The limits of compulsory cyber power: Assessing ecological potential and restraints in the digital domain

Hans-Inge Langø

NUPI Working Paper 819

Publisher: Norwegian Institute of International Affairs

Visiting address: C.J. Hambros plass 2d
Address: P.O. Box 8159 Dep.
NO-0033 Oslo, Norway
Internet: www.nupi.no
E-mail: info@nupi.no
Fax: [+ 47] 22 99 40 50
Tel: [+ 47] 22 99 40 00

The limits of compulsory cyber power: Assessing ecological potential and restraints in the digital domain

Hans-Inge Langø

Hostile actors in cyberspace are considered one of the fastest growing threats to states. Much has been written on the subject, but the available literature remains parochial, lacking a unifying understanding of the environment. This paper proposes a systematic approach to understanding the political utility of cyberspace, specifically the character of compulsory cyber power. It does so by conducting an ecological analysis of the defining characteristics of cyberspace and its security implications. The paper concludes that although cyberspace introduces new security dynamics such as significant increases in vulnerabilities and a collapse of speed, the compulsory power potential remains limited. Large-scale, destructive attacks are far more difficult to orchestrate than what public discourse might suggest. While actors may attack critical infrastructure in new places and with more ease through cyberspace than physical sabotage, cyber weapons are *primarily* disruptive, rather than destructive, and lack the ability to conquer territory or accumulate assets.

Acknowledgements:
I would like to express my gratitude to my colleagues at NUPI for input and feedback during the course of finishing this paper. In particular I wish to thank Karsten Friis who has offered guidance and encouragement throughout the process. Without his help this paper would be in much worse shape. I would also like to thank Dave Clemente, Adam Elkus, Matt Fay, Storm Jarl Landaasen, and Tim Stevens who read the final draft of this paper and offered helpful advice both on the subject matter and theoretical issues. Of course all mistakes and errors of analysis are mine alone. Finally, I wish to thank the Norwegian Ministry of Defense and the Norwegian Cyber Defense Command for supporting this research and NUPI's contribution to the MNE7 and MCDC projects.

Introduction

> "The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country. Attackers could also seek to disable or degrade critical military systems and communication networks. The collective result of these kinds of attacks could be a "cyber Pearl Harbor:" an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."[1]
> U.S. Secretary of Defense Leon E. Panetta, New York, October 11, 2012

The notion of a "cyber Pearl Harbor" has been a consistent theme of the cyber security discourse for several years.[2] The exact meaning of the term varies, but it implies some form of complex, large-scale cyber attack against the U.S. critical national infrastructure (CNI).[3] It evokes images of massive destruction and chaos, all instigated by a few keystrokes. However, we have yet to see anything close to such a doomsday scenario, either in scale or complexity. Why have we not yet seen cyber war, or a "cyber Pearl Harbor?" This paper posits that such a scenario, used so often to warn of the dangers of our increased dependency on information-communications technology (ICT), is emblematic of a debate founded on a faulty or incomplete understanding of its main object of analysis: cyberspace. This issue is not restricted to policy debates in Washington or elsewhere. Many scholars have written academic work on the topic of cyber security, dealing with a range of issues and taking different approaches, in order to answer the central question of how actors can hurt other actors through cyberspace. However, none have taken a systematic approach to understanding the strategic utility of cyberspace.

Instead, the academic debate is often either parochial, focusing on limited issues such as the definition of war, or fixated on finding commonalities with existing forms of military power, usually sea, nuclear or air power. These works often take a top-down approach, using either empirical data or analogy to generalize about cyberspace, yet both approaches have significant shortcomings. The lack of available em-

---

1 Leon E. Panetta, "Defending the Nation from Cyber Attack" (speech given at Business Executives for National Security, New York, NY, 2012), http://www.defense.gov/speeches/speech.aspx?speechid=1728.

2 Andrew F. Krepinevich defines a "Cyber Pearl Harbor" as a large-scale cyber attack that does not cause debilitating damage, but shocks the United States, much like the original attack on Pearl Harbor. See: Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option"?* (Washington, D.C.: Center for Strategic and Budgetary Assessments, August 24, 2012), http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/.

3 For a broader discussion on CNI, see Dave Clemente, *Cyber Security and Global Interdependence: What Is Critical?* (London: Chatham House, February 2013).14/06/2013 14:25:00

pirical data on cyber conflict renders generalization difficult, while comparisons with other forms of power are inevitably flawed due to their inherently different natures. This study avoids these problems by addressing cyber power, specifically compulsory cyber power, through what I will label an *ecological* analysis. By examining the defining characteristics of cyberspace as an ecological system and its security implications, we arrive at a more detailed picture of cyber power and its potential role in interstate conflict. The aim of such an approach, to borrow the words of Clausewitz, is to achieve a better description of the nature of cyberspace as an arena or tool for conflict and distinguish this nature from cyberspace's current character. If the conclusions drawn here are sound, we should have a better understanding of cyber conflict today, as well as a better understanding of where it might go in the future. The primary research question therefore becomes: How can states utilize cyberspace to coerce or compel its adversaries to achieve political goals?[4]

Cyberspace as an ecological system

An ecological approach to cyberspace means mapping the terrain of cyberspace and describing what actions cyberspace either encourages or restrains. Several scholars have conducted various forms of environmental analysis of cyberspace, and the approach used in this paper is synthesized from several of these texts, with the most influential being Gregory Rattray's study of the strategic features of cyberspace.[5] However, the approach used in this paper is different 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.[6] Second, it is more comprehensive and systematic in analyzing cyberspace as a system by distinguishing between the defin-

4 This paper does not propose a formal model for conflict in cyberspace. For that to be possible, the defining characteristics would have to be better defined and measured, and the causal relationships between the characteristics and the implications would have to be better tested. This is not possible today given the lack of empirical data on cyber conflict.

5 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).

6 "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/.

ing 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 permanent characteristics 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.

There are numerous examples of social science literature that examine the relationship between actors, institutions and structures, and how interaction between these parts causes systemic changes.[7] Similar to network theory and other approaches studying the relationship between actors and structures, this paper argues 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. 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?

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 itself. This paper posits that cyberspace has four defining characteristics: it is malleable, virtual, networked and software-centric. All of these characteristics carry security implications, some of which feature prominently in the cyber security debate, for 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, shape actor behavior. 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. If our assumption is valid, we should

7 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" (presented at the American Political Science Association Annual Convention 2010, Washington, D.C., 2010).

expect certain phenomena to occur, but further testing of the model will be necessary.[8] While a whole host of behaviors and actions might fall under the rubric of cyber security, this paper is primarily interested in actions that can be taken to achieve political ends. As such, this paper is not merely descriptive, but analytical. It seeks to weigh the means and ways of cyberspace against political ends—and more specifically, ends through coercive actions.

This paper comprises three main sections. The first section defines the paper's theoretical approach and thematic scope. It begins with a discussion of definitions and thematic limitations to define the object of analysis, namely cyberspace. This is followed by a brief discussion of the existing literature on cyber security, with a particular focus on cyber power and ecological analysis. The second section offers my analysis of cyberspace through an ecological approach. This section discusses each of the four defining characteristics and their security implications separately, before synthesizing these observations into a general picture of compulsory cyber power. Finally, the third section discusses the implications of this ecological model for both theory and policy. It also suggests future areas of research, especially research questions raised but not answered during the course of this work.

8 While this paper makes the assumption that actor behavior is shaped by the terrain it operates in, this is not the only variable determining actor behavior. Indeed, it is one of three, with the other two being the structural (external) environment, often referred to as the international system, and the actor's political (internal) context. Both variables may have significant impact on actor behavior in cyberspace, but this paper will only deal with the ecological variable. Therefore, addressing the issue of cyber power through an ecological analysis will only tell part of the story of cyber conflict.

Addressing cyber power

Instead of limiting the analysis to military operations and warfare, this paper will focus on cyber *power*. This offers a broader perspective of the strategic utility of cyberspace, including both civilian and military, public and private sectors. Defining cyber power will tell us how states can utilize cyberspace for political ends in the same way past scholars did so with sea or air power. A good starting point for analysis would be Joseph Nye, Jr.'s definition of cyber power:

> "[A] set of resources that relate to the creation, control, and communication of electronic and computer-based information--infrastructure, networks, software, human skills. This includes not only the Internet of networked computers, but also Intranets, cellular technologies, and space-based communications. Defined behaviorally, cyberpower is 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."[9]

This is a broad subject, so the discussion in this paper will be limited to compulsory cyber power, which David J. Betz and Tim Stevens describe as "direct coercion by one cyberspace actor in an attempt to modify the behaviour and conditions of existence of another."[10] Compulsory cyber power is the focus of most of the current academic and policy debates, and by addressing it first the stage is set for discussions of other forms of cyber power.[11]

Definitions

Given the lack of consensus on terminology, precision in terms and concepts is imperative when discussing cyber security. This section is in no way an exhaustive or definitive overview of the terminology of cyber security, but it seeks to articulate and clarify the scope of the discussion and analysis that follow below.[12] A good place to start is by looking at cyberspace itself. Martin C. Libicki has divided cyberspace

9 Nye, *The Future of Power*, 123.
10 Betz and Stevens, *Cyberspace and the State*, 45.
11 For other forms of cyber power, see ibid., chap. 1.
12 In addition to describing what is included when discussing cyber conflict, it is important to note what is not included. Cyber conflict does not usually include cyber crime, industrial espionage or hacktivism conducted by non-state actors, unless these disparate groups are in the employment of states pursuing political goals. While non-state actors may hold a relatively stronger position in cyberspace than in traditional environments or domains, cyber conflict directly between states and non-state actors remains a minor issue in terms of state security. Speculation about cyber terrorism remains precisely that, speculation.

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."[13] The semantic layer "contains the information meaningful to humans or connected devices."[14] 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. Computer Network Operations (CNO) can exploit all levels.[15] Computer Network Exploitation (CNE) will likely target the syntactic layer to extract or manipulate information, while Computer Network Attacks (CNA) will seek to create cognitive effects by manipulating the semantic layer or create kinetic effects by controlling the syntactic layer in order to manipulate the physical layer. It should be noted that CNE and CNA are not mutually exclusive actions. CNA is made possible by first conducting reconnaissance through CNE to identify the structure and vulnerabilities of the targeted network before triggering the attack. As such, intelligence gathering, conducted through CNE or more traditional approaches, enables CNA.

While the layer model may be relatively uncontroversial, defining cyberspace as a whole remains a subject for debate. Depending on the perspective, cyberspace can be imagined as a domain, environment or merely a loose category of functions.[16] Daniel T. Kuehl has described cyberspace as "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."[17] This is a commonly used definition of cyberspace, but it is not entirely adequate for this discussion. The term "domain" is usually used in a military context, and it is the dominant way of conceptualizing cyberspace in most western militaries. It elevates cyberspace to a distinct warfighting domain along with the other domains of air, land, sea and space. This approach is not without detractors. Libicki has argued that calling it a domain is inappropriate because cyberspace as a "thing" does not exist. Rather, it is a grouping term that includes a host of as-

13 Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 8.
14 Ibid., 9.
15 Whether this social function constitutes a fourth layer is unresolved. While the cognitive effects of CNO are not a significant topic of discussion in this paper, it will treat such effects as happening in a fourth, social layer.
16 A fourth definition is the term "infosphere," of which cyberspace is but a part, used by David J. Lonsdale. This definition, however, is too broad and vague to be appropriate for meaningful analysis. See: David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York: Frank Cass, 2004).
17 Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 28.

sets and functions. Furthermore, Libicki argues that treating cyberspace as a distinct domain ignores its subsidiary role to kinetic operations.[18]

The idea that cyberspace is more a function than a terrain is not without merit, at least in military terms when dealing with network-to-network warfare, but it ignores the wider societal implications of cyberspace and ICT integration. When considering cyber power writ large it is therefore appropriate to refer to cyberspace as an environment, as it encompasses society as a whole, including the private sector and civil society. Furthermore, approaching cyberspace as an environment means that we include not just the three primary layers of cyberspace as conceptualized by Libicki, but also the fourth social or cognitive layer.[19] This is important because wielding of cyber power will, if successful, have a political effect beyond the mere operational effect of disrupting, degrading or destroying computer systems. Furthermore, the dense integration of ICT into society means that any cyber warfare or conflict is unlikely to be limited to the governmental or military sphere.

Conflict in cyberspace should therefore be analyzed as its own environment, and not as a military subset of a larger information environment. While interstate conflict is likely to remain the predominant type of conflict, and the military will retain its predominant position, separating the military part of cyberspace from the civilian, and especially the commercial, parts of cyberspace is both difficult and counterproductive. The line between civilian and military is often blurry in cyberspace, and most of the ICT infrastructure is privately owned. This means that the military is vulnerable through privately-held infrastructure, but must also, in time of war, defend these assets. In addition, a significant part of the innovation in this field comes from the private sector, and often the most talented people work for Google or Apple, not the Pentagon. One could argue that the center of gravity of U.S. cyber power lies not at Fort Meade, headquarters of the U.S. Cyber Command (USCYBERCOM) and the National Security Agency (NSA), but in Silicon Valley in California or the many DNS servers across the country.[20]

18 Martin C. Libicki, "Cyberspace Is Not a War-Fighting Domain," *I/S: A Journal of Law and Policy for the Information Age* 8, no. 2 (2012): 321–336.

19 In his work Libicki mentions a possible fourth, pragmatic layer of cyberspace. This layer would deal with a statement's "purpose when considered in a particular context." This contextual understanding of information can be important, but Libicki's concept does not deal with the social effects of cyberspace. See Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, 237.

20 Interview with Jason Healey, Washington, DC, June 2012.

Cyber war and cyber conflict

The term "cyber operations" usually denotes actions undertaken through cyberspace. While kinetic attacks or sabotage against physical infrastructure can cause effects in cyberspace by disrupting communications between parties or access to servers, such actions are not considered part of the field of cyber security. However, cyber security does include actions undertaken through cyberspace to influence physical or organizational processes. An example of the former is Stuxnet, while the latter could be a CNA on a government network meant to disrupt, degrade or destroy the command and control structure. CNO can also have cognitive effects on the operations' targets. This can be achieved by manipulating an opponent's decision-making process, usually through the form of deception or disruption.

Determining exactly what level of destruction or disruption is possible through cyberspace is still an ongoing discussion. Scholars have coined the term Strategic Information Warfare (SIW) as a way of waging cyber warfare on the strategic level, causing independently decisive effects on a target through the use of CNO.[21] While the viability of SIW as a tool of cyber power is contested, that has not kept policymakers and analysts from adopting the general idea in order to warn against the dangers of cyber war.[22] However, using the term cyber war is both conceptually and empirically wrong. Cyber war implies a war between actors that takes place solely in cyberspace, but this is a highly unlikely possibility, at least in the foreseeable future, for two reasons. First, the notion of cyber war ignores the likelihood of escalation into kinetic operations and exaggerates actors' willingness to contain conflicts to cyberspace.[23] Second, it ignores the re-

21 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, California: RAND Corporation, 1996), http://www.rand.org/pubs/monograph_reports/MR661.html; Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, Massachusetts: MIT Press, 2001).

22 The term cyber war is frequently misused by policymakers, scholars and news organizations, using it to describe a wide range of activities from espionage to military operations part of a larger conflict. For examples, see 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, California: RAND Corporation, 1997), 23–60; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010); Mike McConnell, "Mike McConnell on how to win the cyber-war we're losing," *Washington Post*, February 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html; John D. Sutter, "Anonymous Declares 'Cyberwar' on Israel," *CNN.com*, November 20, 2012, http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html.

23 Several scholars have criticized the use of the term cyber war, specifically the idea of stand-alone cyber war. See Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*; Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld & Nicolson, 2005); Jean-Loup Samaan, "Cyber Command: The Rift in US Military Cyber-Strategy," *The RUSI Journal* 155, no. 6 (2010): 16–21; Sean Lawson, *Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History*, Working paper (Fairfax: Mercatus Center, January 2011); Erik Gartzke, *The Myth of Cyberwar*, Working paper, December 7, 2012; Sean Lawson, "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States," *First Monday* 17, no. 7 (July 2, 2012), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3848/3270;

quirement that actions in cyberspace must reach decisive political ends for it to be able to stand alone as a use of force.[24]

A broader, more appropriate term for military operations in cyberspace is cyber warfare, which means conducting CNO as part of a larger war or conflict. This means that cyber operations are not a substitute for regular military operations, but rather as one aspect of a larger military conflict. Still, the term cyber warfare is almost exclusively focused on military operations, with proxy forces only a marginal concern, and does not fully take into account the broader societal aspect of cyber security. Furthermore, it is not a term appropriate for use in peacetime, which is when a lot of malicious activity in cyberspace takes place. A more comprehensive term would then be cyber conflict.[25] This term encompasses all manners of hostile actions taken in cyberspace, ranging from direct CNA against opponents in wartime to covert operations and espionage.

As for what specific operations fall under compulsory cyber conflict, there is a wide range of possibilities, with the most relevant being CNA against infrastructure and command and control systems. CNE could also be used to the extent that espionage can be exploited for compellence purposes, but would most probably only work in a supporting role. CNA can mean directly disruptive, degrading or destructive attacks. Operations aimed at subversion or manipulation of a target population can also have effects, though it is unclear whether it would work as a form of coercion or compellence. It is not a new phenomenon, though society-wide integration of ICT can provide significant economies of scale. [26]

Competing ideas

As a recognizable security practice, cyber security is still in its nascent stage. It is not surprising, therefore, that the academic field of cyber security is still quite young. We can trace discussions of information warfare, a broader term that encompasses much of the ideas of CNO prevalent today, at least back to the 1970s. However, most of the significant academic contributions to the field have been published more

Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

24 Rid, "Cyber War Will Not Take Place."

25 For a broader discussion on cyber conflict, see Athina Karatzogianni, *The Politics of Cyberconflict*, Routledge Research on Internet and Society (London and New York: Routledge, 2006); Athina Karatzogianni, ed., *Cyber Conflict and Global Politics*, Routledge Contemporary Security Studies (London and New York: Routledge, 2009).

26 These are the main categories of cyber warfare, but there are several other types of operations under the broader concept of information warfare, some relevant to cyber power. For more information, see: Martin C. Libicki, *What Is Information Warfare?* (Washington, D.C.: National Defense University, 1995).

or less in the past two decades.[27] While there is much written now on cyber security, it remains a fragmented field of disparate approaches and conceptual thinking.[28] These approaches can offer significant elucidation of certain questions, but are often too parochial or based on concepts of other forms of power to be used for comprehensive analysis. 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. [29] More specifically, information was treated as a material asset, and they posited that information dominance through organizational superiority could be translated into battlefield victory. [30] However, their work does not adequately, or realistically for that matter, describe how actors can exploit cyberspace vulnerabilities, specifically 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.

Another important, yet flawed, component of the cyber security literature is the work surrounding SIW. 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.[31] This is an inherently flawed approach as it inevitably runs the risk of shoehorning something new into an old analytical framework.[32] This, in turn, leads to conceptual and terminological confusion. Furthermore, such a top-down approach to the study of cyberspace is not

27 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: Free Press, 2003), chap. 4 and 6.

28 For a broader discussion on the literature of cyber security, see Hans-Inge Langø, "Den Akademiske Debatten Om Cybersikkerhet," *Internasjonal Politikk* 71, no. 2 (May 2013): 229–240.

29 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, California: RAND Corporation, 1997).

30 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, D.C.: National Defense University, March 1994), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA278484&Location=U2&doc=GetTRDoc.pdf.

31 For examples of scholarly use of analogies in regards to cyber security, see: Rattray, *Strategic Warfare in Cyberspace*; Rattray, "An Environmental Approach to Understanding Cyberpower"; Krepinevich, *Cyber Warfare: A "Nuclear Option"?*; Kuehl, "From Cyberspace to Cyberpower: Defining the Problem."

32 Samaan, "Cyber Command: The Rift in US Military Cyber-Strategy."

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 done a better job of defining the character of cyberspace, or more specifically cyber conflict. Scholars such as Thomas Rid and David J. Lonsdale have made persuasive arguments that delineate the limits of strategic cyber power, or SIW.[33] For instance, Rid argues that cyberspace is not conducive to fighting wars, but more appropriate for sabotage, espionage and subversion.[34] This traditionalist approach has helped cool the cyber hype and offered a more tempered take on the challenges ahead. However, this approach remains insufficient for structured analysis of compulsory cyber power. First, it is overly focused on violence as a necessary component of warfare, dismissing the disruptive potential of cyber warfare.[35] As societies grow more dependent on ICT, so does the number of vulnerabilities, thus potentially making compulsory cyber power more tenable than the traditionalists claim. Second, the empirical approach to cyber security is inherently flawed because 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, as Rid does, this ignores the reality that most actors are still grappling with the security implications of cyberspace. Specifically, states are still trying to figure out whether they can hurt or be hurt through cyberspace. While Rid may be proven right, it is far too early to conclude on the potential for cyber warfare.

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.[36] For instance, when Joseph Nye, Jr. attempts to define cyber power, he uses an environment analysis to describe its character.[37] Nye's main focus is the diffusion of power occurring in cyberspace, while others focus on different characteristics. Libicki indirect-

33 Rid, "Cyber War Will Not Take Place"; Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*.
34 Rid, "Cyber War Will Not Take Place."
35 While Rid defines violence as a requirement for war, other scholars argue that states can use force without bloodshed and still achieve political goals. See: Gray, *Another Bloody Century: Future Warfare*, 293–294; 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): 101–108.
36 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.
37 Nye, *The Future of Power*, chap. 5.

ly addresses compulsory cyber power in his work on deterrence and conquest in cyberspace, while Rattray approximates a systematic analysis of cyberspace's "strategic features" in a 2009 book chapter appropriately called "An Environmental Approach to Understanding Cyberpower."[38]

All of these works inform our discussion about particular characteristics or phenomena, but are not systematic enough to serve as a foundational framework of analysis. Nye's work is not broad enough and does not directly address the security implications of the diffusion of technology, while Libicki focuses more on function than form. The point here is not to detract from their outstanding work, but to show the limits of its broader applicability to compulsory cyber power. Rattray's work is more systematic, but as with other texts discussing what makes cyberspace unique or distinct, does not adequately address the distinction between defining characteristics and their security implications. Examining existing theories of power (land, sea, air and space), he identified four common features: technological advances, speed and scope of operations, control of key features and national mobilization.[39] Though these are all valid observations, he mistakenly groups them together in a single category of "strategic features." Technological advances and speed are defining characteristics, but control of key features is a way of achieving strategic ends. Likewise, national mobilization is the implication of power diffusion and the networked space, and not a characteristic in and of itself. Despite their shortcomings, though, it is clear that the 'environmentalist' school of thought is the most appropriate starting point for an analysis of cyberspace as a strategic environment.

38 Libicki, *Conquest in Cyberspace: National Security and Information Warfare*; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, California: RAND Corporation, 2009); Rattray, "An Environmental Approach to Understanding Cyberpower."

39 Rattray, "An Environmental Approach to Understanding Cyberpower," 262.

An ecological approach

Much of the existing cyber security literature offers observations on what separates cyberspace from other domains or environments. Its uniqueness is often highlighted in order to justify the development of new theories or concepts of security. Precisely how unique cyberspace is lies beyond the scope of this paper, but it is commonly accepted among scholars that the environment holds some distinct properties. 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 defining 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.[40]

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, decentralized (flat and networked) and software-centric.

A Malleable Terrain

Cyberspace is a manmade environment. While the electromagnetic spectrum is not, cyberspace as it exists today consists of hardware and software built and designed by people. The different layers of cyber-

40 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.

space are a result of this 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, as with the introduction of Internet Protocol version 6 (IPv6), 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. We can call this feature 'vertical malleability.'

The other kind, 'horizontal malleability,' implies a change in how humans and society relate to cyberspace.[41] 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 old and new functions.

Both forms of malleability have implications for security. 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 therefore the result of vertical malleability.

Furthermore, efforts to 'fix' the attribution problem illustrate 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

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

vulnerabilities.[42] Nonetheless, it is an example of how vertical malleability can impact security.

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 on the state level, this means that the battleground is in flux and that the perimeter is in constant expansion. The increased focus on critical infrastructure protection amongst many states suggests that governments and officials share this perception, 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.[43] 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.[44] 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.

The malleability of cyberspace is perhaps 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. By definition 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.

42 Atik Pilihanto, *A Complete Guide on IPv6 Attack and Defense* (Bethesda, Maryland: SANS Institute, November 14, 2011).

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

44 This is based on the author's numerous conversations with cyber security practitioners and officials both in the public and private sector, in Norway and across Europe.

A virtual realm

Cyberspace is often described as a virtual or non-physical domain. This is not entirely accurate. Cyberspace is dependent on a physical layer to function, but a significant part of what constitutes cyberspace is virtual. 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.[45]

The reason why these layers and processes are usually referred to as 'virtual' is a question of scale. The information in cyberspace is not non-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.[46] 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 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 concept of 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

45 Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, chap. 10.
46 Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics* 38, no. 8 (April 19, 1965).

against a wide range of targets from thousands of computers spread across several continents.[47]

The strategic implication of the collapse of distance 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.

The collapse of both speed and distance 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."[48] 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.[49]

The difference highlighted is important, but Arquilla and Ronfeldt inaccurately infer from this an advantage over blitzkrieg. Debilitating CNAs against communications or command and control systems can

47 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, 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.

48 Arquilla and Ronfeldt, "Cyberwar Is Coming!," 44.

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

'blind' an opponent, but territorial maneuvering has significant advantages. Whereas German tank divisions were able to 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, or as Thomas Rid and Peter McBurney put it, "the proverbial fire-and-forget missile."[50] 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. According to Adam Elkus, 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."[51] 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.

Cyber weapons also do not have the ability to dislocate its opponents, a key feature of blitzkrieg, according to Barry Posen.[52] The lack of territory in cyberspace to conquer and hold creates opportunities, but also limits the benefits of the offense. This issue will be discussed to a greater extent later under the rubric of cyberspace as a networked environment, but has significant implications for the issue of speed and space as well.

The limitations on surprise attacks mean the increase in speed only yields a limited first-move advantage.[53] 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.[54]

---

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

51 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.

52 Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars* (Ithaca, New York: Cornell University Press, 1984), 86.

53 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).

54 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-

In summary, the collapse of space and time in cyberspace has several implications for security. It eases, or erases entirely, the constraint of geography on offensive actions in cyberspace, and enables actors to launch CNOs with little to no notice. However, given the nature of cyber tools, large-scale attacks are difficult to achieve, and achieving lasting effects may be even harder. Since advanced cyber weapons usually only have single-shot usage, an attacker must continue to hit a target to achieve a cumulative effect, thus reducing the element of surprise and first-move advantage. In practical terms, this would suggest that an actor would need significant resources to conduct and maintain operations to a high enough level and for a long enough period of time to reach political goals.

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 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 attacks 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.[55] The third subcomponent

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.

55 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.

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.[56]

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.[57] The chokepoints in terms of cyberspace, according to Gregory J. Rattray, "include the physical infrastructures that enable communications, such as undersea fiber optic cables and communications satellites, and major interconnection points for large global networks."[58] 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 bor-

56 Réka Albert, Hawoong Jeong, and Albert-László Barabási, "Error and Attack Tolerance of Complex Networks," *Nature* 406 (July 27, 2000): 378–382; Reuven Cohen et al., "Resilience of the Internet to Random Breakdowns," *Physical Review Letters* 85, no. 21 (November 20, 2000): 4626–4628; Reuven Cohen et al., "Breakdown of the Internet Under Intentional Attack," *Physical Review Letters* 86, no. 16 (April 16, 2001): 3682–3685.

57 Nye, *The Future of Power*, 123.

58 Rattray, "An Environmental Approach to Understanding Cyberpower," 268.

ders and not easily disentangled.[59] Only an irrational or desperate actor would destroy a chokepoint because 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 highly risky.

As mentioned earlier, the territory of cyberspace is intangible. In the same way that it is impossible to blockade an undersea cable without physically controlling it, it is also not possible to conquer networks. They can be remotely accessed and controlled, but all the system administrator has to do in response is to cut the power or sever the external link. Without physical assets, it is not possible to accumulate territory in cyberspace overtly. This lack of conquerable land likely means that CNOs have to have either destructive or degrading effects on the networks for them to have tangible effects outside of cyberspace. Disruptive attacks will have only fleeting effects, which are of limited use unless used in support of operations in other domains, enabling physical gains.

Attacking the chokepoints of the Internet is not the same as striking the physical layer of closed networks, and differentiating between the two is important for conceptual clarity and security implications. The key differences are ways of access and issues of containment. Militaries usually use closed networks for classified information and communication. Communications networks are likely encrypted (theoretically these can be broken, but it would require computing power few, if any, countries possess or inside knowledge of the cryptosystem itself to enable so-called side channel attacks), while information processing networks can be restricted to a physical location, like a base, and air-gapped. The latter means there is no connection to outside networks, such as the Internet. There are also semi-closed networks that have access and authentication measures in place to keep unwanted visitors out, and these are the most common targets for CNE, or cyber espionage. Currently, the only way to access a closed network is to gain physical access to the facility itself. This was done in the case of Stuxnet, where a USB thumb drive carrying the malware made its way to a computer connected to the network at the Natanz enrichment facility.[60] Such an operation requires an insider or covert operations

59 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.

60 Richard Sale, "Stuxnet Loaded by Iran Double Agents," *Industrial Safety and Security Source*, April 11, 2012, http://www.isssource.com/stuxnet-loaded-by-iran-double-agents/.

capabilities. While this makes it harder to gain access, it should theoretically also keep the malware, or any effects of the malware, from spreading. This is often not the case, as many perceivably closed networks have some vulnerabilities; for instance, the air gap can be jumped backwards by someone taking material out of the facility and inserting it into open networks. Allegedly, the subsequent spread of Stuxnet was a case of the latter as an Iranian scientist brought the infected USB thumb drive home and plugged it into a computer connected to the Internet, though that particular version has been disputed.[61]

The spread of other complex malware, such as Flame and Duqu, suggests that these cyber tools are not accurate or easily contained. 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.[62] 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.[63]

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 both a comprehensive situational awareness of the system and precise, contained attacks. The unintended consequences of cyber weapons appear to be potentially significant, as the ground itself is dynamic and the tools used can be difficult to control.

---

61 David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012), 204; Steven Cherry, "Stuxnet: Leaks or Lies?," *IEEE Spectrum*, September 4, 2012, http://spectrum.ieee.org/podcast/computing/embedded-systems/stuxnet-leaks-or-lies.

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

63 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.

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."[64]

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.[65]

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

64 Nye, *The Future of Power*, 115.

65 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* (Washington, D.C., 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).

before, that threshold is now significantly lower. Developing malware is mostly an 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.[66] Moreover, there are a limited number of individuals who can do the sophisticated kind of programming necessary for malware such as Stuxnet or Flame. Second, hardware is not irrelevant, as some CNOs necessitate access to significant computing power to perform complex tasks.[67] 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)."[68] 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 phys-

66 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*, 2012–2013 Edition, 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*, 2012–13 Edition, accessed May 23, 2013, http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts-web-developers-and-computer-network-architects.htm.

67 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/.

68 Nye, *The Future of Power*, 118.

ical infrastructure used at Natanz, specifically the centrifuges, to test out and properly calibrate the malware.[69]

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.[70] 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.[71] 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

69 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.

70 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.

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

Internet, which can then be redesigned for other targets.[72] The U.S. 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."[73]

Given these developments, the diffusion of technology in relation to cyber security has significant 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.[74] 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.[75] 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.

Measuring the model

The defining characteristics suggest what hostile actions are possible, practical and effective. Malleability means a wide 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.[76] These are relatively crude operations aimed at disrupting communications, and as such the threshold for conducting them might be relatively low.

More advanced operations would likely manifest themselves in attacks on critical national infrastructure, such as power grids, stock exchanges and telecom infrastructure. The difference is that while DDoS at-

72 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.

73 Roberta Stempfley and Sean P. McGurk, *Statement for the Record* (Washington, D.C.: Department of Homeland Security, 2011).

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

75 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.

76 *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.

tacks 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. As of today there are no known incidents of states launching such attacks on CNI, though states are developing the capability and capacity for complex offensive operations. Stuxnet showed that critical infrastructure attacks are possible, and there have been other, though smaller, examples of attacks or so-called proofs of concepts of attacks on critical national infrastructure.[77] Yet the details of the Stuxnet operation reveal the challenges of implementing such operations.

The challenge of attributing actions to actors, enabled by the malleability and networked nature of cyberspace, would suggest a low threshold for malicious activity, but given the uncertain accuracy and effects of attacks, not to mention the single-shot nature of most tools, it is more likely that states would be hesitant about launching attacks. These factors, combined with increased vulnerabilities leaving information available through cyberspace, suggest that states would be more inclined to use their cyber resources on espionage, at least in peacetime. This is largely the picture of cyber security today. While states worry about the potential threat against CNI, cyber security today, on a state level, is almost entirely about espionage. A list 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

77 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.

78 James A. Lewis, "Significant Cyber Incidents Since 2006" (Center for Strategic and International Studies, August 16, 2012), http://csis.org/files/publication/121120_Significant_Cyber_Incidents_Since_2006.pdf.

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.

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

In regards to attribution, it should be noted that behavior during war, or intensified conflict, could be different. 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.

Regarding how the collapse of distance 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.[83] The cyber attacks on Georgia were part of a military campaign, attempting to disrupt communications, albeit in limited ways, during fighting.[84] However, the operational value of the attacks was quite small as Georgian authorities were able to reroute traffic and move servers abroad, evidencing both the resilience of the networked space and the inefficiency of blunt tools such as DDoS.

From an offensive perspective, diffusion of technology should not have significant influence on state behavior. It may enable more states

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.

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 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.

84 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.

to conduct CNOs, thus increasing the risk of retaliation in cyberspace, but it is unclear whether moderate cyber capabilities in smaller states would successfully deter more powerful ones from attacking them.

Implications

The defining characteristics of cyberspace suggest a picture of conflict that closely resembles what has been seen in the past decade. There have been few attacks, and most malicious activity is espionage. What little attacks have happened in war or intense conflict have either been of entirely auxiliary nature (Estonia, Georgia), harassment (Korea) or simple 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 is 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.[85]

If this model and its construction is sound, the defining characteristics and their security implications indicate how actors might leverage cyberspace to achieve political goals, and thus describe the mechanics underpinning compulsory cyber power. The model illustrates the possibilities of cyber operations, but perhaps more so their limitations. While concluding would be premature, the findings presented here suggest that states have limited coercive power in cyberspace. In the same way that strategic bombing and sea blockades have only limited utility by themselves, cyber operations alone cannot be decisive in war because they cannot dislodge an opponent or accumulate territory or material assets. In other words, they do not challenge the primacy of land power.[86]

Others have reached similar conclusions, but there are flaws in the traditionalist arguments. Thomas Rid argues that cyberspace is not used for warfare, but sabotage, espionage and subversion.[87] The assumption is that cyberspace holds little potential for large-scale damage, and thus coercion. The focus on violence by critics of the cyber hype is a conceptual issue that can be debated. However, the empirical approach has shortcomings. There is simply not enough data on the strategic utility of cyberspace, rendering any conclusion over cyber power incomplete. In addition, the malleability of cyberspace ensures that the environment does not remain static. In other words, while the model presented here also accentuates the limits of cyber power, it

85 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.

86 John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W. W. Norton & Company, 2001), chap. 4.

87 Rid, "Cyber War Will Not Take Place."

acknowledges that it is not static either. A change in any of the defining characteristics might change the utility of cyberspace, though its malleability is probably the most important. Changes in dependency and actors' ability to exploit those accompanying vulnerabilities can significantly alter the coercive potential. Similarly, improvements in attributing hostile actions to actors, a wicked problem in cyber security today, could mean increased relevance for deterrence and coercion theory. What seems difficult today might be entirely plausible in the future. Only time will tell.

If the structural restraints further decrease the coercive potential of cyberspace, perhaps other forms of cyber power are more potent. David J. Betz and Tim Stevens' conceptualization of productive cyber power, meaning the ability to create and disseminate ideas and affect discourse, can offer significant cognitive effects usable for states.[88] Similarly, John Arquilla and David Ronfeldt's concept of netwar, or cultural conflict on a societal level using cyber tools, was much more conceptual than policy-prescription when it was written, but the idea offers other avenues for gaining influence or affecting political or strategic change.[89] Netwar and similar concepts of information warfare should be further studied. Only then will a more detailed picture of cyber power emerge.

Future research

When discussing cyber security, the discussion is usually focused on possibilities. The questions of how one can be attacked and how one can attack usually form the focal points of the debate. These are important questions, but any discussion of 'how' is meaningless without answering the 'why'. While it is beyond the scope of this paper, the political context of cyber conflict is vital to the understanding of cyber security. For instance, power diffusion suggests some implications for operational cyber power, such as more actors being able to execute certain operations in cyberspace, but the strategic implications for cyber power are more unclear. Even if smaller states or non-state actors should circumvent the resource requirements outlined above, there is still the risk of escalation. Any operation conducted against a more powerful opponent would have to be executed in a way that avoids the risk of escalation into kinetic war or significant diplomatic or economic sanctions. States wishing to conduct such operations would have to anticipate with a high degree of certainty the opposing state's reaction to such events. In other words, the diffusion of power in cyberspace does not suspend the laws of Clausewitz. Malicious ac-

88 Betz and Stevens, *Cyberspace and the State*, 50.
89 John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, California: RAND Corporation, 1996), http://www.rand.org/pubs/monograph_reports/MR789.html.

tivity will happen in a political context, whether the attacking actor intends this or not, and runs the risk of retaliation. Corporations do not start wars, and states do not purposefully ignore their own survival.

Therefore, developments in cyber security should be further discussed in the context of existing international relations theories. The implications the information revolution has had and will continue to have on international security remain largely unexplored, but there are clearly relevant questions to be asked. One obvious question is whether the development of more sophisticated cyber weapons and continued societal vulnerability related to cyberspace will increase the risk of international conflict. This is not to say that cyberspace will create necessarily conflict, but proliferation and digital arms races can trigger escalation in diplomatic conflicts or cause security dilemmas. Proponents of offense-defense theory would perhaps contend that cyber weapons can have this effect, given their general offense-dominance, but recent work by Keir Lieber would suggest that this would not be the case.[90]

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, but much work remains.[91] 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. As Martin C. Libicki wrote in 1995, "Because to judge what otherwise sober analysts choose to include as information warfare—such as hacker warfare or esoteric

90 For more on offense-defense theory, 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*; Charles L. Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?," *International Security* 22, no. 4 (Spring 1998): 44–82. For criticism of offense-defense theory, see Kier A. Lieber, *War and the Engineers : the Primacy of Politics over Technology* (Ithaca: Cornell University Press, 2005). 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): 174–194.

91 Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (December 2009): 1155–1175; Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Abingdon: Routledge, 2008).

versions of psychological warfare—the range of what can be included in its definition is hardly limited by reality..”[92]

92 Libicki, *What Is Information Warfare?*, 81–82.