Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security

Hans-Inge Langø

Norsk Utenrikspolitisk Institutt
Norwegian Institute of International Affairs

NUPI Working Paper 820

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

Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security

Hans-Inge Langø

Abstract

Much has been written on the subject of cyber security over the past two decades, but there remain significant shortcomings in the literature. Cyber security is a field filled with fundamental conceptual, theoretical and empirical disagreements, making any systematic analysis of cyberspace difficult. This paper seeks to categorize the various approaches, here referred to as schools of thought, to cyber security and identify the sources of their disagreements. Much of the academic and policy debate has revolved around the "revolutionist" and "traditionalist" schools of thought, with debates over cyberwar and the efficacy of strategic information warfare. However, none of the schools offer a systematic approach to understanding the strategic utility of cyberspace. This paper identifies a third, less known approach that is best described as "environmentalist." The "environmentalist" school's approach to cyber power and analysis of cyberspace as a distinct environment or system offers the best way forward for the field.

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. 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

Since the rise of cyber security as a prominent policy issue in the early 1990s, the overarching question has been: "What is the role of cyber security in international relations?" Government officials, policymakers, and academics have tried to define the utility of cyberspace as both a weapon and an arena for conflict. This question is two-fold: how can "we" use cyberspace to our advantage? and how can "our" opponents use cyberspace to their advantage?

In essence, the object of analysis is power: *cyber power*. However, answers to these questions are clouded by significant uncertainty around the nature of information technology, how it will be used in society in the future, and how actors can leverage the technology and its accompanying vulnerabilities to achieve political goals. The result of this uncertainty, fueled by a lack of empirical data, is that there is little common understanding of the conceptual and theoretical nature of cyberspace as it relates to security.[1] There is a growing body of scholarly work dedicated to cyber security, but much of it has been policy-oriented, overly technical, or both. The remainder of the field is characterized by differing approaches and competing views on concepts as well as empirics—none offering any systematic and comprehensive understanding of cyberspace as a tool of power.

This paper discusses the various schools of thought on cyber security and what they offer for understanding cyber power. The main conflict lies between what in this paper are classifies as the Revolutionist and Traditionalist schools of cyber security. Adherents of these schools differ strongly on how information communications technology (ICT) may change conflict, and what kinds of actions are both possible and plausible through cyberspace. Briefly put, the Revolutionists hold an expansive view of the impact of ICT, claiming that it can change the character, if not the nature, of warfare. Traditionalists, by contrast, are skeptical to these claims, with some saying that the prospects of extensive cyber conflict have been exaggerated. These two schools do not share a common conceptual idea of cyberspace and cyber conflict, making it difficult to synthesize some kind of overarching theory. What this paper aims to do is to identify the core ideas represented in these competing views, illustrate the conflict in conceptual and empirical terms, and offer a more productive way forward for the field. That

[1] For various reasons, there are simply not enough data available for testing hypotheses adequately. Many CNOs are not disclosed or adequately measured in terms of origins and motives, and government capabilities and vulnerabilities are generally kept classified.

suggested framework draws on a third approach: the Environmental school. The primary objective of the texts that comprise the Environmental school of cyber security is to address cyber power, either implicitly or explicitly. By analyzing cyberspace as a distinct environment, they go beyond purely military or state-centric analysis, and offer a more comprehensive way of approaching cyber security than the two other schools. However, the Environmental school has not yet offered a systematic framework of analysis, so this paper will synthesize the various texts and define theory gaps that need to be filled.

While the primary aim of this working paper is to bring clarity to an academic debate, there are also implications for the ongoing debate about cyber policy. Much of the Traditionalist literature has in fact attempted to link theory with practice, though it has some shortcomings that will be discussed later on in the paper. Scholars like Thomas Rid have criticized the theoretical and conceptual underpinnings of the Revolutionists by examining what is practically possible in cyberspace. Rid argues that extensive cyber warfare is unlikely to occur, given the nature of cyberspace and cyber weapons, and that cyberspace is more suited for other kinds of military operations, like espionage, sabotage and subversion.[2] This is an issue of direct policy relevance because it concerns how states can utilize the digital environment to pursue political objectives.

This paper begins by examining the oldest school of cyber security, the Revolutionist school, based largely on texts written in the infancy of the information revolution. To illustrate the core ideas of this school, I present some selected central texts, showing how these ideas have influenced current thinking on cyber policy, the potential for cyberwar in particular. The next section presents the Traditionalist school. This school is largely defined by its function as a corrective to the more expansive claims of the Revolutionists, so many of its core texts and ideas have been written in response to Revolutionist thinking. As that debate is still ongoing, this section will also cover texts that criticize the Traditionalist approach. These critiques usually attempt to find a middle way between the two schools, without offering an inherently new approach to the study of cyber security. However, as we will see, the third school does offer that new approach. What can best be described as the Environmentalist school has not played a prominent part in the academic debate, but it offers the best potential for a systematic framework of analysis for cyber security. However, it is an incomplete approach, so this section will synthesize its various texts and suggest possible ways forward. The final section of this working paper summarizes the findings of the literature review and

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

discusses what ideas and concepts from the three schools can be included in a more systematic framework. I also suggest some agendas for future research, and discuss how possible changes in the technology and in its use might affect the ideas presented.

The Revolutionists

The Revolutionist school of cyber security is represented by a wide range of texts. As several of these were written in the formative years of the information revolution, they have to a certain extent defined how cyber security is understood today.[3] It is therefore important to consider the historical roots of this field. As we will see, the Revolutionist school includes two overlapping approaches to cyber security. The first, and oldest, is traditional in its approach, as it focuses on military-to-military operations and either kinetic effects or disruptive effects similar to electronic warfare. While this approach was maturing in places like the Pentagon, a second approach surfaced, one that was more holistic in examining the potential marriage of technology and organization. Whereas the two approaches may differ as to the subject of analysis (military versus societal structures) and purpose (empirical analysis versus conceptual development), both seek to identify the potential for cyber warfare in a strategic context. Moreover, the entire school of Revolutionist thinking is marked by an expansive, optimistic view of the role of technology in conflict—with some even claiming that new technology will change the very nature of war.

The idea of waging war against and through computer systems is nothing new. Even though most of the literature on cyber warfare has appeared in the past two decades, the vulnerabilities associated with

---

3 The following texts are considered to be part of the revolutionist school. Some texts overlap with other schools, while some authors listed here, such as Martin C. Libicki and Gregory J. Rattray, moved on to other approaches with their later works. See: Thomas P. Rona, "Weapon Systems and Information War" (Office of the Secretary of Defense, July 1, 1976); Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon* (Washington, DC: National Defense University, March 1994), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA278484&Location=U2&doc=GetTRDoc.pdf; Roger C. Molander, Andrew Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND Corporation, 1996), http://www.rand.org/pubs/monograph_reports/MR661.html; John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND Corporation, 1996), http://www.rand.org/pubs/monograph_reports/MR789.html; George J. Stein, *Information Attack: Information Warfare In 2025* (Montgomery, AL: U.S. Air War College, August 1996); John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997); Buard Q. Clemmons and Gary D. Brown, "Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction," *Military Review* 79, no. 5 (October 1999): 35–45; Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001); Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Weidenfeld & Nicolson, 2005); Phillip S. Meilinger, "The Mutable Nature of War," *Air & Space Power Journal* 24, no. 4 (2010): 24–30; Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option"?* (Washington, DC: Center for Strategic and Budgetary Assessments, August 24, 2012), http://www.csbaonline.org/publications/2012/08/cyber-warfare-a-nuclear-option/; John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies* 36, no. 1 (2013): 101–108.

widespread ICT integration were being discussed well before the spread of the Internet and the personal computer. In 1976, defense analyst Thomas P. Rona coined the term "information warfare" in a report on the potential vulnerabilities of US weapons platforms that had become reliant on computer systems.[4] I f someone could manipulate or disrupt the processes controlling these platforms, Rona noted, that actor could keep the weapons from receiving launch commands. That would have implications for defense as well as offense: the United States could be the target of such operations, but could also exploit similar vulnerabilities in Soviet systems.[5] As the Cold War persisted, Pentagon analysts continued working on the concept of information warfare throughout the 1980s.[6]

Although the Soviet Union dissolved, fears of ICT-associated vulnerabilities did not recede. In the 1990s information warfare was being discussed in a strategic context. A 1996 RAND report described the concept of Strategic Information Warfare (SIW). It was primarily military in nature, and the report argued that the United States and a range of other countries had grown so dependent on ICT that computer network attacks (CNA) against these networks could have strategic effect.[7] Cyber warfare was thus elevated, at least conceptually, to the same level as other forms of strategic warfare. Cyber power was then (and still is) compared to strategic air power, but other authors have also characterized cyber tools as potential, albeit indirect, weapons of mass destruction.[8]

Published a few years later, Gregory J. Rattray's *Strategic Warfare in Cyberspace* is arguably the most influential book on SIW.[9] Rattray draws several parallels between the rise of strategic air power in the 1930s and 1940s and the possible use of cyberspace as an arena for strategic warfare, a concept that he calls "Strategic Information Warfare" (SIW).[10] Rattray rejects "the assumption that strategic information warfare should be treated as a completely new phenomenon because of the 'virtual' or nonphysical nature of operating in the cyberspace environment," because "[c]yberspace is…actually a *physical*

4 The concept of information warfare, as used by Rona, is more or less identical with the concept of cyber warfare, meaning the aggressive use of computer network operations to disrupt, degrade or destroy an opponent's networks.
5 Rona, "Weapon Systems and Information War."
6 Bruce D. Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century* (New York, NY: Free Press, 2003), chap. 4.
7 Molander, Riddile, and Wilson, *Strategic Information Warfare: A New Face of War*.
8 Clemmons and Brown, "Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction."
9 Rattray, *Strategic Warfare in Cyberspace*.
10 Technically, Rattray's comparativist approach falls under the Environmentalist school, but will be used here to illustrate thinking on SIW. Further discussion of the merits of the comparitivist approach is presented in section on the Environmentalist school.

domain resulting from the creation of information systems and networks that enable electronic interactions to take place."[11]

As regards digital warfare, Rattray distinguishes between three types of attacks: mechanical, electromagnetic and digital. He describes the first as attacks on physical infrastructure; the second type involves the use of electromagnetic pulse and jammers to disrupt or destroy electronic components and transmissions. Neither of these two is directly relevant to our discussion here, but the third one is directly applicable. Digital attacks may come in a wide range of forms, and include network-based attacks on other networks—computer network operations (CNO).[12]

According to Rattray, SIW can be conducted in either a physically violent or a nonviolent way. Even if a digital attack does not cause damage or shed blood, that does not mean it does not constitute a use of force. In fact, Rattray argues, "the achievement of political objectives may not require the actual use of violent means. The use of nonviolent digital attacks to achieve political objectives must be understood as part of a new form of warfare."[13] He refers to digital warfare as a type of microforce that can cause significant amounts of damage, despite the low level of energy expended:[14]

> Compared to other types of military force, digital warfare represents a type of microforce. The distinction is analogous to the difference drawn between conventional military forces employing chemical explosives or kinetic energy as their primary means of achieving effect versus the megaforce unleashed by nuclear weapons based on the fission or fusion of atoms. At issue here is the amount of energy unleashed by a given weapon at the time of attack. Weapons across the micro-conventional-mega force spectrum can all cause very significant impacts. *Chemical or biological weapons are referred to as weapons of mass destruction, not because of the amount of destructive energy released when they are deployed but because of the number of deaths they can cause*. Large-scale conventional use of force, such as the bombings of Tokyo and Dresden in World War II, has caused massive damage. Despite the microforce nature of information attacks, disruption of the digital control systems of a nuclear power plant could cause similarly large-scale effects.[15] (emphasis added)

Using nuclear power plants as an example is reductive and the focus on deaths belies Rattray's previous point on nonviolent use of force, but his observation that secondary effects of digital attacks can cause damage is important. Shutting down a network in and of itself is of minor importance; the potential for paralyzing economies or societal functions is of significant importance. The key point here is the poten-

11 Rattray, *Strategic Warfare in Cyberspace*, 17.
12 Rattray, *Strategic Warfare in Cyberspace*, 17–18.
13 Ibid, 20.
14 Ibid, 20.
15 Ibid, 20.

tial for coercion and achieving political objectives; whether that happens through killing the population or inflicting serious economic or other nonmaterial damage is largely irrelevant. However, as Rattray himself admits, the "microforce potential of digital information warfare is as yet unclear."[16]

Information revolution

While the concept of SIW depicted new types of military operations and targets, its focus on kinetic-like effects was largely traditional. Other scholars sought to reveal the broader implications of the information revolution underway, including, but not limited to, computer network attacks. This came with the debate on cyber security in the 1990s, when speculation about the potential for cyber power was debated through the prism of the Revolution in Military Affairs (RMA).[17] Together with the concept of SIW, much of Western thinking and the scholarship of recent years can be traced back to those initial texts.[18]

At the forefront of this debate were John Arquilla and Don Ronfeldt, who wrote extensively about how the information revolution would revolutionize the way the military would wage war. This revolution would not be limited to new tools, the purely technological aspect, but would also encompass organizational changes enabling a more coordinated and efficient military. In 1993, Arquilla and Ronfeldt indicated that, in the future, "warfare is no longer primarily a function of who puts the most capital, labor and technology on the battlefield, but of who has the best information about the battlefield."[19]c They elaborated on this concept, stressing that the information revolution had the potential to transform the way the military is organized and operates. We should keep in mind Arquilla and Ronfeldt's expansive use of the concept of information warfare when examining their ideas. They do not use the term "information warfare," but terms with the "cyber" prefix, with reference to its Greek root *kybernan*, meaning to steer or govern. Thus, the prefix implies a form of "control warfare" that encompasses control not only of one's own organization but of the opponent's as well, through the control, use or manipulation of infor-

16 Ibid, 22.
17 Colin S. Gray distinguishes between an information RMA and a cyberwar RMA. See: Gray, *Another Bloody Century: Future Warfare*, 105. For a discussion of the intersection of information systems and organization in the military to enable greater, speed and precision, see William A. Owens, "The Emerging System of Systems," *Military Review* 75, no. 3 (June 1995): 15–19.
18 Chinese and Russian schools of thinking on cyber security differ substantially from Western thinking, but that is a topic beyond the scope of this paper.
19 John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 1997), 23.

mation.[20] Arquilla and Ronfeldt then go on to create two distinct terms: *netwar* and *cyberwar*. The former is described thus:

> Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may include public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote a dissident or opposition movements across computer networks.[21]

As these authors would later clarify, netwar is distinct from cyberwar by being "normally about low-intensity conflict (LIC) and operations other than war (OOTW—a broader concept than LIC that includes peacekeeping and humanitarian relief operations)."[22]a Given both its form (asymmetrical, non-hierarchical, and probably non-violent) and function (societal change), netwar can be seen as a hypothetical continuation of traditional *Kulturkampf*. Thomas Rid and Marc Hecker have come up with a related concept, "War 2.0," to describe the role of media operations and information technology in asymmetrical conflict. While it encompasses public affairs, psychological operations, public diplomacy and information operations, "War 2.0" should be seen as a subcategory of netwar.[23]

In a military context, the aim of netwar is to manipulate the opponent's decisionmaking processes. According to George J. Stein, by conducting information or computer network operations, the opponent may be positioned "in space and time, by his own decision, in a fatally disadvantageous strategic situation." [24] Further: "Information attack is not so much perception management as orientation management. Information is both the target and the weapon: the weapon effect is predictable error."[25] As such, command and control warfare and CNO are means to an end—technological tools used to achieve cognitive effects on the strategic level.

---

20 Arquilla and Ronfeldt, "Cyberwar Is Coming!," 57–58, endnote 7.

21 Ibid., 28.

22 John Arquilla and David Ronfeldt, "The Advent of Netwar," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 1997), 275.

23 "Netwar" is a broader term meant to encompass whole societies, while "War 2.0" can simply mean one insurgent group, politically motivated, fighting government forces or forces intervening from the outside. "War 2.0" is a way of fighting war, but in an asymmetrical setting. See Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age* (Westpost, Connecticut: Prager Security International, 2009).

24 Stein's use of key terms is somewhat confusing. He uses "netwar" as analogous to information warfare, and places "cyberwar" as the operational level of information warfare, but his focus on military operations is perhaps more fitting of Arquilla and Ronfeldt's "cyberwar" term. Stein, *Information Attack: Information Warfare In 2025*, iv.

25 Ibid.

Let us now turn to Arquilla and Ronfeldt's definition of cyberwar. In their 1993 article, it is defined broadly as encompassing organization, doctrine and technology:

> [C]onducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture…It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the "balance of information and knowledge in one's favor, *especially if the balance of forces is not*. It means using knowledge so that less capital and labor may have to be expended.[26] (emphasis added)

The basic idea behind Arquilla and Ronfeldt's concept, and thus its link to the RMA debate, is the translation of nonmaterial factors into material gains. How do "we" use information and information systems to defeat an opponent when we need to do this cheaply or have no other options, due to imbalance in resources? As the authors stress, cyberwar "should not be confused with past meanings of computerized, automated, robotic, or electronic warfare."[27] To them, it is a broader concept that encompasses technology but also much more than that. The marriage of organization, doctrine, and technology can transform warfare, and even war itself. Information is the key here: how to obtain it, and how to use it. As Arquilla and Ronfeldt write, "[i]f information is a veritable physical property, then in the information age winning wars may depend on being able to hurl the most information at the enemy, while safeguarding against retaliation."[28]

Though much of what they write is speculative, Arquilla and Ronfeldt draw on historical examples such as *Blitzkrieg* and Mongol warfare to show how the information revolution might further change warfare. One of their proposals is a doctrine based on swarming: "when the dispersed nodes of a network of small (and also perhaps some large) forces can converge on an enemy from multiple directions, through either fire or maneuver." As they describe swarming, "[t]he overall aim should be *sustainable pulsing*—swarm networks must be able to coalesce rapidly and stealthily on a target, then dissever and redisperse, immediately ready to recombine for a new pulse."[29]

The material value of information is fundamental to the RMA thinking, and others have presented concepts stressing the informational

---

26 Arquilla and Ronfeldt, "Cyberwar Is Coming!," 30.
27 Arquilla and Ronfeldt, "Cyberwar Is Coming!," 30.
28 John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp--Section 1," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 1997), 158.
29 John Arquilla and David Ronfeldt, "Looking Ahead: Preparing for Information-Age Conflict," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND Corporation, 1997), 465.

and organizational impact of cyberspace. Martin C. Libicki coined the term "Mesh" in a 1994 article to describe the use of information on the battlefield, and particularly the utility of extensive sensor networks. Mesh, according to Libicki, "points to the holes; as information technology places a finer mesh atop the battlefield, more objects are caught in it."[30] The concept is based on the assumption that the United States will not fight a war against a peer rival, but instead fight against an opponent with underdeveloped informational capabilities that seeks to "create as many casualties as possible in hopes that the United States would be dissuaded from further pursuit."[31] The Mesh strategy would then offer the United States the ability "to control the battlefield to the greatest possible extent so as to minimize exposure and casualties."[32] As with swarming, the Mesh is facilitated by technology and is probably contingent on the information revolution. Computer networks and sensors enable, and illuminate, organizational and doctrinal change—but they remain a means to an end.

Alarmism

The group of scholars described above can be described as "revolutionists." This does not imply uniform agreement as to the mechanics of cyber conflict, but the two groups share a fundamental view on the implications of cyberspace in security—that the information revolution is, or has the potential for, changing warfare, and possibly war itself. This basic idea of a revolution in warfare has been adopted by many in the policy community, leading to what can only be described as hyperbolic predictions on the destructive potential of cyberspace.[33] While the object of this paper is not to analyze policy per se, the policy and discourse implications of revolutionist ideas have a direct bearing on our discussion of the Traditionalist school, so a brief description is in order.

---

30 Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, 3.

31 Ibid, 24.

32 Ibid, 24.

33 For more on the issue of threat inflation in cyber security, see Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Abingdon: Routledge, 2008); Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard National Security Journal* 3, no. 1 (April 2011): 39–84; Sean Lawson, *Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History*, Working paper (Fairfax, VA: Mercatus Center, January 2011); Gary McGraw and Nathaniel Fick, "Separating Threat from the Hype: What Washington Needs to Know About Cyber Security," in *America's Cyber Future: Security and Prosperity in the Information Age: Volume II*, ed. Kristin M. Lord and Travis Sharp (Washington, D.C.: Center for a New American Security, 2011), 43–53, http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf; Erik Gartzke, *The Myth of Cyberwar*, Working paper, December 7, 2012; Diego Rafael Canabarro and Thiago Borne, *Reflections on The Fog of (Cyber)War*, NCDG Policy Working Paper (Amherst, Massachusetts, March 1, 2013).

For quite some time policymakers, and some analysts, have warned of a potential "Cyber Pearl Harbor" or "Cyber 9/11."[34] Andrew F. Krepinevich has described the former as involving some sort of complex cyber attack, possibly against critical infrastructure, which "would likely generate a similar sense of shock [as the attack on Pearl Harbor]. However, just as the attack on Pearl Harbor did not inflict a decisive blow to the United States, neither is a surprise massive cyber attack likely to do so."[35] Others have gone even further in ascribing destructive qualities to cyber weapons. In his confirmation hearing, Secretary of State John F. Kerry called the challenges associated with cyber security "the 21st century nuclear weapons equivalent," while former Secretary of Defense Leon Panetta in 2012 warned that a series of cyber attacks aimed at the national critical infrastructure "would paralyze and shock the nation and create a new, profound sense of vulnerability."[36] This imagery is used to underscore the significant challenges and potential threats associated with cyber security. In a much-cited 2010 *Foreign Affairs* article, former Deputy Secretary of Defense William J. Lynn III laid out the challenges the US military faces related to cyberspace, including the dominance of offensive warfare, a lack of credible deterrence and extensive vulnerabilities.[37] This all adds up to a high level of uncertainty, as regards both the threats and their potential effects.

Related to this, policymakers, analyst and the media also use the term *cyberwar* quite liberally.[38] This term is frequently used as a catch-all for all kinds of extensive cyber operations and conflict, ranging from organized cyber-espionage to attacks against critical national infrastructure (CNI). It is *not* applied in the way Arquilla and Ronfeldt use it to describe a form of warfare; nor is it used to describe a stand-alone conflict in cyberspace, as a narrow definition of the term would suggest. It is used to refer to an ongoing cyber conflict, but with more vivid and urgent language.
'

34 Leon E. Panetta, "Defending the Nation from Cyber Attack" (presented at the Business Executives for National Security, New York, NY, 2012), http://www.defense.gov/speeches/speech.aspx?speechid=1728; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York, NY: Ecco, 2010).

35 Krepinevich, *Cyber Warfare: A "Nuclear Option"?*, iii.

36 John F. Kerry, *Nomination: U.S. Senate Committee on Foreign Relations* (Washington, D.C., 2013); Panetta, "Defending the Nation from Cyber Attack."

37 William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (October 2010): 97–108.

38 Arquilla and Ronfeldt, "Cyberwar Is Coming!"; Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*; 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.

While the policymakers and analysts who use these terms rarely refer explicitly to texts from the Revolutionist school, their ideas seem strongly influenced by this school's expansive view, and particularly SIW. They share the Revolutionist idea that society is growing increasingly dependent on ICT and thus vulnerable to disruption. Furthermore, they hold that the allegedly low costs of entry into cyberspace mean that more states and non-state actors are capable of committing malicious actions in cyberspace as opposed to in the traditional domains of military power. [39] However, by failing to take into account the caveats on cyber power noted by Arquilla and Ronfeldt and others, these policymakers and analysts leave themselves open to criticism.

39 The US national security apparatus has warned that an increasing number of actors, including non-state ones, are capable of launching attacks in cyberspace. See U.S. Department of Homeland Security, "The National Strategy to Secure Cyberspace," February 2003; "Department of Defense Strategy for Operating in Cyberspace" (U.S. Department of Defense, July 2011), http://www.defense.gov/news/d20110714cyber.pdf; 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, DC, 2013).

The Traditionalists

It might seem that the "revolutionists" have successfully defined the debate over cyber security. However, there is a strong and growing opposition to the expansive view of cyber security.[40] This trend can best be described as the "traditionalist" school of cyber security. The name does not imply backwardness or rejection of changing circumstances, but a reluctance to discard existing concepts, doctrines and policies prematurely. This school is fundamentally defined by its skepticism concerning the effects of the information revolution on international security and relations, but should also be understood as a direct reaction to the ideas put forth by revolutionists, or more precisely, their alarmist offshoots. Most of the traditionalist literature has emerged in recent years as the public debate over cyber security and policy has gained momentum, but critical texts date further back.

An early example of scholarly work critical to "revolutionist" thinking on cyber security is Martin C. Libicki's *What is Information Warfare?* from 1995. Libicki tackles the issue of information warfare head-on, dismantling and examining the various components of the concept. His work can give clarity to our discussion, and offers the closest thing we have to an authoritative and succinct definition of the core concepts discussed in this paper. "Information warfare, as a separate technique of waging war, does not exist," he writes, adding: "[t]here are, instead, several distinct forms of information warfare, each laying claim to the larger concept."[41] One of these forms is cyber warfare, while some of the other forms show how ICT can assist other, more traditional military or covert operations.[42] For instance, ICT can im-

---

40 For examples of traditionalist writing, see Martin C. Libicki, *What Is Information Warfare?* (Washington, DC: National Defense University, 1995); Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century*; David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (New York: Frank Cass, 2004); Dorothy E. Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?," *IO Journal* 1, no. 1 (2009); Jean-Loup Samaan, "Cyber Command: The Rift in US Military Cyber-Strategy," *The RUSI Journal* 155, no. 6 (2010): 16–21; Brito and Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy"; Lawson, *Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History*; Gartzke, *The Myth of Cyberwar*; 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; Rid, "Cyber War Will Not Take Place"; Thomas Rid and Peter McBurney, "Cyber-Weapons," *RUSI Journal* 157, no. 1 (2012): 6–13; Canabarro and Borne, *Reflections on The Fog of (Cyber)War*.

41 Martin C. Libicki, *What is information warfare?* (Washington, D.C.: National Defense University, 1995), x.

42 The seven forms are: command-and-control warfare (C2W), which aims to strike at the opponent's figurative head and neck; intelligence-based warfare (IBW), which occurs when intelligence is fed directly into operations, targeting, and battle-damage assessment; electronic warfare (EW), which includes the use of EMPs, jammers, and cryptography aimed at radar and communications systems; psychological warfare, which can be di-

prove intelligence-based warfare by enabling greater collection of information and better facilitation of communications; while electronic warfare has been gaining more prominence not because of cyber tools, but because the greater use of ICT means a greater range of possible targets.

Of all the forms listed by Libicki, only economic information warfare and cyber warfare can be deemed new concepts, although Libicki questions the utility of both. Economic information warfare would be a form of information blockade or information imperialism, but the concept is both unproven and conceptually hard to imagine working. Cyber warfare is the most relevant for this discussion, but also the most problematic, according to Libicki. It is "clearly the least tractable because by far the most fictitious, differing only in degree from information warfare as a whole."[43] Under the broad rubric of cyber warfare, there are four categories of attacks: information terrorism, semantic attacks, simula warfare and Gibson warfare. Terrorism needs no further discussion at this point. Semantic attacks mean systematically planting false information in another network. Simula warfare simply means simulated conflict on a computer network to determine the outcome of a conflict without actual conflict. As Libicki notes, this is akin to laser tag or war gaming[44] —a marginal issue at best. It is the fourth category that is most applicable to this discussion. The term "Gibson warfare" is a reference to William Gibson's *Neuromancer*, [45] which introduced the term "cyberspace." As to why he brings up Gibson's novel, and the Disney movie *TRON*, Libicki explains:

> Because to judge what otherwise sober analysts choose to include as information warfare—such as hacker warfare or esoteric versions of psychological warfare—the range of what can be included in its definition is hardly limited by reality.[46]

Libicki concedes that the scenarios of science fiction are possible, but will not be relevant for national security anytime soon. This is the crux of the traditionalist argument: while the theoretical potential for cyber warfare, and specifically SIW, exists, it is improbable at present and unlikely in the future. Libicki's skepticism is grounded in two assertions, one of concept and one of empirics. The former concerns imagination, though grounded in reality, which is stretched considerably to discuss the prospects of such warfare. The latter is simply a lack of empirical data showing the capability to conduct such warfare, or at least show a somewhat reasonable hypothetical scenario for that to

---

rected at the national will, opposing commanders, opposing troops, or in a cultural conflict; hacker warfare, which includes network attacks against civilian targets, but not military ones; economic information warfare, like information blockade and information imperialism; and lastly, cyber warfare.

43 Ibid, 75.
44 Ibid, 81.
45 William Gibson, *Neuromancer* (New York, NY: Ace Books, 1984).
46 Libicki, *What Is Information Warfare?*, 81–82.

happen anytime soon. There have been obvious changes to cyberspace in the intervening years since Libicki's book appeared, but the question is whether our empirical foundations have changed to such an extent that we can imagine plausible scenarios of cyber warfare. In recent years other scholars have picked up Libicki's mantle and sought to critique revolutionist thinking with a better empirical grounding.

Taking the "strategic" out of SIW

The fundamental idea behind SIW is that actions taken through cyberspace can have some stand-alone, strategic effect, and may, at the final extreme, constrain conflict to cyberspace alone. Several traditionalists have criticized this particular idea. Erik Gartzke has argued that cyberattacks' lack of physical effects and the inability to conquer ground in cyberspace mean that threats of cyber attacks would not be particularly effective in deterring or compelling an opponent.[47] As such, cyberspace does not have much stand-alone value. The introduction of cyber conflict entails not a narrowing of conflict, but rather a "broadening of the dimensions of warfare."[48]

Jean-Loup Samaan has taken an even more reductionist view. He argues that cyber attack should be considered a subset of offensive operations, "a means of *denial* rather than a means of *punishment*," thus integrating it into a joint analysis of warfare in general.[49] The basis of this conclusion is his analysis of the cyber domain. Samaan implicitly rejects the idea of SIW. In his view, analogies to nuclear warfare and strategic bombing inevitably fall apart. Cyber attacks cannot be compared to nuclear attacks: the former "do[es] not have any direct lethal effect," while the latter "remain[s] the single most destructive asset available." His criticism of the comparison to strategic bombing is perhaps more contentious. Cyber attacks "could resemble air strikes in terms of disruptive effects," Samaan writes, but he adds: "there is little evidence that strategic bombing has ever decisively determined victory."[50] Thus, by logic, the limited coercive power of strategic bombing translates to the cyber domain.[51] This limitation also extends to how people respond to attacks. As Sean Lawson notes, history has shown that "both infrastructures and societies are more resilient than often assumed by policy makers."[52] The implication is that even if an actor were able to launch a large-scale attack, it is questionable whether that

47 Gartzke, *The Myth of Cyberwar*, 30.
48 Ibid.
49 Samaan, "Cyber Command: The Rift in US Military Cyber-Strategy," 16.
50 Ibid., 19.
51 Samaan refers to the works of Robert Pape and Barry D. Watts as representatives of the arguments against and for the utility of strategic bombing and coercion. See: Robert Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996); Barry D. Watts, "Ignoring Reality: Problems of Theory and Evidence in Security Studies," *Security Studies* 7, no. 2 (1997): 115–171.
52 Lawson, *Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History*, 12.

would result in concessions or modified behavior as intended by the attacker.

Given that cyber warfare does not hold much value as a separate form of warfare, Samaan argues that electronic warfare might serve as a better model: "It may be less strategic and more technical, but it is also more relevant."[53] Libicki has made a similar point by arguing that cyberspace is not a war-fighting domain, but rather a technological function.[54] Both arguments are interesting, but do not satisfy our intention of examining the actual utility of cyber warfare. Electronic warfare is relevant in a functional sense, as both seek to disrupt information systems, but there are two major caveats to this: (1) cyber warfare is defined more broadly than being simply disruptive, as it includes the ability to degrade and destroy systems; and (2) cyberspace encompasses much more than military communications systems and radars. Given these caveats, Samaan's article serves as more of a critique of current understanding than as a full-fledged alternative model.

In addition to raising doubts about the effects of cyber-attacks, traditionalists have also criticized the view that the barrier to entry is much lower in cyberspace than in other domains of warfare. While it is cheaper to buy computers and develop malware than investing in traditional military capabilities like bombers and naval warships, the dichotomy is not quite that simple, according to some scholars. Dorothy E. Denning argues that while the threshold for conducting low-level cyber warfare such as DDoS and webpage defacement is low, it is doubtful that CNA can have the equivalent effect of kinetic attacks at a lower cost:[55]

> the effects of cyber-attacks are relatively minor compared to what is achieved with armed forces, especially military operations that lead to the overthrow of governments, seizure of land, and human casualties. The discrepancy may narrow with more sophisticated cyber attacks that affect physical systems, but such attacks are likely to also have higher costs, raising the barriers to entry.[56]

It should be noted that the barrier is not defined solely by one's ability to code effective software. As Thomas Rid and Peter McBurney point out, "developing and deploying potentially destructive cyber-weapons against hardened targets will require significant resources, hard-to-get and highly specific target intelligence, and time to prepare, launch and execute an attack."[57] This distinction between simple attacks and complex attacks is often lost in the discourse, but helps to further il-

53 Samaan, "Cyber Command: The Rift in US Military Cyber-Strategy," 20.
54 Libicki, "Cyberspace Is Not a War-Fighting Domain."
55 Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?".
56 Ibid., 10.
57 Rid and McBurney, "Cyber-Weapons," 11.

lustrate the fact that CNO are defined by their targets, particularly their vulnerabilities and context.

Defining war and warfare

Beyond the empirical and conceptual problems discussed above, scholars in the "traditionalist" camp have criticized what they see as flaws in the theory foundation of the "revolutionist" perspective on cyberspace. The focal point of the discussion is defining war and distinguishing it from warfare—though the traditionalists' criticism cuts much deeper and goes to the core of some revolutionist ideas. Using Clausewitz' writings as a basis, we may say that *war* is a continuation of politics, a form of political violence, intended to compel the opponent to surrender or offer concessions, whereas *warfare* is the set of techniques used to wage war.[58] In the context of cyber security, this well-established definition and distinction has become muddied by lack of conceptual clarity. This problem frequently emerges in the discourse on cyber security. The conflation of CNA and CNE is an oft-repeated mistake, while a poor understanding of the mechanics of cyberspace has led policymakers to underestimate the difficulty and overestimate the probability of catastrophic cyber attacks. Both of these phenomena are emblematic of a conflation of cyberwar and cyber warfare, confusing ways and means with ends. The source of this confusion is beyond the scope of this paper, but it seems probable that the imaginative potential of cyber-attacks has blurred the distinction between war and warfare by keeping the focus predominantly on the technical aspects of cyberspace and ignoring the political context necessary for cyber conflict to occur.[59] As with all other forms of warfare, large-scale CNA operations must serve a political purpose in order to be considered war.

A central text in this discussion, and a central part of the traditionalist school, is a 2011 article by Thomas Rid titled "Cyber War Will Not Take Place." By applying Clausewitz's principles of war to the concept of cyberwar, Rid outlines three criteria for war: (1) all war is violence or potential violence, used to compel your enemy to do your will; (2) an act of war is instrumental, meaning there has to be an end to the war, and not just war for war's sake; (3) and an act of war is always political. With regard to cyber security, he makes an important distinction: whereas traditional acts of war are "usually rather compact

58 The implication of using Clausewitz is that it gives cyberwar a political context and objectives beyond the disruption or destruction of computer networks.

59 This phenomenon of an overly technocratic approach to security is similar to what Russell Weigley has referred to as "the American way of war." As opposed to coercing the opponent to give you what you want through the diplomacy of violence, "the main kind of American strategy…remained the strategy of brute force…" See: Russell Frank Weigley, *The American way of war: a history of United States military strategy and policy* (Indianapolis, Indiana: Indiana University Press, 1977), 475.

and dense," cyberwar can be "a far more complex and mediated sequence of causes and consequences that ultimately result in violence and casualties."[60] Referring to the scant empirical data available on cyber warfare, Rid argues that the events we have seen do not constitute cyberwar: first, the cyber attacks to date have had no possibility of causing physical violence, and therefore do not meet the criteria of violence; second, because of the difficulty attributing actions to actors, the instrumental aspect of the action cannot be proven; and third, much of what has occurred in terms of malicious actions in cyberspace have been criminal acts with no clear political motivation.

Rid uses a narrow definition of the use of force, restricting it to physical violence. This is in line with traditionalist thinking of war that holds that the introduction of technology does not fundamentally alter the nature of war. The nature of war is violent struggle, and this remains constant. As Clausewitz wrote:

> Now, philanthropists may easily imagine there is a skilful method of disarming and overcoming an enemy without great bloodshed, and that this is the proper tendency of the Art of War. However plausible this may appear, still it is an error which must be extirpated; for in such dangerous things as War, the errors which proceed from a spirit of benevolence are the worst.[61]

Phillip S. Meilinger argues that this view is mistaken. While certain military historians and generals, inspired by Clausewitzian thinking, believe that the nature of war is immutable, Meilinger contends, "[they] most seriously err in equating land warfare—specifically, conventional battle as once practiced—with war. This error reflects institutional bias and downplays the role of technology.[62]

According to Meilinger, naval blockades are evidence that technology can change war and make it less bloody:

> The nature of war is mutable. Warfare in the modern world remains deadly and destructive, but it need not be violent or bloody. The fundamental aspect of war in centuries past may have taken the form of sanguinary battles between infantrymen, but that is no longer necessarily the case. Traditional sea warfare, as well as present- day cyber operations, can become enormously deadly and destructive—but neither violent nor bloody.[63]

Meilinger has an important point, but he confuses two concepts: the nature and the character of war. The former is permanent, while the latter is ever-changing. As Colin S. Gray writes, the tools of warf-

60 Rid, "Cyber War Will Not Take Place," 8–9.
61 Carl von Clausewitz, *On War*, eBook Collection (Web: Project Gutenberg, 2006), bk. 1, chapt. 1, sect. 3, par. 1, http://www.gutenberg.org/ebooks/1946.
62 Meilinger, "The Mutable Nature of War," 26.
63 Ibid., 28.

ighting are a secondary matter of detail.[64] What matters is that cyber tools are used in a political context to achieve strategic goals. This is what is meant by the permanent nature of war: it inevitably means using power to impose your will on an opponent. It does not have to involve actual bloodshed, although that is how it has been done historically. It is worth quoting at length why Gray holds that cyber conflict qualifies as cyberwar:

> The answer is twofold. First, war is conducted to serve policy and a political vision that inspires policy, and policy has many instruments with which 'to impose our will on the enemy'. Cyberwar, *in the particular sense of strategic, stand-alone, information warfare operations*, can be seen as a reasonably distinct tool of grand strategy. A country may wage economic warfare also without using force. Coercion can take many forms. Second, cyberwar generally will be a team player to provide more or less direct support for the sharp end of the spear. Even if cyber combat has some stand-alone qualities, still it must occur in the political and strategic context of warfare. In other words, provided we are intelligent in thinking about new military instruments according to their unique natures, a traditional definition of war will not trouble us. Cyber power, and indeed space power in its current, though not future, form, cannot itself apply organized violence, or force. But so what?[65] (emphasis added)

Gray's definition of cyberwar is distinct from Rid's in one important aspect. While Rid sees the use of force in war as violent, instrumental, and political, Gray clearly states that violence is not necessary to constitute an act of force. "Coercion can take many forms," he writes. Fulfilling the other two criteria is hardly impossible, but Rid's article, and the cyberwar debate writ large, is largely about semantics. [66] The debate has been colored by the rhetoric used by the policy community, which means that an explanatory approach to cyber conflict has been neglected.

In the second half of his article, Rid makes an effort, by delineating the usefulness of cyber warfare, and thus attempting to explain the political and strategic utility of cyberspace. According to Rid, there are three forms of cyber warfare—sabotage, espionage, and subversion—none of which amounts to more than "an auxiliary tool that is nice to have."[67] This is a reductive view. Though they may remain rare, destructive, or highly disruptive, CNAs are indeed possible, and might become more frequent as the vulnerabilities and knowledge of exploiting those vulnerabilities increase. Rid seems to equate large-scale CNAs implicitly with cyberwar. In fact, it is possible to imagine cyber warfare aimed at critical infrastructure or command and control systems without it escalating into cyberwar. Even still, beyond a certain

64 Gray, *Another Bloody Century: Future Warfare*, 33.
65 Ibid., 293–294.
66 Sean Lawson, "Cyber War and the Expanding Definition of War," *Forbes*, October 26, 2011, http://www.forbes.com/sites/seanlawson/2011/10/26/cyber-war-and-the-expanding-definition-of-war/?feed=rss_home.
67 Rid, "Cyber War Will Not Take Place," 25.

threshold, conflict in cyberspace is unlikely to remain "out there," as states will resort to other military or political tools to defend themselves or to force compliance. Rid is therefore correct in claiming that cyberspace does not exist in a vacuum, but his assessment of what utility the environment holds is limited by the very small number of cases. Whereas "revolutionists" see possibilities without empirics, "traditionalists" tend to see only as far as the empirics go. This might suffice in other subfields, but cyber security is marked by rapid expansion and uncertain change.

Because of the fundamentally different beliefs about the information revolution and its impact on international security, the debate over the strategic utility of cyberspace is often framed as an either/or proposition. Either cyberspace represents a new way of warfare, with the potential for SIW—or it is simply another tool in the toolbox. While this discussion is fruitful in forcing through conceptual clarity, it does not fully address the current use of cyberspace as an arena for conflict. Understanding the granular qualities of cyberspace will give a better idea of how cyberspace works today and is likely to work in the near future. To achieve this, we must turn to a different approach to cyber security, one often ignored in the larger debate.

The Environmentalists

There is a third school of cyber security, but it has not been as prominent in the academic or policy debate. Whereas the revolutionist school is defined by what might be called technological optimism and the traditionalist school is defined by its skepticism regarding such expansive claims, this third school is defined by its conceptual and empirical approach. I will call this the *environmental* school of cyber security. The school is fragmented and not as complete as the others (largely because it has ambitions to be more systematic), so this section will attempt to synthesize the various texts into a more coherent whole. Despite its flaws, this school offers better chances of developing a systematic framework of analysis for the strategic utility of cyberspace. What defines this approach is its focus on power in the context of cyberspace.[68] While we could call it the "power" school, the texts have a common analytical approach that describes it better: an environmental analysis of cyberspace. In essence, this means that the texts seek to define and measure the inherent characteristics or features of cyberspace as a distinct environment, separate from other domains and greater than the sum of its technological parts. This comprehensive approach offers the potential for a better understanding of cyberspace than the often parochial or speculative approaches of the two other schools.

---

68 For discussions on cyber power, see: Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 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, DC: National Defense University Press, 2009), 253–274; David Betz, "Cyberpower and International Security," *Foreign Policy Research Institute*, June 2012, http://www.fpri.org/enotes/2012/201206.betz.cyberpower-international-security.html; John A. McCarthy, "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K Wentz (Washington, DC: National Defense University Press, 2009), 543–556; Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 3–23; Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 24–42; Martin C. Libicki, "Military Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 275–284; Stuart H. Star, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 43–87.

Cyberpower

Before discussing the specifics of the environmental school, let us first define what is actually meant by cyberpower. Among the many definitions, we may note that Joseph S. Nye, Jr. defines cyberpower as:

> [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.[69]

The first part of this definition specifies the "what" of cyberpower, while the second part defines the "how." Here we are primarily interested in the latter. Nye gives a succinct definition of what cyberpower means, but it is not sufficiently detailed for our purposes. Let us turn to David J. Betz and Tim Stevens, who have delineated four types of cyberpower: compulsory, institutional, structural and productive.[70] Compulsory power is defined as "direct coercion by one cyberspace actor in an attempt to modify the behaviour and conditions of existence of another."[71] Institutional power means being able to exert influence and affect norms through intermediaries, in this case being international regulatory or governing bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunication Union (ITU). [72] This is an indirect way of achieving political goals, but can help create a beneficial environment, even enhancing structural power by changing the structure of cyberspace to the liking of the state in question. Structural power, as the name indicates, is based on the structural quality of cyberspace and how it created and distributes power. For instance, cyberspace may give oppressed populations in the Middle East and North Africa the opportunity to "network" through the Internet and empower themselves politically.[73] Productive cyberpower as a form of power is more elusive. It refers to "the constitution of social subjects through discourse mediated by and enacted in cyberspace, which therefore defines the 'fields of possibility' that constrain and facilitate social action."[74] Given cyberspace's ability to both "reproduce and reinforce existing discourses, as well as to construct and disseminate new ones,"

69 Nye, *The Future of Power*, 123.
70 David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyberpower* (New York: Routledge, 2011), chap. 1.
71 Ibid., 45.
72 According to Betz and Stevens, for it to be institutional power, "[t]he intermediary institution [cannot be] under the total control of a specific state actor. If it is, it should be considered as an agent of compulsory power." Ibid., 47.
73 Ibid., 48–50.
74 Ibid., 50.

productive cyberpower is in many ways, according to Betz and Stevens, "the foundation for other forms of cyber power."[75]

Together, these four types of cyberpower cover the various ways an actor can leverage cyberspace for political gains. In practical terms, compulsory power would mean the ability to attack or credibly threaten an opponent into making concessions or surrendering, and this would most likely be measured by an actor's CNA capabilities and/or the opponent's vulnerabilities. Institutional power would mean an actor's ability to use IOs to gain influence, whereas structural power defines whether the cyberspace environment is favorable to a particular actor, or not. Lastly, productive cyberpower would probably refer to the ability to create norms of behavior.

Having defined and dismantled the term cyber power, let us move on to how scholars in the environmental school of cyber security have attempted to measure cyberpower.

Comparitivists

Roughly speaking, there are two environmentalist strains. The first of these has been discussed indirectly in the traditionalist section, but deserves a better introduction here. What we are referring to is the use of analogies, as criticized by Samaan earlier. This comparativist approach attempts to draw similarities between cyberpower, understood as a form of military power, and other forms. Here we note the evident similarities with SIW and revolutionist thinking; but the comparitivist approach is best described as an environmental approach, because it attempts to compare the inherent characteristics of cyber power vis-à-vis other forms of military power. Those characteristics are derived from the properties of the cyberspace environment. In his seminal work on SIW, Rattray undertakes a comparative study of cyberspace and the rise of strategic air power in the 1930s, while other works have compared cyberpower to sea power and nuclear power.[76]

The comparative approach is intended to offer something familiar when talking about something new, but this approach is not without pitfalls. Referring back to Samaan's criticism, comparing cyberpower with some other power invariably means examining cyberpower through the lens of understanding of some other form of power. And so we get descriptions of cyberspace or its characteristics that are—at best—almost, but not quite, accurate. Instead of dissecting cyberspace by itself, we find ourselves grasping at commonalities that can be illu-

75 Ibid., 50–51.
76 Rattray, *Strategic Warfare in Cyberspace*; Rattray, "An Environmental Approach to Understanding Cyberpower"; Krepinevich, *Cyber Warfare: A "Nuclear Option"?*.

sory or parochial (the latter being a particular danger, due to the small amount of cases).

A clear example is the persistent comparison with strategic air power. Because cyber attacks can apparently be effectuated anywhere, with little or no warning, coupled with the focus on attacks against critical infrastructure, long-range bombers headed towards the enemy's center of gravity in order to force a surrender may seem an appropriate analogy. However, such a comparison obscures the value and character of cyber attacks. Obviously, the kinetic potential involved is vastly different, but there are other differences as well. Bombs function largely independent of their targets. Fortification or underground facilities can prevent damage, but this can be remedied by scale. Cyber weapons, on the other hand, are defined by their targets and specifically their vulnerabilities. You cannot simply make the worm bigger: each piece of malware must be specifically designed for a certain target for it to be able to exploit an existing vulnerability, and only then can it have an effect. There are many other differences as well. Cyber weapons can have highly unpredictable effects, causing cascade effects throughout systems and across sectors. In that sense, they can be more like biological viruses than bombs—but that is a discussion for another time. Here my main point is that the comparitivist approach has perverse incentives, making it more appealing to look for commonalities than differences.

Mapping the terrain

Others have attempted to avoid this trap. The second strand of the environmentalist school is markedly different, as it approaches cyberspace on its own terms. The characteristics of cyberspace are defined independently before any comparative study is undertaken (which is generally not necessary and is often perfunctory). The texts are not without flaws, but this still represents the most promising approach to the study of cyber security on a strategic level. It is well-suited for systematic studies of cyberspace as a strategic environment, and can better distinguish between the inherent nature of cyberspace and fluctuating trends. Because this strand approaches cyberspace on its own terms, it also forces greater conceptual clarity—avoiding a conflation of terms and ideas.

Not all the texts in this strand of the environmental school have taken a systematic approach to cyberspace, though they all offer some important insights. Nye's work on cyberpower does not address its subject in a granular and comprehensive way, but offers a cogent discussion of what he calls "power diffusion," a consequence of the information revolution. According to Nye, "two types of power shifts are

occurring in this century: power transition and power diffusion. Power transition from one dominant state to another is a familiar historical event, but power diffusion is a more novel process."[77] The latter is relevant to our discussion, as the "information revolution is changing the nature of power and increasing its diffusion."[78] Nye maintains that states will remain the dominant actor, but will face increased competition from new actors, and difficulties in controlling society.[79]

Similarly, the unique nature of cyberspace means some of the traditional concepts of international security and international relations theory do not translate well into the new environment. Martin Libicki has addressed the challenges of deterrence in cyberspace. Although not explicitly focusing on cyberpower, his analysis is based on an environmental analysis of cyberspace. Libicki questions whether "we" (the United States in his text) can hold the opponent's assets at risk, and if so, can "we" do so repeatedly. Because of the imprecise nature of cyber weapons, successful retaliation is not assured, and unforeseen effects may run the risk of escalation.[80] The second issue is the ability to strike repeatedly. Unlike nuclear deterrence, which is singular and symmetric, "[c]yber deterrence has to be repeatable because no feasible act of cyberretaliation is likely to eliminate the offending state, lead to the government's overthrow, or even disarm the state."[81]

While these texts deal primarily with specific phenomena, Rattray has offered a more comprehensive framework of analysis. Picking up on his earlier work on SIW, Rattray wrote in 2009 of an environmental approach to understanding cyberspace and cyberpower. 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.[82] In technological advances, "[t]he rise of digital connectivity will have transformative impacts," but the increase in availability and anonymity creates new vulnerabilities to attack.[83] Not surprisingly, the speed and scope of operations in cyberspace can increase with automation and increased connectedness, but this also benefits non-state actors.[84] When it comes to control of key features, cyberspace is reliant on physical infrastructure, but also governance. The latter comes in the shape of organizations like the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunica-

77 Joseph S. Nye, *The future of power* (New York: PublicAffairs, 2011), 113.
78 Ibid., 114.
79 Ibid.
80 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, California: RAND Corporation, 2009), 52.
81 Ibid, 31.
82 Rattray, "An Environmental Approach to Understanding Cyberpower," 262.
83 Ibid, 264-265.
84 Ibid, 266-267.

tion Union (ITU), whereas the former means assuring the safety (and possibly the control) of choke-points like undersea fiber optic cables.[85] Here, Rattray makes reference to naval power theory, but it is unclear how any country would be able to defend such choke-points effectively.[86] Defending cyberspace would also require a form of national mobilization. Rattray mentions several ways of achieving this, from harnessing the expertise of the private sector, where expertise mainly resides, to a type of whole-of-nation approach encompassing economic, diplomatic and military power.[87]

Rattray's article is one of the most systematic analyses put to paper, but he commits one common error in discussing the strategic features or defining characteristics of cyberspace: he confuses the inherent qualities of cyberspace as an environment, with their security implications. This is a question of causality, as the former defines the latter. For instance, the attribution problem in cyberspace is not an inherent feature, but is the result of cyberspace's malleability and decentralized nature. Any systematic framework of analysis of cyberspace should therefore begin with the inherent, if not permanent, features of cyberspace itself, and from there draw existing or potential security implications. That would make it easier to see what is likely to be the permanent nature of cyber conflict and what is its mutable character.[88]

The main strength of the environmental school of cyberspace is that it strives to provide better understanding of the environment itself, as a whole, and not only certain parochial or temporal issues stemming from it. Still, much work remains to be done. The comparativist strand offers some grounding in the familiar, but increases our understanding of cyberspace only indirectly, and often incorrectly. The second strand of the environmental school offers better potential for understanding cyberspace on its own terms. The works of Nye, Libicki and others on specific phenomena or characteristics do not provide a comprehensive look at cyberspace—but that does not mean these parts cannot be synthesized into a greater framework, like that used by Rattray. While Libicki's work deals explicitly with deterrence, his observations on

85 Ibid, 268-270.

86 Here there is also the issue of stakeholding and interdependence. There are few incentives for countries to attack choke-points because the effects would not be limited to the target country, thus risking diplomatic or military backlash from third-parties.

87 In an attempt to harness civil-society and private-sector resources, Estonia has established a cyber-wing of its paramilitary force, the Cyber Defense League. This volunteer model might not be applicable to larger states such as the United States because of command and control issues, but this is a matter in need of further examination. Alexander Klimburg has written extensively about a whole-of-nation approach to cyber defense and offense (Alexander Klimburg, "The Whole of Nation in Cyberpower," *Georgetown Journal of International Affairs* 11 (2010): 171–179; Alexander Klimburg, "Mobilising Cyber Power," *Survival* 53, no. 1 (March 2011): 41–60.)

88 The present author has drafted a more comprehensive, systematic framework of analysis for understanding compulsory cyber power. See Hans-Inge Langø, *The Limits of Compulsory Cyber Power: Assessing Ecological Potential and Restraints in the Digital Domain*, Working paper (NUPI, June 2013).

the limited effectiveness of cyber weapons, and thus threats, have implications far beyond deterrence. They tell us something about the nature of cyberspace, and should thus be part of any larger analysis.

Conclusions

In recent years, revolutionist and traditionalist thinking on a select few issues has dominated the debate on cyber security. The possibilities of cyberwar and devastating attacks on critical national infrastructure have become perhaps the most common subjects of discussion—yet the sides often seem to be talking past each other, or with a flawed understanding of the issue at hand. That said, these two schools of thought in cyber security have contributed understanding to the strategic utility of cyberspace.

The revolutionist school of cyber security is marked by an inherent optimism: not optimism in the sense that technology can solve problems, but that it will change warfare and perhaps even war itself. Twenty years after John Arquilla and David Ronfeldt's declaration that "Cyberwar is Coming," there remains little evidence to justify their claim. This is partly an issue of semantics, but we are still waiting for the full effects of the information revolution. Much of the revolutionist literature is best seen as concept development, and not empirically based research. Nonetheless, their concepts and ideas are forward-looking and delineate the possibilities of cyberpower. Similarly, Strategic Information Warfare can serve as a warning against society's increased dependence on information communication technology, even though this is a far cry from the types of attacks mentioned by the alarmists.

The traditionalist school has served an important function as a corrective against the more expansive claims of the revolutionists—though both make similar errors of inference. While the revolutionists conclude too much about the impact of ICT, traditionalists have restricted themselves to the very small number of cases, implicitly assuming that the situation is static.

However, cyberspace is anything but static. Considered as an environment, it is both diffuse and malleable—neither of which qualities enables easy analysis. The traditionalist position is thus perfectly understandable for trying to anchor something new to something old, but, as explained in this working paper, cyberspace must be understood primarily on its own terms.

The environmentalist school offers the potential for a more systematic, foundational framework of analysis. The comparitivist strand has limited utility, as it may lead to conceptual confusion, but the more com-

prehensive strand sketched out by Gregory J. Rattray can provide a good start. Coupled with the more in-depth studies of scholars like Joseph Nye and Martin Libicki, as well as insights from computer science studies, this approach can enable a more profound understanding of both cyberspace and its security implications. This is important because what might seem highly alarming today might prove to be a false alarm. Developments in cyber network defense may be able to render threats against critical infrastructure harmless, whereas new and unforeseen threats could emerge through cyberspace. Whatever transpires, this field of security is in flux, and it is imperative for the literature to reflect that fact.