

The Cybersecurity Dilemma

by

Nicholas C. Rueter

Department of Political Science
Duke University

Date: _____

Approved:

Alexander Downes, Supervisor

Peter Feaver

Charles Dunlap

Thesis submitted in partial fulfillment of
the requirements for the degree of Master of Arts in the Department of
Political Science in the Graduate School
of Duke University

2011

ABSTRACT

The Cybersecurity Dilemma

by

Nicholas C. Rueter

Department of Political Science
Duke University

Date: _____

Approved:

Alexander Downes, Supervisor

Peter Feaver

Charles Dunlap

An abstract of a thesis submitted in partial
fulfillment of the requirements for the degree
of Master of Arts in the Department of
Political Science in the Graduate School
of Duke University

2011

Copyright by
Nicholas C. Rueter
2011

Abstract

Scholars have long recognized and debated the effects of the “security dilemma,” where efforts by states to enhance their security can decrease the security of others. The severity of a security dilemma, and the prospects for cooperation under the dilemma, are greatly affected by military technology. In this article, I apply the security dilemma framework to a revolutionary new form of conflict: cyberwarfare. I argue that cooperation over cyberwarfare is made challenging due to the security dilemma, and that the unique characteristics of cyberwarfare make it difficult to break out of this dilemma. The reluctance and failure of states to achieve cooperation over cyberwarfare likely reflects, in part, the constraints of this “cybersecurity dilemma.” Some states have strong incentives, however, to promote limitations on offensive cyberwarfare. Thus, I propose ways in which cooperation may eventually be achieved despite these challenges.

Contents

Abstract.....	iv
I. Introduction.....	1
II. Cyberwarfare	8
Categories and Concepts	8
The World at Cyberwar	14
III. Realism and the Security Dilemma	24
Offensive and Defensive Realism	24
The Security Dilemma	27
Military Technology	30
Cooperation	31
IV. The Cybersecurity Dilemma	35
The Offense-Defense Balance	35
Offense-Defense Differentiation	40
V. Efforts at Cooperation	43
VI. Achieving Cyber Peace	48
Institutions and Norms	48
Technological Developments	53
Organization and Doctrine	54

VII. Conclusion..... 56

References 58

I. Introduction

One of the foremost goals of any state is to protect its citizens from external threats. Given this shared objective, one might expect that cooperation among states to enhance their mutual security would be more common.

However, while peaceful means of enhancing security do exist, the world remains tragically characterized by conflict and strife.

The international system has a number of features that make cooperation difficult. Most important is the prevalence of uncertainty and mistrust. Mistrust of other states is natural, as history has shown that promises of peace and partnership are rarely upheld for long. Interstate diplomacy is plagued by information asymmetry, which makes the true intentions of others perpetually unknown. While many states are satisfied with their place in the international hierarchy and seek only to protect their position, some states endeavor to enhance their security by dominating others, apparently subscribing to the theory that "the best defense is a good offense." Furthermore, the system is plagued by a handful of belligerent state and non-state actors who pursue violence for ideological or other non-security related reasons. Because the

system is anarchic (i.e., there is no common or overarching world government), states must provide for their own security needs. Thus, while states may sincerely engage in diplomatic efforts toward cooperation and peace, they must at the same time guarantee the safety of their citizens by raising and maintaining proficient militaries.

Although a state's purpose in pursuing military power may be purely defensive in nature, other states can never be certain that their adversary's intentions are benign. Many if not most weapons systems, after all, have both defensive and offensive capabilities. Thus, well-meaning states often find themselves in what has come to be known as a "security dilemma," where efforts by one state to enhance its security decrease the security of others. In response, threatened states will seek to improve their own capabilities, resulting in arms racing, diplomatic tension, and sometimes war. The tragedy of the security dilemma is that neither state involved actually desires conflict, but instead wishes only to defend itself from potential aggressors.

The severity of a security dilemma is greatly affected by military technology.¹ Even purely defensive technologies like missile defense systems can exacerbate the dilemma by throwing off the balance of relative security between two adversaries.² Because many of the most effective weapons systems tend to worsen security dilemmas, cooperation between non-aggressive states to reduce the amount or use of these weapons (i.e., arms control) is especially difficult.

Fortunately, cooperation in the face of a security dilemma is not impossible. Under the right conditions, and with proper signaling, scholars have posited that a security dilemma can be “broken.” Where a particular military technology or policy has affected a security dilemma, the potential for achieving cooperation depends in large part on whether: 1) the standoff between two states favors offensive or defensive action; and 2) whether those states’ offensive and defensive weapons can be readily distinguished. Where offense has the

¹ Robert Jervis, “Cooperation Under the Security Dilemma,” *World Politics*, Vol. 30, No. 2 (January 1978), p. 194; Charles Glaser, “Realists as Optimists: Cooperation as Self-Help,” *International Security*, Vol. 19, No. 3 (Winter 1994/1995), p. 62.

² For further discussion of this example, see Ken Booth and Nicholas Wheeler, *The Security Dilemma: Fear, Cooperation and Trust in World Politics* (New York: Palgrave, 2008), p. 51.

advantage, or where it is difficult for adversaries to distinguish between offensive and defensive weapons, the security dilemma will persist and cooperation is unlikely. However, where defense has the advantage, or where offensive and defensive weapons are more easily distinguishable, the security dilemma is reduced and cooperation is possible.³

In what follows, I apply the security dilemma framework to an emerging, controversial, and potentially revolutionary new form of conflict: cyberwarfare. I argue that cooperation over cyberwarfare is made challenging due to the security dilemma, and that the unique characteristics of cyberwarfare make it difficult to break out of this dilemma. At present, it is far easier for a sophisticated cyber attacker to inflict massive damage on a nation's military and civilian networks than it is to defend against such an attack. Furthermore, it is nearly impossible to distinguish between offensive and defensive cyber weapons and cyberwarfare programs. The reluctance and failure of states to achieve cooperation over

³ Jervis, "Cooperation Under the Security Dilemma," p. 187. Some scholars have argued that international institutions can facilitate cooperation even in light of the security dilemma. This argument is discussed in more detail in Part VI.

cyberwarfare likely reflects, in part, the constraints of this “cybersecurity dilemma.”

There is a growing literature on the topic of cyberwarfare. Many authors have addressed technical aspects of cyberwarfare and cybersecurity, providing practical guidance for security experts and potential cyberwarriors.⁴ Others have focused on issues of military doctrine,⁵ government organization and strategy,⁶ and domestic and international law.⁷ But relatively few authors have addressed cyberwarfare in the language of international relations theory. This article

⁴ See, e.g., Jian Wei-Wang and Li-Li Rong, “Cascade-Based Attack Vulnerability on the US Power Grid,” *Safety Science*, Vol. 47 (2009), pp. 1332-1336. This controversial paper proposed strategies to effectively attack the U.S. electrical grid, triggering alarm in the United States Congress and media. John Markoff and David Barboza, “Academic Paper in China Sets Off Alarms in U.S.,” *New York Times*, March 20, 2010.

⁵ See, e.g., Mark D. Young, “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power,” *Journal of National Security Law and Policy*, Vol. 4, No. 1 (2010), pp. 173-196.

⁶ See, e.g., Paul Rosenzweig, “The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence,” in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council (Washington, D.C.: National Academies Press, 2010), pp. 245-270.

⁷ See, e.g., Michael N. Schmitt, “Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts,” in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council (Washington, D.C.: National Academies Press, 2010), pp. 151-178; David E. Graham, “Cyber Threats and the Law of War,” *Journal of National Security Law & Policy*, Vol. 4, No. 1 (2010), pp. 87-102; Sean Watts, “Combatant Status and Computer Network Attack,” *Virginia Journal of International Law*, Vol. 50, No. 2 (2009), pp. 391-447; Charles Dunlap, “Perspectives for Cyber Strategists on Law for Cyberwar,” *Strategic Studies Quarterly*, Vol. 5, No. 1 (Spring 2011), pp. 81-99.

contributes to the discussion by proposing a useful framework through which international relations scholars can understand cyberwarfare and the challenges it poses for cooperation.

Of course, the security dilemma is not the only obstacle making cooperation over cyberwarfare difficult. Efforts are also complicated by problems of attribution (the ability to identify the source of an attack),⁸ verifiability (the ability to confirm compliance with an international agreement),⁹ and definition (e.g., agreeing on what constitutes a “cyber weapon”).¹⁰ While these are daunting practical challenges, they could be overcome through

⁸ “Attribution” refers to the ability to identify the source of an attack. Attribution is especially difficult in the cyber context for a number of reasons, one of which is that many sophisticated cyber attacks are “multi-stage.” For example, an attacker might use their own computer to penetrate another computer, and then use that computer to launch an attack on a target computer. For a more in-depth discussion of this and other attribution challenges, see David D. Clark and Susan Landau, “Untangling Attribution,” in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council (Washington, D.C.: National Academies Press, 2010), pp. 25-40. Still, some have suggested that the attribution problem is less significant than it is usually made out to be. See, e.g., Will Goodman, “Cyber Deterrence: Tougher in Theory than in Practice,” *Strategic Studies Quarterly*, Vol. 4, No. 3 (Fall 2010), pp. 102-135.

⁹ Richard Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), p. 6.

¹⁰ Tom Gjetlen, “Seeing the Internet as an Information Weapon,” *NPR*, September 23, 2010, <http://www.npr.org/templates/story/story.php?storyId=130052701>.

concerted effort. The problem of the security dilemma arises from the very structure of the international system, and thus deserves special consideration.

In Part II, I provide background and context regarding cyberwarfare, cybersecurity, and related concepts. I argue that, while a true “cyberwar” has yet to occur, and while the exact parameters of such a conflict remain unknown, the threat is very real and nations are already taking steps to both carry out and defend against cyber attacks. In Part III, I provide a brief review of the security dilemma literature with an emphasis on the offense-defense variables identified by Robert Jervis. In Part IV, I analyze the concept of cyberwarfare through the lens of the security dilemma and discuss the challenges that the dilemma poses to international cooperation over cyberwarfare. In Part V, I discuss the reluctance of many states, particularly the United States, to pursue cooperation over cyberwarfare. While this reluctance may once have been justified, I argue that powerful states now have great incentives to pursue cooperation over cyberwarfare. In Part VI, I propose ways in which cooperation might still be achieved despite the apparent severity of the “cybersecurity dilemma.” I conclude in Part VII.

II. Cyberwarfare

Categories and Concepts

The term “cyberwarfare” is used loosely by most commentators. This is understandable. The very nature of cyberwarfare is one of innovation and adaptation, and thus any workable definition must be sufficiently broad. To understand what cyberwarfare *is*, however, it is helpful to understand what it is not. Discussions of cyberwarfare are often combined with discussions of “cybersecurity,” “cyber crime,” and “cyber terrorism.” While the boundaries between them are admittedly thin, it is important to distinguish these concepts from one other.

There are essentially four categories of cyber threat, best understood not by the nature of the attack, but by their source and purpose. A cyber crime is simply “a crime committed through the use of information technology” and is usually a concern of law enforcement.¹ Cyber criminals are sometimes hackers motivated merely by the challenge of circumventing security measures.

¹ Lech Janczewski and Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism* (Hershey, Penn.: Information Science Reference, 2008), p. xiv.

Oftentimes, hackers also seek notoriety.² Cyber criminals may also engage in attacks and intrusions for financial gain (by stealing money, intellectual property, confidential business secrets, etc.).³ Cyber criminals sometimes target government servers, but will just as often target private entities. Cyber crime is certainly troubling, but it is not generally a military concern.

A second category of threat is “cyber espionage.”⁴ Cyber espionage is essentially spying for political or military gain. Cyber espionage is probably very common, and is typically a concern of the intelligence community (including the military intelligence community). While cyber espionage may be utilized during warfare, and may at times even be considered a subset of cyberwarfare, it should not be considered warfare in and of itself.⁵

² Kamal T. Jabour, “50 Cyber Questions Every Airman Can Answer,” Air Force Research Laboratory, May 7, 2008, http://www.au.af.mil/au/awc/awcgate/afrl/50_cyber_questions.pdf.

³ Ibid.

⁴ See James Andrew Lewis, “The Cyber War Has Not Begun,” Center for Strategic and International Studies, March 2010, pp. 1-2, http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf.

⁵ Ibid.

Cyber terrorism, like other forms of terrorism, is carried out primarily for ideological purposes.⁶ Cyber terrorists could utilize many of the same methods as other cyber criminals, but their goals would be markedly different. So-called “hacktivism” can be considered a subset of cyber terrorism, although the motives and goals of these activists are not usually as vile as those typically associated with terrorism.

The fourth category of threat is cyberwarfare. Many definitions of cyberwarfare exist, but few achieve the appropriate balance between precision and inclusiveness.⁷ In one of the most popular works on the subject, Richard Clarke, the former Special Advisor to the President on Cybersecurity, defines cyberwarfare as “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.”⁸ Clarke’s definition is sufficiently broad, but correctly identifies the feature that

⁶ In 2009, the Congressional Research Service noted that it was unaware of any reported acts of cyberterrorism. Catherine A. Theohary, “Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues,” CRS Report RL31787, March 17, 2009, p. 8.

⁷ For example, a report by the Air Force Research Laboratory defines cyberwarfare as “the use of information and signals to deliver effects against military systems.” Jabour, “50 Cyber Questions.” This definition is too narrow, as it restricts itself to attacks against military targets.

⁸ Clarke and Knake, *Cyber War*, p. 6. Clarke does not apparently consider physical attacks on network infrastructures, such as attacks on computer servers, to be “cyberwarfare.” While this distinction may be fair, it is important to note that such attacks could result in similarly grave consequences.

distinguishes cyberwarfare from other forms of cyber activity—that it is the domain of states, not petty criminals.

Concern over cyber attacks and cyber intrusions, be they carried out by criminals, terrorists, or other governments, has brought the issue of “cybersecurity” to the forefront of national security debate. While cyberwarfare is a practice (a means to a political end), cybersecurity is often touted as a goal. The United States government has undertaken numerous efforts to bolster the security of its digital infrastructure, both military and civilian.⁹

In U.S. military circles, cyberwarfare activities are referred to as “computer network operations” (CNO).¹⁰ The “defensive” or “security” component of CNO is “computer network defense” (CND). The offensive component is “computer network attack” (CNA).¹¹ CNA encompasses a broad range of tactics including, but certainly not limited to, the spread of

⁹ For example, the 2002 Federal Information Security Management Act gave the Office of Management and Budget (OMB) responsibility for coordinating the information security standards of federal agencies. The Department of Homeland Security has established the Cyber Warning and Information Network (CWIN) to serve as an early warning system for cyber attacks. For more information on these and other examples of federal cybersecurity efforts, see Theohary, “Information Operations, Cyberwarfare, and Cybersecurity,” pp. 20-22.

¹⁰ Young, “National Cyber Doctrine,” p. 7

¹¹ Carole N. Best, “Computer Network Defense and Attack: Information Warfare in the Department of Defense” (USAWC Strategy Research Project, U.S. Army War College, 2001), <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA390581&Location=U2&doc=GetTRDoc.pdf>.

disinformation through an enemy's computer networks, "denial of service" type attacks that prevent Internet sites or services from being utilized, and the planting of "worms" or viruses to disrupt or destroy enemy computer systems. A related activity is "computer network exploitation" (CNE), defined as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."¹² For years, CNO has been recognized by the United States military as a subset of "information operations" — a collection of strategies that seek to "influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."¹³

Perhaps the most distinctive characteristic of cyberwarfare is the battlefield upon which it takes place. Although its effects may be realized in the physical world, cyberwarfare is not conducted on air, land, sea, or space, but rather in a virtual arena called "cyberspace."

Like cyberwarfare, "cyberspace" is difficult to conceptualize. The U.S. Army defines cyberspace as: "A global domain within the information

¹² Young, "National Cyber Doctrine," p. 7, quoting Joint Chiefs of Staff, *Joint Pub. 3-13: Information Operations*, 2006, p. II-5, http://www.fas.org/irp/doddir/dod/jp3_13.pdf.

¹³ Joint Chiefs of Staff, *Joint Pub. 3-13: Information Operations*, p. ix.

environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."¹⁴ The U.S. military has come to understand cyberspace as an entirely new domain or "operational environment" for warfare. As stated in the 2004 National Military Strategy: "The Armed Forces must have the ability to operate in and across the air, land, maritime, space and cyberspace domains of the battlespace."¹⁵ As the Department of Defense explains, "treating cyberspace as a domain establishes a foundation to understand and define its place in military operations."¹⁶

Conceptualizing cyberspace as a discrete domain allows a better understanding of cyberwarfare's significance. Cyberspace is a man-made domain that can be destroyed or damaged by both virtual and physical attacks. One state cannot invade another's cyberspace. It is a domain without geographic or territorial boundaries. As discussed later, these battlefield

¹⁴ United States Army, *Cyberspace Operations Concept Capability Plan 2016-2028*, February 22, 2010, p. 6, <http://www.fas.org/irp/doddir/army/pam525-7-8.pdf>.

¹⁵ Joint Chiefs of Staff, *The National Military Strategy of the United States*, 2004, p. 18, <http://www.defense.gov/news/mar2005/d20050318nms.pdf>.

¹⁶ Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, 2006, p. 3, <http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf>.

properties make cyberwarfare unique and extremely consequential. They also pose unparalleled challenges for international cooperation.

The World at Cyberwar

According to Clarke, nation-states are preparing for, and have already engaged in, cyberwarfare.¹⁷ Former Director of National Intelligence Mike McConnell has stated that: “The United States is fighting a cyber-war today, and we are losing. It's that simple.”¹⁸ Popular media accounts tend to agree, and U.S. military officials have on many occasions confirmed that states have already carried out attacks on U.S. government networks.¹⁹ Still, there are many that contest both the reality and gravity of cyberwarfare.²⁰ As Howard Schmidt, President Obama’s cybersecurity-czar stated frankly: “There is no cyberwar. I think that is a terrible metaphor and I think that is a terrible concept.”²¹

¹⁷ Clarke and Knake, *Cyber War*, pp. 30-31.

¹⁸ Mike McConnell, “Mike McConnell on How to Win the Cyber-War We’re Losing,” Op-ed, *Washington Post*, February 28, 2010.

¹⁹ See, e.g., Lolita C. Baldor, “Pentagon Spends \$100 Million to Fix Cyber Attacks,” *USA Today*, April 8, 2009.

²⁰ See, e.g., Lewis, “The Cyber War Has Not Begun.”

²¹ Ryan Singel, “White House Cyber Czar: ‘There is No Cyberwar,’” *Wired*, March 4, 2010, <http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/>.

Perhaps the most commonly cited incident of cyberwarfare was carried out against the nation of Estonia. In February 2007, the Estonian legislature passed a law requiring the removal of any structure symbolizing five decades of Soviet occupation following World War II. Included among the targeted structures was a large bronze statue of a Red Army soldier in the capital city of Tallinn. After complaints from Moscow, the Estonian president vetoed the law. Public pressure to remove the statue continued, however, ultimately resulting in several violent confrontations between Estonians and ethnic Russians living in the country. In response to these riots, Estonian authorities moved the statue to a more protected location. This move only further irritated Russian critics and provoked a series of attacks against Estonia's highly developed cyber infrastructure.²² For weeks, servers throughout the country were jammed by "distributed denial of service" or "DDOS" attacks, which prevented access to major and minor websites, including online banking, newspaper, and government electronic services.²³

²² Estonia is one of the most wired countries in the world. Theohary, "Information Operations, Cyberwarfare, and Cybersecurity," p. 5.

²³ Clarke and Knake, *Cyber War*, p. 13. In a typical DDOS attack, a hacker penetrates and takes control of a large stock of computers owned by others. The computers are collectively referred to

The government of Estonia petitioned NATO for assistance. With the help of foreign security experts, Estonian authorities traced the attacks back to “controlling machines” in Russia. Finger-pointing ensued, and while the Russian government denied its role in the attacks, it acknowledged that individuals or criminal organizations within Russia, likely provoked by the incident over the Red Army statue, may have been responsible.²⁴

It is possible that the cyber attacks against Estonia were merely acts of cyber terrorism or protest carried out by incensed Russian hackers. It remains possible, however, that the attacks were tacitly condoned, or even expressly approved, by authorities within the Russian government. Either way, the Estonian incident brought the prospect and gravity of cyberwarfare into the forefront of public awareness.

as a “bot-net.” The hacker then instructs those computers to simultaneously flood a targeted system with requests. Although such requests may normally be legitimate, when too many machines make the request at the same time, the targeted server can become overloaded. Because attacks are launched from machines that are not owned by the hacker, it is frequently difficult to identify the original culprit of the attack. Clark and Landau, “Untangling Attribution,” p. 28.

²⁴ Ian Traynor, “Russia Accused of Unleashing Cyberwar to Disable Estonia,” *The Guardian*, May 17, 2007.

Russia again found itself at the center of cyberwarfare allegations during the 2008 Russo-Georgian War. After over a decade of ethnic tensions in the Georgian territory of South Ossetia, and in response to a series of rebel missile attacks on Georgian cities, the Georgian army attempted to retake the region in August 2008. In response, the Russian army quickly moved into South Ossetia to expel the Georgian government. A series of battles ensued that ultimately resulted in Russian victory. In accordance with their ceasefire agreement, the Russian army has slowly withdrawn from the region, but tensions remain high.

Prior to the Russian invasion, Georgian government websites were hit with a series of DDOS attacks similar to those seen in Estonia in 2007. As ground fighting broke out, the intensity of the attacks increased. Russian hackers seized control of the routers that support web traffic to Georgia, thus denying Georgians any Internet connection with the outside world. Banking operations, credit card, and mobile phone systems in Georgia were shut down. In response, Georgian authorities attempted to transfer their government websites and other sensitive operations to servers outside the country, but most of the damage was irreparable.

Again, Russian authorities attributed the cyber attacks to individuals and criminal elements acting without government approval. Many experts, however, have traced the attacks back to websites linked to the Russian intelligence community.²⁵

Russia is not the only player in the cyberwarfare game. Acts of cyberwarfare have been attributed to North Korea,²⁶ China,²⁷ Israel,²⁸ and even the United States.²⁹ In fact, reports have recently surfaced that the United States and Israel may have unleashed the most sophisticated cyber attack to date in a successful effort to delay Iran's nuclear program. The cyber weapon—a computer worm called “Stuxnet”—began spreading indiscriminately throughout the world in 2009. While it has infected many computers, the virus is relatively harmless unless it detects a specific configuration and brand of controllers and process that are found almost exclusively in nuclear centrifuge plants.³⁰

²⁵ This account comes from Clarke and Knake, *Cyber War*, pp. 17-20.

²⁶ See Clarke and Knake, *Cyber War*, p. 21.

²⁷ Robert Marquand, “China Emerges as Leader in Cyberwarfare,” *The Christian Science Monitor*, September 14, 2007, <http://www.csmonitor.com/2007/0914/p01s01-woap.html>.

²⁸ William J. Broad, John Markoff, and David E. Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay,” *New York Times*, January 15, 2011.

²⁹ *Ibid.*

³⁰ *Ibid.*

Numerous experts have asserted that the complexity and sophistication of the Stuxnet virus indicates that it was produced by a nation-state, and many have speculated that it was intentionally developed and released by the United States, Israel, and possibly other Western countries in an effort to cripple Iran's nuclear program.³¹ If this accusation is correct, then Iran may be the first true victim of cyberwarfare.

All of this evidence is anecdotal at best. One of the greatest challenges created by cyberwarfare is the problem of attribution. Due to the amorphous nature of cyberspace, it is exceedingly difficult to identify the exact source of a cyber attack. Regardless of whether cyberwarfare has occurred or not, however, it is clear that the potential for cyberwarfare does exist and that nations are taking its prospect very seriously.

As Clarke notes, the attackers in the Estonian and Georgian incidents "showed considerable restraint."³² The potential consequences of less restricted cyberwarfare are far more severe. Imagine, for instance, the financial costs

³¹ See Broad, Markoff, and Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay;" Jonathan Fildes, "Stuxnet Worm Targeted High-Value Iranian Assets," *BBC News*, September 23, 2010, <http://www.bbc.co.uk/news/technology-11388018>; Claudine Beaumont, "Stuxnet Virus: Worm Could Be Aimed At High-Profile Iranian Targets," *Daily Telegraph*, September 23, 2010.

³² Clarke and Knake, *Cyber War*, p. 21.

associated with an attack on the servers of the New York Stock Exchange,³³ or the casualties that could result from an attack on a nation's air traffic control systems. In prolonged wars, cyber attacks could be carried out for years on end. As stated in the White House's 2009 Cyberspace Policy Review: "Cyberspace touches practically everything and everyone."³⁴ An attack on any single component of the United States' computer infrastructure could result in devastating economic and human costs. The consequences of repeated successful attacks could be unfathomable.

Recognizing its inevitable significance, the United States military has undertaken a series of efforts to establish cyberwarfare doctrine and to enhance its cyberwarfare capabilities. In 2006, the Department of Defense (DOD) drafted

³³ Stock exchanges have been targeted with cyber attacks in the past. In 2009, the public website of the NYSE Euronext was targeted with a DDOS attack. News of the attack apparently caused the value of shares of NYSE Euronext to drop. "NYSE Website Targeted by Cyber Attack; Shares Fall," *CNBC.com*, July 8, 2009, http://www.cnbc.com/id/31801659/NYSE_Website_Targeted_by_Cyber_Attack_Shares_Fall. A February 2011 report revealed that the computer network of the Nasdaq Stock Exchange was penetrated multiple times throughout 2010. Devlin Barrett, "Hackers Penetrate Nasdaq Computers," *Wall Street Journal*, February 5, 2011. Although the source and purpose of these intrusions has not been identified, they have prompted inquiry from lawmakers regarding the cybersecurity practices of various stock exchanges and financial regulators. Telis Demos, "Cyber-Attack Raises SEC Questions," *Financial Times*, February 9, 2011.

³⁴ The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

the National Military Strategy for Cyber Operations. The document summarized the U.S. military's vision for its role in cyberwarfare:

"DOD will execute the full range of military operations (ROMO) in and through cyberspace to defeat, dissuade, and deter threats against the US interests...DOD will use network exploitation to gather intelligence and shape the cyberspace environment as necessary to provide integrated offensive and defensive options."³⁵

The DOD's 2009 Quadrennial Roles and Missions Review Report

identified cyberspace and cyberwarfare as one of four major focus areas for the U.S. military.³⁶ An article recently published in the Air Force's *Strategic Studies Quarterly* goes so far as to argue that: "In the future, cyber will evolve into a weapon of preference, replacing many of the kinetic choices in today's arsenal."³⁷ All four major branches of the Armed Forces have developed commands dedicated to the conduct of cyberwarfare.³⁸ To coordinate these efforts, the

³⁵ Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*, p. 2.

³⁶ Department of Defense, *Quadrennial Roles and Missions Review Report*, 2009, http://www.defense.gov/news/Jan2009/QRMFinalReport_v26Jan.pdf.

³⁷ John A. Shaud, "An Air Force Strategic Vision for 2020-2030," *Strategic Studies Quarterly*, Vol. 5, No. 1 (Spring 2009), p. 17.

³⁸ See, e.g., the Army Forces Cyber Command (ARFORCYBER), the 24th USAF, The Navy's Fleet Cyber Command (FLTCYBERCOM), and the Marine Forces Cyber Command (MARFORCYBER).

Department of Defense has created the U.S. Cyber Command as a unified sub-command under the authority of the U.S. Strategic Command.³⁹

Other countries have placed similar emphasis on cyberwarfare capabilities. The Chinese military has developed a strategy called “Integrated Network Electronic Warfare,” which consolidates its cyber attack and other electronic warfare capabilities under its General Staff Department (the highest organizational authority in the People’s Liberation Army), while dispersing cyber defense and intelligence gathering activities among other military and civilian intelligence organizations.⁴⁰ Russia’s cyberwarfare capabilities, considered some of the most sophisticated in the world, are likely orchestrated by the Service of Special Communications and Information—an organization that evolved from the former-KGB.⁴¹ Less obvious suspects like Australia have also

³⁹ Clarke and Knake, *Cyber War*, p. 32.

⁴⁰ Bryan Krekel, “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,” prepared for The U.S.-China Economic and Security Review Commission, October 9, 2009, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

⁴¹ Clarke and Knake, *Cyber War*, p. 63.

developed extensive cyberwarfare facilities.⁴² To date, it is estimated that at least 30 state militaries have established a respectable cyberwarfare capacity.⁴³

While some skepticism over the hype surrounding cyberwarfare may be justified, it is clear that the major governments of the world consider cyber operations an integral component of the future of warfare. Regardless of whether it has yet occurred, cyberwarfare appears inevitable and consequential.

⁴² See Gary Waters, Desmond Ball and Ian Dudgeon, *Australia and Cyber-Warfare* (Canberra, Australia: Australia National University Press, 2008).

⁴³ Clarke and Knake, *Cyber War*, p. 64.

III. Realism and the Security Dilemma

Offensive and Defensive Realism

Since the publication of Kenneth Waltz's *Theory of International Relations*,¹ much attention in the field of international relations has centered on the debate between the so-called "realists" and their various critics and opponents.² Realists depict a world characterized by fear, competition, and conflict. Because there is no overarching authority, states are viewed as the principal actors in the international system. States are driven toward their own national interests, with the overriding interest always being survival. The realist view of the world is undeniably pessimistic, especially when compared to competing theories from liberals, institutionalists, and others. As their name suggests, however, realists are not usually concerned with ideals and archetypes.³

Still, many realists believe that there is hope for peace and cooperation in the international system. To understand the root of such optimism, it is

¹ Kenneth Waltz, *Theory of International Relations* (New York: Random House, 1979).

² Waltz's theory is typically categorized as part of the "neorealist" or "structural realist" tradition. See Robert O. Keohane, *Neorealism and its Critics* (New York: Columbia University Press, 1986), p. 16.

³ As Keohane notes, political realism is "the language of power and interests rather than of ideals or norms." Keohane, *Neorealism and its Critics*, p. 9.

important to distinguish between two variants of contemporary realist theory: offensive and defensive realism.⁴

Offensive realism, epitomized by the work of John Mearsheimer, depicts an international system characterized by unending conflict and strife.⁵ Fear and uncertainty will rationally drive states to maximize their relative power, with the ultimate goal being the attainment of regional hegemony.⁶ Only when this is achieved can a state be satisfied with its place in the global hierarchy. In order for a state to maximize its power, it must improve its military advantage over others. The result is a constant race to develop both offensive and defensive military capabilities. Unsurprisingly, this structure leaves little opportunity or hope for cooperation between states.

Defensive realists, on the other hand, maintain that much of the world's military conflict is avoidable if only states could better communicate and

⁴ For more extensive analyses of the distinction between offensive and defensive realism, see Robert Jervis, "Realism, Neorealism, and Cooperation: Understanding the Debate," *International Security*, Vol. 24, No. 1 (Summer 1999), pp. 42-63; Evan Baden Montgomery, "Breaking out of the Security Dilemma: Realism, Reassurance, and the Problem of Uncertainty," *International Security*, Vol. 31, No. 2 (Fall 2006), pp. 151-185; John Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton & Co., 2001), Ch. 1.

⁵ John Mearsheimer, "The False Promise of International Institutions," *International Security*, Vol. 19, No. 3 (Winter 1994-1995), p. 10.

⁶ Ibid.

interpret each others' intentions and interests. Offensive realism, they argue, places too much emphasis on power, when in fact the ultimate goal of many states is simply to maintain security.⁷ These states are generally satisfied with the status quo, their military buildup being driven more by fear and uncertainty than by a desire to improve their position in the international military hierarchy. Such states share with each other an interest in survival, not conquest, and thus cooperation that enhances mutual security, such as arms control, should be both possible and desirable.

Defensive realism is far more palatable to those who hold out hope that we may one day see a world without war. Yet despite this relative optimism, the fact remains that cooperation of this sort is exceedingly difficult and historically rare.⁸ Even if they recognize the potential for cooperation and mutual reward, security-seeking states must still deal with the problems of uncertainty and

⁷ Defensive realists tend to agree that the vast majority of states, both aggressive and not, have security as their fundamental goal. Charles Glaser, *Rational Theory of International Politics: The Logic of Competition and Cooperation* (Princeton: Princeton University Press, 2010), p. 37. Robert Jervis has identified a small number of states that did not have security as their prime goal, such as Hitler's Germany, which he suggests valued territorial expansion and domination over security. Robert Jervis, *Perception and Misperception in International Politics* (Princeton: Princeton University Press, 1976), pp. 50-51. If such cases do exist, they are likely rare exceptions to the rule. Glaser, *Rational Theory of International Politics*, p. 37.

⁸ George W. Downs, David M. Rocke and Randolph M. Siverson, "Arms Races and Cooperation," *World Politics*, Vol. 38, No. 1 (October 1985), p. 119.

mistrust. While states may know that their own intentions are noble, they can never be truly certain of the intentions of others. States can thus find themselves in a “security dilemma.”

The Security Dilemma

The term “security dilemma” was first used by John Herz in his 1951 book *Political Realism and Political Idealism*,⁹ although a similar concept was identified in the same year by historian Robert Butterfield.¹⁰ Both authors described a situation where two states might go to war not because they seek conflict with each other, but rather because they are uncertain and fearful of their adversary’s intentions. For these authors, this fear and uncertainty is a fundamental part of human nature.

Robert Jervis incorporated the concept of the security dilemma into the neorealist framework. Jervis defined the security dilemma as a situation where “many of the means by which a state tries to increase its security decrease the

⁹ John H. Herz, *Political Realism and Political Idealism: A Study in Theories and Realities* (Chicago: University of Chicago Press, 1951); Paul Roe, “The Intrastate Security Dilemma: Ethnic Conflict as a ‘Tragedy?’” *Journal of Peace Research*, Vol. 36, No. 2 (March 1999), pp. 183-202.

¹⁰ Roe, “The Intrastate Security Dilemma,” pp. 183-202.

security of others.”¹¹ For Jervis, the fear that so often leads otherwise well-intentioned states into conflict is less the result of human nature than of the anarchy that characterizes the international system. Because states must rely on “self-help” (i.e., there is no higher authority to look to for assistance), and because the international system is plagued by uncertainty, states are inclined to assume the worst of one another. The rational response to a potential adversary’s military buildup is to improve one’s own capabilities, since one can never be certain whether their adversary’s intentions are aggressive or merely defensive.¹²

¹¹ Jervis, “Cooperation Under the Security Dilemma,” p. 160. Similarly, Glaser describes the security dilemma as existing when “a state’s efforts to increase its security would have the unintended effect of reducing its adversary’s security.” Other authors have emphasized that the security dilemma is mainly a problem of perception. For instance, Montgomery defines the security dilemma as “the situation where one state’s attempts to increase its security appear threatening to others and provoke an unnecessary conflict.” Montgomery, “Breaking Out of the Security Dilemma,” p. 151. Wheeler and Booth argue that: “If the threat posed by one state to another...is accurately perceived...then the situation cannot be classified as a security ‘dilemma.’ It is simply a security ‘problem,’ albeit a perhaps difficult one.” Roe, “The Intrastate Security Dilemma,” pp. 185, 187, quoting Nick Wheeler and Ken Booth, “The Security Dilemma,” in John Baylis & Nick J. Renger, eds., *Dilemmas in World Politics: International Issues in a Changing World* (Oxford: Clarendon Press, 1992), pp. 30-31. Schweller claims that: “The security dilemma is *always* apparent, not real.” Randall Schweller, “Neorealism’s Security Bias: What Security Dilemma?” *Security Studies*, Vol. 5, No. 3 (Spring 1996), p. 117.

¹² Note that a security dilemma only exists when both states have benign intentions. If one or both states do in fact intend to harm or threaten the other, then there is no security dilemma. Thus, Schweller correctly notes that: “If states are arming for something other than security; that

As long as a state responds in kind to its adversary's security enhancements, it might make the mistake of believing that it is engaged in a zero-sum game. The problem, however, is that a state's efforts to enhance its security are not only a threat to others, but that these measures can leave the state worse off than before. Glaser recognizes three ways in which a state's security-enhancing measures can be self-defeating. First, if a state grows its offensive military arsenal, its adversary is likely to do the same, thus leaving the first state worse off from a defensive standpoint than it was before. Second, by making an adversary more insecure, a state might drive that otherwise benign adversary to seek aggression or expansion as a means of enhancing its security. Third, by taking actions that intensify arms competition, states cause themselves to expend financial resources that could be used for other purposes.¹³

is, if aggressors do in fact exist, then it is no longer a *security* dilemma." Schweller, "Neorealism's Security Bias," p. 117.

¹³ Charles Glaser, "The Security Dilemma Revisited," *World Politics*, Vol. 50, No. 1 (October 1997), pp. 174-175.

Military Technology

While fear and uncertainty are the causes of the security dilemma, weapons are the means through which it is perpetuated.¹⁴ Weapons can be used by aggressor states to threaten or dominate others, but they can also be used to defend against other weapons (e.g., a missile defense system) or to deter hostile actions by signaling to adversaries that an attack will be reciprocated in kind.

When one state develops a new military technology, other states are threatened. In response, they must take action to enhance their own security. This often results in arms racing, where states find themselves continually developing more and better weapons in order to stay ahead in the competition for relative security.

What makes weapons and other military technologies especially threatening is not merely their destructive potential, but that their purpose can be difficult to discern. As Booth and Wheeler state, “weapons are inherently ambiguous in their politico-strategic meaning; consequently, their very material

¹⁴ For an extensive discussion of the effect of weapons on the security dilemma, see Booth and Wheeler, *The Security Dilemma*, pp. 42-61.

potential invites mistrust.”¹⁵ Even benign, security-seeking states can find themselves engaged in arms races, not because either state wishes the other any harm, but because neither can discern the purpose of their adversary’s weapons. Unsurprisingly, military technology is one of the most cited factors that can influence the severity of a security dilemma between states.¹⁶

Cooperation

Cooperation among states to enhance mutual security is difficult, since an increase in one state’s security has the tendency to diminish the security of others. However, where states truly do not wish to harm each other, hope for cooperation remains. Jervis argues that “it is possible for a state to make itself more secure without making others less secure.”¹⁷ By doing so, a state could continue to pursue self-help solutions while at the same time opening up the possibility for cooperation toward mutual security.

¹⁵ Booth and Wheeler, *The Security Dilemma*, p. 42.

¹⁶ Montgomery, “Breaking Out of the Security Dilemma,” p. 151.

¹⁷ Jervis, “Cooperation Under the Security Dilemma,” p. 187.

Jervis describes two variables that can affect the magnitude and nature of the security dilemma. The first is whether, in a potential standoff between two states, the offense or defense has the advantage. Jervis explains:

“When we say that the offense has the advantage, we simply mean that it is easier to destroy the other’s army and take its territory than it is to defend one’s own. When the defense has the advantage, it is easier to protect and to hold than it is to move forward, destroy, and take.”¹⁸

To determine whether offense or defense has the advantage, one can ask:

“Does the state have to spend more or less than one dollar on defensive forces to offset each dollar spent by the other side on forces that could be used to attack?”¹⁹ If the answer is less, then the defense has the advantage, since it would be easier and cheaper to pursue a defensive strategy than an offensive one. If the answer is more, then states are better off deterring their adversaries from attacking by building their own offensive weapons.²⁰

Where defense has the advantage, the severity of the security dilemma is reduced since states can take measures that increase their own security more

¹⁸ Ibid, p. 187.

¹⁹ Ibid, p. 188.

²⁰ There is substantial debate over how to define the offense-defense balance, as well as whether and how the balance can be measured. For an extensive discussion of these debates, see Charles Glaser, “What is the Offense-Defense Balance and Can We Measure It?” *International Security*, Vol. 22, No. 4 (Spring 1988), pp. 44-82.

than they decrease their adversary's security.²¹ The greater the defensive advantage, the less benefit states are likely to gain by going to war.

Theoretically, if the balance shifts greatly enough toward defense, states could reach a point at which they are no longer seriously threatened by their adversaries.

When offense has the advantage, the reverse occurs since two adversaries cannot both enjoy high levels of security. Instead, to achieve security relative to their adversary, a state must improve their offensive capabilities. When offense has the advantage, states will feel less secure from one another, war is likely to be quicker and victory more decisive, and the advantage will often go to the state that strikes first. Thus, states have a greater incentive to enhance their security by going on the offensive. Cooperation is difficult when offense has the advantage.²²

A second variable that can affect the security dilemma is the ability to differentiate between offensive and defensive weapons and policies. States cannot be certain of the purpose of their adversary's weapons and military

²¹ Glaser, "The Security Dilemma Revisited," p. 185.

²² Ibid., pp. 185-186.

programs. Thus, states look to the capabilities of those weapons and programs to determine the extent of their threat. Many weapons have both offensive and defensive uses. As long as a weapon can be used for offensive purposes, it poses a threat to others and the security dilemma will persist. However, where it is clear that a weapon is primarily capable of defense, states are less threatened by that weapon and the security dilemma is reduced.

Offense-defense differentiation provides a means for non-aggressive states to shift the offense-defense balance toward the defense without reducing their own security. By increasing their security through the development of defensive weapons, states can leave open the possibility of cooperative agreements to reduce or ban offensive ones.²³

²³ Ibid., p. 186.

IV. The Cybersecurity Dilemma

A “cybersecurity dilemma” exists when efforts by one state to enhance the security of its digital infrastructure, either through the development of offensive or defensive cyberwarfare capabilities, decrease the cybersecurity of others. Due to cyberwarfare’s unique properties, the cybersecurity dilemma may be more difficult to break than the typical security dilemma.

To initially assess the prospects for cooperation over interstate cyberwarfare, we must determine: 1) whether the offense or defense would have the advantage in a cyberwar; and 2) whether offensive and defensive cyberwarfare weapons and policies can be distinguished from one another.

The Offense-Defense Balance

There are a number of ways in which cyberwarfare differs from traditional, kinetic warfare. All of these features tend to favor the offense.¹

¹ Recall that Jervis defines the offense-defense balance in terms of the resources necessary to attack and take territory versus the costs of defending that territory. Jervis, “Cooperation Under the Security Dilemma,” pp. 187-188; also see Glaser, *Rational Theory*, p. 43. In the cyberwarfare context, the offense-defense balance can be understood as a state’s ability to attack an adversary’s cyber infrastructure compared to its ability to defend against a similar attack.

For one, cyber attacks can be carried out almost instantaneously.² Under traditional military doctrine, mobility is considered to favor the offense.³ This is because greater mobility leaves targets with less opportunity to prepare a decent defense. Mobility is closely related to two factors that have historically played a significant role in kinetic warfare: terrain and surprise. As Jervis observes, “anything that increases the amount of ground an attacker has to cross...increases the advantage accruing to the defense.”⁴ While in kinetic warfare terrain may serve as an impediment to an attack, there is no such buffer in cyberspace. The lack of terrain also allows for surprise attacks on previously unrecognized network vulnerabilities. As Jervis notes, “weapons and strategies that depend for their effectiveness on surprise are almost always offensive.”⁵ In short, the speed with which cyber attacks can be executed makes defending against them very difficult, and thus greatly advantages the offense.

² A U.S. Army document notes that “forces can attack or be attacked with a speed not achievable in other domains.” U.S. Army, *Cyberspace Operations Concept Capability Plan*, p. 10.

³ See Ned Moran, “A Historical Perspective on the Cybersecurity Dilemma,” *Insecure Magazine*, Issue 21 (June 2009), p. 113, <http://www.net-security.org/dl/insecure/INSECURE-Mag-21.pdf>.

⁴ Jervis, “Cooperation Under the Security Dilemma,” p. 194.

⁵ *Ibid.*, p. 205.

Cyberwarfare has extremely low costs of entry with potentially high returns on investment.⁶ As a report by the U.S. Air Force Research Laboratory notes, “anyone with a computer and an Internet connection can launch attacks....”⁷ A recent study by the U.S. Army similarly argues that cyberwarfare is “a relatively inexpensive way to gain parity with the U.S. as compared to buying tanks and aircraft or training thousands of soldiers.”⁸ Tied to this is the fact that cyber attacks are an attractive tool for waging asymmetric war.⁹ Weaker actors can engage in cyberwarfare with relatively low costs. The potential devastation resulting from an effective cyber attack on an advanced industrial nation like the United States could be huge. At the same time, if the weaker actor does not have a similarly sophisticated digital infrastructure or economy, a

⁶ Theohary, “Information Operations, Cyberwarfare, and Cybersecurity,” p. 3. Note that there is some disagreement on this point. For example, Knake claims that: “Analysts who have studied capabilities of foreign governments and private groups have concluded that no more than 100 groups and possibly as few as four foreign militaries have the capability to cause real world harm through cyber attacks.” “Ability to Conduct Cyber Attack Should Simplify Attribution, Official Says,” *Defense Daily*, February 21, 2011, http://findarticles.com/p/articles/mi_6712/is_11_247/ai_n54800803/?tag=content;col1.

⁷ Jabour, “50 Cyber Questions.”

⁸ U.S. Army, *Cyberspace Operations Concept Capability Plan*, p. 11.

⁹ I use the term “asymmetric war” or “asymmetric warfare” to mean: “conflicts between actors with wide disparities in power.” Ivan Arreguín-Toft, *How the Weak Win Wars* (Cambridge: Cambridge University Press, 2005), p. 2. The concept of asymmetric warfare should not be confused with “unconventional warfare,” which can be waged effectively by both weak and strong states.

reciprocal attack may not be as effective. Thus, where a weaker or less “wired” state faces off against a stronger, more industrialized nation, an intricate cyber defense strategy may not even be necessary.

Like other forms of warfare, cyber attacks are a means through which states can coerce their adversaries. However, unlike most other military options, cyber attacks need not be accompanied with excessive (or any) human costs. Cyber attacks tend to coerce by disrupting economies and communications, not by taking lives. Many states are hesitant to pursue their political ends through violent means. Similarly, states prefer to limit their own casualties during war. Cyberwarfare provides a means of enhancing security and coercing others without causing loss of life to either side.¹⁰ In this way, it is not only an attractive alternative to other modes of warfare, but it may provide states with an excuse to engage in a conflict that they otherwise would not have pursued. Thus, the availability of cyberwarfare could increase the overall frequency of conflict.

¹⁰ In this sense, cyberwarfare might be compared to the practice of targeted killing, which some have championed as a means of obtaining military goals while limiting casualties on both sides of a conflict. See, e.g., Kenneth Anderson, “Targeted Killing in U.S. Counterterrorism Strategy and Law,” Working Paper, Brookings Institution, May 11, 2009, http://www.brookings.edu/~media/Files/rc/papers/2009/0511_counterterrorism_anderson/0511_counterterrorism_anderson.pdf.

All of these reasons suggest that cyberwarfare favors the offense. Many analysts and scholars agree. A report by the National Research Council states that “[c]yber-attack is easier, faster, and cheaper than cyber-defense,” because “effective defense must be successful against all attacks, whereas an attacker need succeed only once.”¹¹ Kenneth Geers, the U.S. Representative to the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, claims that “the asymmetric nature of cyber attacks strongly favors the attacker.”¹² Ned Moran, a Professor of Information Privacy and Security at Georgetown University, concludes that “the development and deployment of cyber warfare strategies, tactics, and weapons favors the offense and exacerbates the security dilemma.”¹³ Matthew Crosston argues that “the most basic axiom of the cyber realm” is that “offense will always trump defense.”¹⁴

¹¹ National Research Council, Computer Science and Telecommunications Board, *Realizing the Potential of C4I: Fundamental Challenges* (Washington, D.C.: National Academy Press, 1999), p. 12.

¹² Kenneth Geers, “Sun Tzu and Cyber War,” Cooperative Cyber Defence Centre of Excellence February 9, 2011, p. 21, http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf.

¹³ Moran, “A Historical Perspective on the Cybersecurity Dilemma,” p. 116.

¹⁴ Matthew D. Crosston, “World Gone Cyber MAD: How ‘Mutually Assured Debilitation’ is the Best Hope for Cyber Deterrence,” *Strategic Studies Quarterly*, Vol. 5, No. 1 (Spring 2011), p. 103. Crosston therefore concludes that “the goal for major powers should not be the futile hope of developing a perfect defensive system of cyber deterrence, but rather the ability to instill deterrence based on a mutually shared fear of an offensive threat.” *Ibid.*, p. 103.

Offense-Defense Differentiation

While offense may have the advantage in cyberwarfare, cooperation is still possible if states can distinguish between offensive and defensive cyber weapons, programs, and policies. The problem of differentiation is closely tied to the verification problem that plagues many arms control efforts. Unfortunately, the outlook here is equally grim.

One challenge with differentiation is that the apparatus necessary to conduct cyberwarfare exists primarily in the virtual world. The only identifiable, physical tool used in cyberwarfare is a computer. Both cyber attacks and cyber defense are carried out through this widespread and typically non-menacing platform. While many of the world's largest militaries have organized cyberwarfare units and programs, a substantial cyber attack could just as easily be carried out from a personal home or business. The greatest challenge for differentiating between offensive and defensive cyber weapons is therefore to identify a weapon in the first place.

Of course, this problem is not wholly unique to cyberwarfare. States can similarly find it difficult to determine whether an adversary's nuclear pursuits are intended to power cities or to create bombs. Still, the challenge here is less

profound. Dedicated intelligence efforts can eventually reveal whether a plant is producing nuclear bombs or nuclear power. Computers are far more common and have far more varied uses.

Even if a cyber weapon can be identified, it remains exceedingly difficult to distinguish between offensive and defensive capabilities. Many military organizations tasked with conducting cyberwarfare have both offensive and defensive capabilities, both of which are conducted through the same mechanisms and machines. The line between offensive and defensive modes is blurry at best, and as one commentator puts it, “the difference between being able to probe and penetrate an adversary’s computer network or attack comes down to a couple of keystrokes...”¹⁵ In that same vein, a weapon’s destructive capability can be almost impossible to determine until it has been used. As cybersecurity expert Paul Kurtz notes: “You can have a small piece of code that can do a whole of a lot of damage or just a little bit of damage depending on how you choose to use it.”¹⁶

¹⁵ Ben Bain, “Military Wrestles with Cyber War Battle Planning,” *DefenseSystems.com*, July 26, 2010, p. 3, <http://defensesystems.com/Articles/2010/07/26/FEAT-Cyber-Command-tackles-cyber-war.aspx?Page=1>.

¹⁶ *Ibid.*, p. 4.

The most important weapons of cyberwar are the “cyber warriors” that conduct it. But it can be equally difficult to identify a cyber warrior. Many militaries have officially-designated cyberwarfare units, yet responsibility for both cyber offense and cyber defense can easily be spread throughout various security and intelligence agencies, and even into the private sector. Even when cyber warriors are recognizable, it is nearly impossible to distinguish between their offensive and defensive intentions and abilities. This is because the same knowledge and tools that cyber warriors use to defend against attacks, such as firewalls and intrusion detection programs, can be used to circumvent those same protections.

V. Efforts at Cooperation

There have been numerous calls over the years for international cooperation to reduce or limit cyberwarfare.¹ Until recently, however, these have fallen on mostly deaf ears.

Ironically, one of the most vocal advocates of cyber arms control is Russia. In 1998, Russia introduced to the U.N. assembly a resolution calling on states to develop international principles to combat “information terrorism.” The resolution did not gain traction, but Russia has continued to call for similar agreements. The idea of strengthening states’ abilities to censor information transmitted over the Internet has appealed to authoritarian regimes but flies in the face of free speech principles.² In order to win broader support, Russia has repeatedly amended and softened their resolution, but fundamental disagreements still exist.³ Many remain suspicious of Russia’s true intentions, and for good reason. In a 2007 paper to the United Nations, experts from the

¹ See, e.g., Rex Hughes, “A Treaty for Cyberspace,” *International Affairs*, Vol. 86, No. 2 (March 2010), pp. 523-541; Tom Gjetlen, “Shadow Wars: Debating Cyber ‘Disarmament,’” *World Affairs* November/December 2010, <http://www.worldaffairsjournal.org/articles/2010-NovDec/full-Gjetlen-ND-2010.html>.

² Gjetlen, “Shadow Wars.”

³ John Markoff and Andrew E. Kramer, “U.S. and Russia Differ on a Treaty for Cyberspace,” *New York Times*, June 27, 2009.

Russian Ministry of Defense argued that: “Almost any information operation with a psychological basis, implemented in peacetime with respect to another state, would qualify as intervention in its domestic affairs. Even good intentions, such as the advancement of democracy, cannot justify such operations.”⁴

The United States has consistently rejected proposals for cyber arms control, often citing problems of verifiability and attribution.⁵ Furthermore, as Clarke notes, early proposals for cyber arms control were considered premature since “[i]t was not obvious then whether or not cyber war added to or subtracted from U.S. national security.”⁶

Calls for cooperation are intensifying,⁷ but whatever the outcome, it is important to remember that a merely symbolic agreement over cyberwarfare does not constitute true “cooperation.” Without the ability to verify compliance,

⁴ Gjetlen, “Shadow Wars.”

⁵ Clarke and Knake, *Cyber War*, p. 219.

⁶ *Ibid.*, p. 220.

⁷ For example, the United Nations’ Telecommunications chief has called for a comprehensive cyber treaty that includes legal and regulatory frameworks as well as “cross-contingency plans” in case of a large-scale cyber attack. Tim Gray, “U.N. Telecom Boss Warns of Pending Cyberwar,” *MSNBC*, September 10, 2010, http://www.msnbc.msn.com/id/39102447/ns/technology_and_science-security/.

a cyberwarfare treaty at this time would not likely serve as an actual constraint on state behavior.

Recently, the United States has expressed interest in greater cooperation over cybersecurity and the policing of criminal activity over the Internet. Still, it has continued to reject calls for constraints on offensive cyber capabilities.⁸ One oft-cited fear is that nations will use a ban on cyberwarfare to justify greater government control over political speech on the Internet.⁹ Others have argued that existing international laws of war adequately deal with the cyberwarfare phenomenon, or that cyberwarfare should not be banned or limited because it is a morally preferable alternative to more costly kinetic warfare.¹⁰ Of course, the problem of verification is frequently cited as a practical limitation on any potential cyber arms control agreement.

Perhaps most important, however, is that the United States continues to see an offensive advantage to cyberwarfare or, at the very least, sees no benefit to reducing its ability to respond in kind to a cyber attack. Rightfully

⁸ Markoff and Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace."

⁹ Gjetlen, "Shadow Wars."

¹⁰ Dorothy E. Denning, "Obstacles and Options for Cyber Arms Controls" (paper presented at Heinrich Böll Foundation's conference on *Arms Control in Cyberspace*, Berlin, Germany, June 29-30, 2001), pp. 6-7, <http://faculty.nps.edu/dedennin/publications/Berlin.pdf>.

acknowledging what defensive realists have asserted for decades, Clarke argues that:

“To determine our national policy toward concepts of arms control or limits on cyber war activities, we first need to ask whether this new form of combat gives the United States such an advantage over other nations that we would not wish to see international constraints. If we believe that we do enjoy such a unilateral advantage, and that it is likely to continue, then we should not ask the follow-on questions about what kinds of limits might be created, whether they could be verified, and so on.”¹¹

However, while offense has the advantage in cyberwarfare, that advantage may reward some states more than others. In asymmetric wars, weaker states might benefit more than stronger ones from using offensive cyberwarfare. Although cyber offense remains easier than cyber defense, the costs of this offensive advantage could be disproportionately borne by stronger states. Thus, powerful states do have an incentive to cooperate to reduce or ban offensive cyberwarfare.¹²

The United States and other powerful nations may be slowly shifting their stance on cyber arms control. For example, in June 2010, the United States signed an agreement with fifteen other nations calling for greater cyberwarfare

¹¹ Clarke and Knake, “Cyber War,” p. 226.

¹² Similarly, Clarke argues that the United States is more vulnerable to cyberwarfare than other nations. Because of this, he suggests that the U.S. should reconsider its position on cyber arms control. Ibid., pp. 220, 226-228.

collaboration. Among the group's recommendations were the creation of norms of accepted behavior in cyberspace, the exchange of information on cybersecurity strategies, and the strengthening of poorer countries' abilities to protect their computer systems. Robert Knake, a cyberwarfare expert with the Council on Foreign Relations, has described this agreement as a "significant change in U.S. posture."¹³

This momentum toward cooperation is still in a very early stage. It does suggest, however, that states may be acknowledging previously unrecognized advantages to cooperation over cyberwarfare.

¹³ Warwick Ashford, "US Joins UN Cyber Arms Control Collaboration," *Computer Weekly*, July 20, 2010, <http://www.computerweekly.com/Articles/2010/07/20/242045/US-joins-UN-cyber-arms-control-collaboration.htm>.

VI. Achieving Cyber Peace

As I have noted, many states have strong incentives to cooperate over cyberwarfare. Such cooperation could be in the form of cyber arms control, but perhaps more easily could take the form of rules and norms that govern the use of offensive cyber weapons. By limiting the use of offensive weapons, powerful nations could reduce the asymmetric advantages that cyber warfare provides to weaker states.

While the prospects for international agreement are currently grim, this is not to say that cooperation over cyberwarfare will always be impossible. Here, I suggest three ways in which cooperation might be facilitated.

Institutions and Norms

Many scholars have argued that international institutions (including international rules, norms, principles, and decision-making procedures) can help to facilitate cooperation even in the face of a security dilemma.¹ These scholars

¹ See, e.g., Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton: Princeton University Press, 1984); Stephen D. Krasner, ed., *International Regimes* (Ithaca: Cornell University Press, 1983); Robert Axelrod and Robert O. Keohane, "Achieving Cooperation under Anarchy: Strategies and Institutions," in Kenneth A. Oye, ed.,

do not usually disagree with the fundamental tenets of realism (i.e., that the international system is anarchic, that states are generally egoistic and must rely on self-help, and that fear and uncertainty make cooperation difficult). Instead, they merely emphasize the role that international regimes can play in reducing problems of information asymmetry, limiting uncertainty regarding other states' intentions, reducing the costs and risks associated with cooperation, and even changing states' perceptions of their own interests. Under this line of reasoning, institutions serve as instruments through which states can achieve the cooperation that they already do, or should, desire. To the extent that they may impose constraints on state behavior, these constraints are usually accepted as the inevitable costs of cooperation. In other words, states have made a rational

Cooperation Under Anarchy, (Princeton: Princeton University Press, 1986), pp. 226-254. While this type of argument is usually associated with the "neoliberal" tradition, similar claims have also been made by several noted realists. See, e.g., Glaser, *Rational Theory of International Politics*, pp. 161-166; Randall L. Schweller and David Priess, "A Tale of Two Realisms: Expanding the Institutions Debate," *Mershon International Studies Review*, Vol. 41, No. 1 (May 1997), pp. 1-32. For an overview of the broader literature on international institutions, see Lisa L. Martin and Beth A. Simmons, "Theories and Empirical Studies of International Institutions," *International Organization*, Vol. 52, No. 4 (Autumn 1998), pp. 729-757.

choice that the benefits of cooperation outweigh the constraints that accompany their participation in international institutions.²

Institutions could facilitate cooperation over cyberwarfare in a number of ways. Participation in international organizations could help states identify their common interests and serve as a forum to develop laws and procedures governing the use of cyberwarfare. International organizations could also assist in verifying compliance with cyber arms control agreements. Multilateral arrangements over cyberwarfare could increase the costs of cheating and defection by tying compliance with cyberwarfare agreements to other cooperative efforts. Even a state's very participation in an institutional arrangement can send valuable signals to others about that state's motives. After

² This explanation of institutions is not that far removed from defensive realist theory. In general, neoliberals put greater emphasis on the ability of institutions to facilitate cooperation than do neorealists. Neoliberals usually argue that institutions can have at least some degree of independent impact on cooperation, whereas neorealists emphasize that states will only establish or participate in an international institution if that institution will help them achieve their goals. Jervis has suggested that concern over such doctrinal distinctions is misplaced, since neoliberals usually study cases of economic and environmental cooperation, whereas realists emphasize the challenge of security cooperation. For a detailed examination of the debate between neorealists and neoliberals, see Jervis, "Realism, Neoliberalism, and Cooperation: Understanding the Debate" *International Security*, Vol. 24, No. 1 (Summer 1999), pp. 42-63.

all, a state is unlikely to enter an institutional arrangement if it does not actually desire cooperation.

A related but distinct line of argument emphasizes the role that international norms can play in both constraining state behavior and encouraging interstate cooperation. In the context of international relations theory, norms refer to “collective understandings of the proper behavior of actors.³ Although norms are not always codified in law, they often inspire or lead to the development of international law. Institutions can help create and foster norms, although norms can also develop at the domestic level and then “diffuse” throughout the international system.⁴ Scholars have argued the existence of strong international norms against various weapons and practices including chemical weapons, landmines, assassination, and nuclear weapons.⁵

³ See Jeffrey W. Legro, “Which Norms Matter? Revisiting the ‘Failure’ of Internationalism,” *International Organization*, Vol. 51, No. 1 (Winter 1997), p. 2.

⁴ On norm “diffusion” and other theories regarding the development, spread, and eventual internalization of norms, see Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change,” *International Organization*, Vol. 52, No. 4 (Autumn 1998), pp. 887-917.

⁵ Regarding norms against chemical weapons, see Richard Price, “A Genealogy of the Chemical Weapons Taboo,” *International Organization*, Vol. 49, No. 1 (Winter 1995), pp. 73-103. For landmines, see Richard Price, “Reversing the Gun Sights: Transnational Civil Society Targets Landmines,” *International Organization*, Vol. 52, No. 3 (Summer 1998), pp. 613-644. On assassination, see Ward Thomas, *The Ethics of Destruction: Norms and Force in International*

Norms are typically the result of ethical considerations and are often said to act as moral constraints on state behavior. Thus, unsurprisingly, the study of norms is frequently viewed as antithetical to the neorealist tradition. However, many authors have noted ways in which norms often conform to states' own interests and can thus be explained by neorealist theory.⁶ States can develop and spread norms as a means of encouraging others to reevaluate and change their interests and priorities.

Norms could serve as a promising means of limiting the use of cyberwarfare. For instance, a norm could develop against the use of cyber attacks on civilian targets, or at the very least, against civilian collateral damage during cyberwarfare.⁷ Norms can take years to develop and spread, and cannot be unnaturally imposed on other states (else they serve merely as symbolic or

Relations (Ithaca: Cornell University Press, 2001). On nuclear weapons, see Nina Tannenwald, "Stigmatizing the Bomb: Origins of the Nuclear Taboo," *International Security*, Vol. 29, No. 4 (Spring 2005), pp. 5-49.

⁶ Thomas, *Ethics of Destruction*, p. 8.

⁷ Many scholars have argued that an important factor in norm development is how well that norm resonates with previously established norms. Price argues that the norm against land mines was successful in part because it was "grafted" from previous norms regarding non-combatant immunity and unnecessary suffering. Price, "Reversing the Gun Sights," p. 628. A norm against civilian collateral damage in cyberwarfare could be "grafted" in a similar way.

idealistic propositions). The acceptance of a norm is largely dependent on the quality of the ethical argument underpinning its creation. Thus, it is unclear to what extent norms against cyberwarfare would be effective. As I have mentioned, there are compelling moral arguments *in favor of* cyberwarfare over traditional, kinetic warfare.

Technological Developments

Although cyberwarfare technology currently favors the offense, this may not always be the case. While defensive technology currently lags behind, the intense focus that both the private and public sectors are currently placing on cybersecurity suggests that this gap could narrow. As one study notes:

“Given the pace of technological development, defensive measures will always trail offensive ones, at least for the foreseeable future. That being said, we assess that there are feasible technology advances whose development will enhance cybersecurity.”⁸

It is also foreseeable that the cyber infrastructure of less “wired” nations will become more sophisticated as time goes by. Should this occur, the perceived offensive advantage that cyberwarfare provides to weaker states might be reduced.

⁸ Paul Rosenzweig, *National Security Threats in Cyberspace*, Workshop Report, American Bar Association Standing Committee on Law and National Security, September 2009.

However, while some features giving offense the advantage are the result of current limits in technology, others, such as the lack of terrain, are intrinsic and will persist even as cybersecurity technology improves. Thus, while the offense-defense gap could narrow, we may never see the day when the defense takes the advantage.

Organization and Doctrine

It is difficult to conceive of a way in which offensive and defensive cyber weapons will ever become fully distinguishable. However, the trouble of distinguishing between offensive and defensive cyberwarfare programs and policies could be reduced through proper signaling. Militaries are necessarily secretive about their cyberwarfare programs and capabilities. But by clarifying and improving military doctrine on cyberwarfare, and by increasing the transparency of various cyberwarfare programs and units, states could better signal their intentions to potential adversaries and thus partially reduce the fear and uncertainty that exacerbate the security dilemma.

For example, states could clearly divide responsibility for cyber defense and cyber offense into separate military units. Similarly, they could increase the transparency, where possible, of both military and civilian cybersecurity

organizations and efforts. By doing so, they might be able to allocate further resources and personnel to cybersecurity programs without substantially threatening their adversaries.

States could also reduce fear and uncertainty by clarifying their military doctrines regarding cyberwarfare. For instance, a doctrine holding that offensive cyber capabilities should only be used in response to a kinetic or cyber attack might help reassure adversaries that weapons are not being developed for hostile or aggressive uses. While there can be clear advantages to doctrinal ambiguity, these may be outweighed by the benefits of reducing an adversary's fear. Of course, actions speak louder than words, and in order to realize these benefits, states will be expected to comply with their own doctrine. Thus, doctrine should be carefully crafted, and promises should not be made if they cannot be kept.

While these measures would not eliminate the uncertainty and mistrust inherent in interstate relations, such signals come at little cost and have the potential to at least partially reduce the security dilemma.

VII. Conclusion

The purpose of this article has been to identify and illuminate some of the many challenges facing cooperation over cyberwarfare. I have argued that the security dilemma is particularly acute in this context, due in large part to: 1) cyberwarfare's offensive bias; and 2) the difficulty of distinguishing between offensive and defensive cyber weapons. Because these variables weigh against the prospects for cooperation, we can expect to see a continued race by both strong and weak states to develop cyberwarfare technologies, programs, and policies in the near future.

I have also endeavored to incorporate prescriptive elements by suggesting ways in which cooperation over cyberwarfare might be achieved despite the security dilemma. Some of these proposals draw from academic traditions that are markedly different from the neorealist one relied on throughout most of this article. Still, each suggests intriguing ways in which cooperation between well-meaning states can be achieved, and is thus deserving of earnest consideration. Further research into the potential role of institutions and norms in shaping cyberwarfare law and policy would go a long way toward developing a more complete picture of the prospects and perils of cyber arms control. However, in

accordance with the emphasis I have placed on the security dilemma and on the traditional offense-defense variables, I maintain that improvements in cybersecurity technology and clarification of military policies remain the most promising avenues for future cooperation.

Many critics have argued that cyberwarfare treaties are premature, and they are likely correct. The anarchic structure of our international system and the uncertainty and mistrust that have resulted make cooperation inherently difficult. Overcoming these odds will require dedication, risk, sacrifice and perhaps a bit of luck.

References

- Anderson, Kenneth. 2009. "Targeted Killing in U.S. Counterterrorism Strategy and Law." Working Paper. Brookings Institution, May 11.
http://www.brookings.edu/~media/Files/rc/papers/2009/0511_counterterrorism_anderson/0511_counterterrorism_anderson.pdf (March 21, 2011).
- Arreguín-Toft, Ivan. 2005. *How the Weak Win Wars*. Cambridge: Cambridge University Press.
- Ashford, Warwick. 2010. "US Joins UN Cyber Arms Control Collaboration," *Computer Weekly*, July 20.
<http://www.computerweekly.com/Articles/2010/07/20/242045/US-joins-UN-cyber-arms-control-collaboration.htm> (March 21, 2011).
- Axelrod, Robert and Robert O. Keohane. 1986. "Achieving Cooperation under Anarchy: Strategies and Institutions." In *Cooperation Under Anarchy*, ed. Kenneth A. Oye. Princeton: Princeton University Press.
- Bain, Ben. 2010. "Military Wrestles With Cyber War Battle Planning," *Defense Systems*, July 26. <http://defensesystems.com/Articles/2010/07/26/FEAT-Cyber-Command-tackles-cyber-war.aspx?Page=1> (March 21, 2011).
- Baldor, Lolita C. 2009. "Pentagon Spends \$100 Million to Fix Cyber Attacks," *USA Today*, 9 April.
- Barrett, Devlin. 2011. "Hackers Penetrate Nasdaq Computers." *Wall Street Journal*, 5 February.
- Beaumont, Claudine. 2010. "Stuxnet Virus: Worm Could Be Aimed At High-Profile Iranian Targets." *Daily Telegraph*, 23 September.

- Best, Carole N. 2001. "Computer Network Defense and Attack: Information Warfare in the Department of Defense." USAWC Strategy Research Project. U.S. Army War College, April 10. <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA390581&Location=U2&doc=GetTRDoc.pdf> (March 21, 2011).
- Booth, Ken and Nicholas Wheeler. 2008. *The Security Dilemma: Fear, Cooperation and Trust in World Politics*. New York: Palgrave.
- Broad, William J., John Markoff, and David. E. Sanger. 2011. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *New York Times*, 15 January.
- Clark, David D. and Susan Landau. 2010. "Untangling Attribution." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council. Washington, D.C.: National Academies Press.
- Clarke, Richard and Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Harper Collins.
- CNBC. 2009. "NYSE Website Targeted by Cyber Attack; Shares Fall." July 9. http://www.cnbc.com/id/31801659/NYSE_Website_Targeted_by_Cyber_Attack_Shares_Fall (March 21, 2011).
- Defense Daily*. 2011. "Ability to Conduct Cyber Attack Should Simplify Attribution, Official Says." February 21. http://findarticles.com/p/articles/mi_6712/is_11_247/ai_n54800803/?tag=content;col1 (March 21, 2011).
- Demos, Telis. 2011. "Cyber-Attack Raises SEC Questions," *Financial Times*, 9 February.

- Denning, Dorothy E. 2001. "Obstacles and Options for Cyber Arms Controls." presented at *Arms Control in Cyberspace*, Heinrich Böll Foundation, Berlin, June 29-30. <http://faculty.nps.edu/dedennin/publications/Berlin.pdf> (March 21, 2011).
- Department of Defense. 2009. *Quadrennial Roles and Missions Review Report*, Washington: Department of Defense, available at http://www.defense.gov/news/Jan2009/QRMFinalReport_v26Jan.pdf.
- Downs, George W., David M. Rocke and Randolph M. Siverson. 1985. "Arms Races and Cooperation." *World Politics* 38/1 (October): 118-46.
- Dunlap, Charles. 2011. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* 5/1 (Spring): 81-99.
- Fildes, Jonathan. 2010. "Stuxnet Worm Targeted High-Value Iranian Assets." BBC News, September 23. <http://www.bbc.co.uk/news/technology-11388018> (March 21, 2011).
- Finnemore, Martha and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52/4 (Autumn): 887-917.
- Geers, Kenneth. 2011. "Sun Tzu and Cyber War." Cooperative Cyber Defence Centre of Excellence, February 9. http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf (March 21, 2011).
- Gjetlen, Tom. 2010. "Seeing the Internet as an Information Weapon." NPR, September 23. <http://www.npr.org/templates/story/story.php?storyId=130052701> (March 21, 2011).

- Gjetlen, Tom. 2010. "Shadow Wars: Debating Cyber 'Disarmament.'" *World Affairs*, November/December.
<http://www.worldaffairsjournal.org/articles/2010-NovDec/full-Gjetlen-ND-2010.htm> (March 21, 2011).
- Glaser, Charles and Chaim Kaufmann. 1998. "What is the Offense-Defense Balance and Can We Measure It?" *International Security* 22/4 (Spring): 44-82.
- Glaser, Charles. 2010. *Rational Theory of International Politics: The Logic of Competition and Cooperation*. Princeton: Princeton University Press.
- Glaser, Charles. 1997. "The Security Dilemma Revisited." *World Politics* 50/1 (October): 171-201.
- Glaser, Charles. 1994/1995. "Realists as Optimists: Cooperation as Self-Help." *International Security* 19/3 (Winter): 50-90.
- Goodman, Will. 2010. "Cyber Deterrence: Tougher in Theory than in Practice." *Strategic Studies Quarterly* 4/3 (Fall): 102-35.
- Graham, David E. 2010. "Cyber Threats and the Law of War," *Journal of National Security Law & Policy* 4/1: 87-102.
- Gray, Tim. 2010. "U.N. Telecom Boss Warns of Pending Cyberwar," *MSNBC*, September 10.
http://www.msnbc.msn.com/id/39102447/ns/technology_and_science-security/ (March 21, 2011).
- Herz, John H. 1951. *Political Realism and Political Idealism: A Study in Theories and Realities*. Chicago: University of Chicago Press.
- Hughes, Rex. 2010. "A Treaty for Cyberspace." *International Affairs* 86/2 (March): 523-41.

- Jabour, Kamal T. 2008. "50 Cyber Questions Every Airman Can Answer." Air Force Research Laboratory, May 7.
http://www.au.af.mil/au/awc/awcgate/afrl/50_cyber_questions.pdf (March 21, 2011).
- Janczewski, Lech and Andrew M. Colarik. 2008. *Cyber Warfare and Cyber Terrorism*. Hershey, Pennsylvania: Information Science Reference.
- Jervis, Robert. 1978. "Cooperation under the Security Dilemma." *World Politics* 30/2 (January): 167-214.
- Jervis, Robert. 1976. *Perception and Misperception in International Politics*. Princeton: Princeton University Press.
- Jervis, Robert. 1999. "Realism, Neorealism, and Cooperation: Understanding the Debate." *International Security* 24/1 (Summer): 42-63.
- Joint Chiefs of Staff. 2006. *Joint Pub. 3-13: Information Operations*, Washington: Department of Defense, available at
http://www.fas.org/irp/doddir/dod/jp3_13.pdf.
- Joint Chiefs of Staff. 2006. *The National Military Strategy for Cyberspace Operations*, Washington: Department of Defense, available at
<http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf>.
- Joint Chiefs of Staff. 2004. *The National Military Strategy of the United States*, Washington: Department of Defense, available at
<http://www.defense.gov/news/mar2005/d20050318nms.pdf>.
- Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.
- Keohane, Robert O. 1986. *Neorealism and its Critics*. New York: Columbia University Press.

- Krasner, Stephen D., ed. 1983. *International Regimes*. Ithaca: Cornell University Press, 1983.
- Krekel, Bryan. 2009. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." prepared for The U.S.-China Economic and Security Review Commission, October 9. http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (March 21, 2011).
- Legro, Jeffrey W. 1997. "Which Norms Matter? Revisiting the 'Failure' of Internationalism." *International Organization* 51/1 (Winter): 31-63.
- Lewis, James Andrew. 2010. "The Cyber War Has Not Begun." Center for Strategic and International Studies, March. http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf (March 21, 2011).
- Markoff, John and David Barboza. 2010. "Academic Paper in China Sets Off Alarms in U.S." *New York Times*, 20 March.
- Markoff, John and Andrew E. Kramer. 2009. "U.S. and Russia Differ on a Treaty for Cyberspace," *New York Times*, 27 June.
- Marquand, Robert. 2007. "China Emerges as Leader in Cyberwarfare," *The Christian Science Monitor*, September 14. <http://www.csmonitor.com/2007/0914/p01s01-woap.html> (March 21, 2011).
- Martin, Lisa L. and Beth A. Simmons. 1998. "Theories and Empirical Studies of International Institutions." *International Organization* 52/4 (Autumn): 729-757.
- McConnell, Mike. 2010. "Mike McConnell on How to Win the Cyber-War We're Losing." Op-ed, *Washington Post*, 28 February.

- Mearsheimer, John. 1994/1995. "The False Promise of International Institutions." *International Security* 19/3 (Winter): 5-49.
- Mearsheimer, John. 2001. *The Tragedy of Great Power Politics*. New York: W.W. Norton & Co.
- Montgomery, Evan Baden. 2006. "Breaking Out of the Security Dilemma: Realism, Reassurance, and the Problem of Uncertainty." *International Security* 31/2 (Fall): 151-85.
- Moran, Ned. 2009. "A Historical Perspective on the Cybersecurity Dilemma." *Insecure Magazine*, June. <http://www.net-security.org/dl/insecure/INSECURE-Mag-21.pdf> (March 21, 2011).
- National Research Council, Computer Science and Telecommunications Board. 1999. *Realizing the Potential of C4I: Fundamental Challenges*. Washington: National Academy Press.
- Price, Richard. 1995. "A Genealogy of the Chemical Weapons Taboo." *International Organization* 49/1 (Winter): 73-103.
- Price, Richard. 1998. "Reversing the Gun Sights: Transnational Civil Society Targets Landmines." *International Organization* 52/3 (Summer): 613-44.
- Roe, Paul. 1999. "The Intrastate Security Dilemma: Ethnic Conflict as a 'Tragedy'?" *Journal of Peace Research* 36/2 (March): 183-202.
- Rosenzweig, Paul. 2009. *National Security Threats in Cyberspace*. Workshop Report, American Bar Association Standing Committee on Law and National Security, September.

- Rosenzweig, Paul. 2010. "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council. Washington, D.C.: National Academies Press.
- Shaud, John A. 2011. "An Air Force Strategic Vision for 2020-2030." *Strategic Studies Quarterly* 5/1 (Spring): 8-31.
- Schmitt, Michael N. 2010. "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council. Washington, D.C.: National Academies Press.
- Schweller, Randall. 1996. "Neorealism's Security Bias: What Security Dilemma?" *Security Studies* 5/3 (Spring): 90-121.
- Schweller, Randall L. and David Priess. 1997. "A Tale of Two Realisms: Expanding the Institutions Debate." *Mershon International Studies Review* 41/1 (May): 1-32.
- Singel, Ryan. 2010. "White House Cyber Czar: 'There is No Cyberwar,'" *Wired* March 4. <http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/> (March 21, 2011).
- Tannenwald, Nina. 2005. "Stigmatizing the Bomb: Origins of the Nuclear Taboo," *International Security* 29/4 (Spring): 5-49.
- Theohary, Catherine A. 2009. *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*. CRS Report No. RL31787, March 17. <http://www.crs.gov/Products//rl/pdf/RL31787.pdf> (March 21, 2011).

- Thomas, Ward. 2001. *The Ethics of Destruction: Norms and Force in International Relations*. Ithaca: Cornell University Press.
- Traynor, Ian. 2007. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian*, 17 May.
- United States Army. 2010. *Cyberspace Operations Concept Capability Plan 2016-2028*, <http://www.fas.org/irp/doddir/army/pam525-7-8.pdf>.
- Waltz, Kenneth. 1979. *Theory of International Relations*. New York: Random House.
- Waters, Gary, Desmond Ball and Ian Dudgeon. 2008. *Australia and Cyber-Warfare*. Canberra, Australia: Australia National University Press.
- Watts, Sean. 2010. "Combatant Status and Computer Network Attack." *Virginia Journal of International Law* 50/2 (December): 391-447.
- Wei-Wang, Jian and Li-Li Rong. 2009. "Cascade-Based Attack Vulnerability on the US Power Grid." *Safety Science* 47: 1332-36.
- Wheeler, Nick and Ken Booth. 1992. "The Security Dilemma." In *Dilemmas in World Politics: International Issues in a Changing World*, eds. John Baylis & Nick J. Renger. Oxford: Clarendon Press.
- The White House. 2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*.
- Young, Mark D. 2010. "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power." *Journal of National Security Law and Policy* 4/1: 173-196.