physical Review Letters* 85, no. 21 (November 20, 2000): 4626–28.
“Cyber Storm Exercise Report.” Washington, D.C.: Department of Homeland Security National Cyber Security Division, September 12, 2006. http://www.dhs.gov/sites/default/files/publications/nppd/CSC/Cyber%20Storm%20I%20After%20Action%20Report.pdf.
“Cyber Storm II Final Report.” Washington, D.C.: Department of Homeland Security National Cyber Security Division, July 2009. http://www.dhs.gov/xlibrary/assets/csc_ncsd_cyber_stormII_final09.pdf.
“Cyber Storm III Final Report.” Washington, D.C.: Department of Homeland Security National Cyber Security Division, July 2011. http://www.dhs.gov/sites/default/files/publications/nppd/CyberStorm%20III%20FINAL%20Report.pdf.
“Cyberspace as ‘EcoSpace.’” SENDS, November 5, 2010. http://sendsonline.org/2010/11/05/cyberspace-as-ecospace/.
Deibert, Ronald J. “Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace.” *Millennium-Journal of International Studies* 32, no. 3 (2003): 501–30.
Denning, Dorothy E. “Barriers to Entry: Are They Lower for Cyber Warfare?” *IO Journal* 1, no. 1 (2009).
Dietz, Thomas, Elinor Ostrom, and Paul C. Stern. “The Struggle to Govern the Commons.” *Science* 302, no. 5652 (2003): 1907–12.
Drummond, David. “A New Approach to China.” Google Official Blog, January 13, 2010. http://googleblog.blogspot.no/2010/01/new-approach-to-china.html.
Elkus, Adam. “Cyber Warfare...Brought To You By J.C. Wylie.” Information Dissemination, May 31, 2012. http://www.informationdissemination.net/2012/05/cyber-warfarebrought-to-you-by-jc-wylie.html.
Eun-jung, Kim. “S. Korea to Upgrade Preparedness against North’s Cyber, Nuclear Attacks.” Yonhap News Agency, August 29, 2012.

http://english.yonhapnews.co.kr/national/2012/08/29/18/0301000000AEN20120829008600315F.HTML.
Farwell, James P., and Rafal Rohozinski. “Stuxnet and the Future of Cyber War.” *Survival* 53, no. 1 (2011): 23–40.
Fearon, James D. “Rationalist Explanations for War.” *International Organization* 49 (1995): 379–379.
Finkle, Jim. “Big Tech Companies Offer Millions after Heartbleed Crisis.” Reuters, April 24, 2014. http://www.reuters.com/article/2014/04/24/us-cybercrime-heartbleed-idUSBREA3N13E20140424.
Fischer, Michael, Joerg Blank, and Christoph Dernbach. “Germany Confirms Existence of Operational Cyberwarfare Unit.” Deutsche Presse-Agentur, June 5, 2012. http://www.stripes.com/news/germany-confirms-existence-of-operational-cyberwarfare-unit-1.179655.
Folke, Carl, Thomas Hahn, Per Olsson, and Jon Norberg. “Adaptive Governance of Social-Ecological Systems.” *Annu. Rev. Environ. Resour.* 30 (2005): 441–73.
Frank, Aaron. “Military Revolutions, Evolution, and International Relations Theory.” Washington, D.C., 2010.
Fung, Brian. “Heartbleed Is about to Get Worse, and It Will Slow the Internet to a Crawl.” Washington Post, April 14, 2014. http://www.washingtonpost.com/blogs/the-switch/wp/2014/04/14/heartbleed-is-about-to-get-worse-and-it-will-slow-the-internet-to-a-crawl/.
Gartzke, Erik. “The Myth of Cyberwar.” *International Security* 38, no. 2 (Fall 2013): 41–73.
Gartzke, Erik, and Jon R. Lindsay. “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.” *Security Studies* 24, no. 2 (2015): 316–48.
Glaser, Charles L., and Chaim Kaufmann. “What Is the Offense-Defense Balance and Can We Measure It?” *International Security* 22, no. 4 (Spring 1998): 44–82.
Goodin, Dan. “Flame’s Crypto Attack May Have Needed $200,000 Worth of Compute Power.” Ars Technica, June 12, 2012. http://arstechnica.com/security/2012/06/flame-crypto-attack-may-have-needed-massive-compute-power/.
———. “Second Water Utility Reportedly Hit by Hack Attack.” The Register, November 18, 2011. http://www.theregister.co.uk/2011/11/18/second_water_utility_hack/print.html.
Gray, Colin S. *Another Bloody Century: Future Warfare*. London: Weidenfeld & Nicolson, 2005.
Greenberg, Andy. “How An Entire Nation Became Russia’s Test Lab for Cyberwar.” *Wired*, June 20, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/.
Grow, Brian, and Mark Hosenball. “Special Report: In Cyberspy vs. Cyberspy, China Has the Edge.” Reuters, April 14, 2011. http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414.
Hansen, Lene, and Helen Nissenbaum. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly* 53, no. 4 (December 2009): 1155–75.
Healey, Jason. “Stuxnets Are Not in the US National Interest: An Arsonist Calling for Better Fire Codes.” New Atlanticist, June 1, 2012. http://www.acus.org/new_atlanticist/stuxnets-are-not-us-national-interest-arsonist-calling-better-fire-codes.

Hopkins, Nick. “UK Developing Cyber-Weapons Programme to Counter Cyber War Threat.” Guardian, May 30, 2011. http://www.guardian.co.uk/uk/2011/may/30/military-cyberwar-offensive.
Hunt, Carl. “The Blogging Luddite: The Two-and-a-Half Faces of Cyberspace Security.” SENDS, April 25, 2011. http://sendsonline.org/2011/04/30/the-blogging-luddite-the-two-and-a-half-faces-of-cyberspace-security/.
Independent International Fact-Finding Mission on the Conflict in Georgia. “Report: Volume II.” Brussels: Independent International Fact-Finding Mission on the Conflict in Georgia, September 2009. http://www.ceiig.ch/pdf/IIFFMCG_Volume_II.pdf.
“Iran Says It Has Detected Duqu Computer Virus.” Reuters, November 13, 2011. http://www.msnbc.msn.com/id/45278589#.Ts6rqUohMXh.
Jervis, Robert. “Cooperation Under the Security Dilemma.” *World Politics* 30, no. 2 (January 1978): 167–214.
Johnson, Loch K. “Bricks and Mortar for a Theory of Intelligence.” *Comparative Strategy* 22, no. 1 (2003): 1–28.
Kaspersky, Eugene. “Shady RAT: Shoddy RAT.” Nota Bene, August 18, 2011. http://eugene.kaspersky.com/2011/08/18/shady-rat-shoddy-rat/.
Keith B. Alexander (Commander of United States Cyber Command). Oversight: U.S. Strategic Command and U.S. Cyber Command, § Senate Committee on Armed Services (2013).
Keizer, Gregg. “How Egypt Pulled Its Internet Plug.” Computerworld, January 28, 2011. http://www.computerworld.com/s/article/9207040/How_Egypt_pulled_its_Internet_plug.
Kello, Lucas. “The Meaning of the Cyber Revolution.” *International Security* 38, no. 2 (Fall 2013): 7–40.
Keohane, Robert O., and David G. Victor. “The Regime Complex for Climate Change.” *Perspectives on Politics* 9, no. 01 (2011): 7–23.
Knafo, Saki. “Anonymous And The War Over The Internet.” Huffington Post, January 30, 2012. http://www.huffingtonpost.com/2012/01/30/anonymous-internet-war_n_1233977.html.
———. “Anonymous And The War Over The Internet (Part II).” Huffington Post, January 31, 2012. http://www.huffingtonpost.com/2012/01/31/anonymous-war-over-internet_n_1237058.html?ncid=edlinkusaolp00000003.
Kotenko, Igor. “Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet.” In *19th European Simulation Multiconference “Simulation in Wider Europe*, 2005.
Krekel, Bryan, Patton Adams, and George Bakos. “Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage.” Washington, D.C.: Northrop Grumman Corp, March 7, 2012.
Krepinevich, Andrew F. “‘Cyber Warfare: A “Nuclear Option”?’” Washington, DC: Center for Strategic and Budgetary Assessments, August 24, 2012. http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/.
Kuehl, Daniel T. “From Cyberspace to Cyberpower: Defining the Problem.” In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 24–42. Washington, DC: National Defense University Press, 2009.
Kurtz, George. “Operation ‘Aurora’ Hit Google, Others by George Kurtz.” CTO, January 14, 2010. http://blogs.mcafee.com/corporate/cto/operation-aurora-hit-google-others.

Langill, Joel. “Want the Source Code to Stuxnet? Come and Get It.” Infosec Island, October 21, 2011. http://infosecisland.com/blogview/17613-Want-the-Source-Code-to-Stuxnet-Come-and-Get-It.html.
Langø, Hans-Inge. “Competing Academic Approaches to Cyber Security.” In *Conflict in Cyber Space*, edited by Karsten Friis and Jens Ringsmose. London: Routledge, 2016.
Lawson, Sean. “Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History.” Working paper. Fairfax, VA: Mercatus Center, January 2011.
Lewis, James A. “Significant Cyber Incidents Since 2006.” Center for Strategic and International Studies, April 2018. https://csis-prod.s3.amazonaws.com/s3fs-public/180425_Significant_Cyber_Events_List.pdf?pqetcWcwV7mvAo33_lAZFlQVQz7.E0qh.
Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2007.
———. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.
———. “The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon.” Washington, DC: National Defense University, March 1994. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA278484&Location=U2&doc=GetTRDoc.pdf.
Lieber, Kier A. *War and the Engineers : The Primacy of Politics over Technology*. Ithaca: Cornell University Press, 2005.
Lindsay, Jon R. “Stuxnet and the Limits of Cyberwarfare.” *Security Studies* 22, no. 3 (2013): 365–404.
Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. New York: Frank Cass, 2004.
Mearsheimer, John J. *Conventional Deterrence*. Ithaca: Cornell University Press, 1983.
Meilinger, Phillip S. “The Mutable Nature of War.” *Air & Space Power Journal* 24, no. 4 (2010): 24–30.
Molander, Roger C., Andrew Riddile, and Peter A. Wilson. “Strategic Information Warfare: A New Face of War.” Santa Monica, CA: RAND Corporation, 1996. http://www.rand.org/pubs/monograph_reports/MR661.html.
Moore, Gordon E. “Cramming More Components onto Integrated Circuits.” *Electronics* 38, no. 8 (April 19, 1965).
Nakashima, Ellen. “With Plan X, Pentagon Seeks to Spread U.S. Military Might to Cyberspace.” Washington Post, May 30, 2012. http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_print.html.
Nakashima, Ellen, Greg Miller, and Julie Tate. “U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say.” Washington Post, June 19, 2012. http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_print.html.
Norton, Quinn. “Anonymous 101: Introduction to the Lulz.” Threat Level, November 8, 2011. http://www.wired.com/threatlevel/2011/11/anonymous-101/all/1.
———. “How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down.” Threat Level, July 3, 2012. http://www.wired.com/threatlevel/2012/07/ff_anonymous/all/.

Nye, Joseph S. *The Future of Power*. New York: PublicAffairs, 2011.
O'Dwyer, Gerard. "Finland To Develop Cyber Defense 'Counterpunch.'" DefenseNews, October 20, 2011. http://www.defensenews.com/article/20111020/DEFSECT04/110200306/Finland-Develop-Cyber-Defense-Counterpunch-.
Peterson, Andrea. "Yes, Terrorists Could Have Hacked Dick Cheney's Heart." Washington Post, October 21, 2013. http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/.
Pilihanto, Atik. "A Complete Guide on IPv6 Attack and Defense." Bethesda, Maryland: SANS Institute, November 14, 2011.
"Quantum Dawn 2: A Simulation to Exercise Cyber Resilience and Crisis Management Capabilities." New York: Deloitte, October 21, 2013. http://www.sifma.org/uploadedfiles/services/bcp/after-actionreport2013.pdf?n=40439.
"Quantum Dawn After Action Report." New York: Security Industry and Financial Markets Association, March 5, 2012.
Rastello, Sandrine, and Jeanna Smialek. "Cybersecurity Starts in High School with Tomorrow's Hires." Bloomberg, May 16, 2013. http://www.bloomberg.com/news/2013-05-16/cybersecurity-starts-in-high-school-with-tomorrow-s-hires.html.
Rattray, Gregory J. "An Environmental Approach to Understanding Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 253–74. Washington, DC: National Defense University Press, 2009.
———. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.
Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.
———. *Cyber War Will Not Take Place*. Oxford University Press, 2013.
Rid, Thomas, and Peter McBurney. "Cyber-Weapons." *RUSI Journal* 157, no. 1 (2012): 6–13.
Rona, Thomas P. "Weapon Systems and Information War." Office of the Secretary of Defense, July 1, 1976.
Samaan, Jean-Loup. "Cyber Command: The Rift in US Military Cyber-Strategy." *The RUSI Journal* 155, no. 6 (2010): 16–21.
Schmitt, Eric, and Thom Shanker. *Counterstrike: The Untold Story of America's Secret Campaign against Al Qaeda*. New York: Times Books, 2011.
———. "U.S. Debated Cyberwarfare Against Libya." New York Times, October 17, 2011. http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=2.
Schultz, Kenneth A. "The Enforcement Problem in Coercive Bargaining: Interstate Conflict over Rebel Support in Civil Wars." *International Organization* 64, no. 02 (2010): 281–312.
Scoones, Ian. "New Ecology and the Social Sciences: What Prospects for a Fruitful Engagement?" *Annual Review of Anthropology* 28, no. 1 (1999): 479–507.
SecureWorks Counter Threat Unit Research Team. "Duqu Trojan Questions and Answers." Dell SecureWorks, October 26, 2011. http://www.secureworks.com/research/threats/duqu/.
Shane, Scott. "U.S. Officials Opening Up on Cyberwarfare." New York Times, September 26, 2012. http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html?pagewanted=all.

Snyder, Jack. “Correspondence: Defensive Realism and the ‘New’ History of World War I.” *International Security* 33, no. 1 (Summer 2008): 174–94.
Stempfley, Roberta, and Sean P. McGurk. Statement for the record, § Committee on Energy and Commerce, Subcommittee on Oversight and Investigations (2011).
Stone, John. “Cyber War Will Take Place!” *Journal of Strategic Studies* 36, no. 1 (2013): 101–8.
“Ten Days of Rain: Expert Analysis of Distributed Denial-of-Service Attacks Targeting.” Santa Clara, California: McAfee, July 2011. https://secure.mcafee.com/us/resources/white-papers/wp-10-days-of-rain.pdf.
Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” Guardian, May 17, 2007. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.
U.S. Department of Defense. “Sustaining U.S. Global Leadership: Priorities for 21st Century Defense,” January 2012.
U.S. Department of Homeland Security. “The National Strategy to Secure Cyberspace,” February 2003.
Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press, 2018.
Valeriano, Brandon, and Ryan C. Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press, USA, 2015.
———. “The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11.” *Journal of Peace Research* 51, no. 3 (2014): 347–60.
Van Evera, Stephen. *Causes of War: Power and the Roots of Conflict*. Ithaca: Cornell University Press, 1999.
———. “Offense, Defense, and the Causes of War.” *International Security* 22, no. 4 (Spring 1998): 5–43.
Vijayan, Jaikumar. “Demand for IT Security Experts Outstrips Supply.” Computerworld, March 7, 2013. http://www.computerworld.com/s/article/9237394/Demand_for_IT_security_experts_outstrips_supply.
Walker, Brian, Crawford S. Holling, Stephen R. Carpenter, and Ann Kinzig. “Resilience, Adaptability and Transformability in Social--Ecological Systems.” *Ecology and Society* 9, no. 2 (2004): 5.
Wendt, Alexander. “Anarchy Is What States Make of It: The Social Construction of Power Politics.” *International Organization* 46, no. 02 (1992): 391–425.
Yannakogeorgos, Panayotis Alexander. *Technogeopolitics of Militarization and Security in Cyberspace*. ProQuest, 2009.
Zetter, Kim. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” *Wired*, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.