Continuity and Change:
Structural Realism and International Stability in the Information Age

By Yuichiro Mitsutomi

B.A. in History and Chinese Literature, May 2007, Middlebury College
Graduate Certificate in Chinese and American Studies, June 2008, The Johns Hopkins University's Paul H. Nitze School of Advanced International Studies (SAIS) and Nanjing University

A Thesis Submitted to

The Faculty of
The Elliott School of International Affairs
of The George Washington University
in partial fulfillment of the requirements
for the degree of Master of Arts

January 31, 2011

Thesis directed by

Mike M. Mochizuki
Associate Professor of Political Science and International Affairs

Dedication

To Miwako and Toshio Mitsutomi. Your unwavering faith, love, and support have crossed land and sea and truly know no bounds. This thesis is dedicated to you.

To Nobuko Sato. Your life and legacy live on through your children and grandchildren. This thesis is in your memory.

Acknowledgments

My greatest intellectual debt is to all of my mentors who have always taught me to ask questions and challenge the conventional wisdom. To my advisors, Mike Mochizuki and Leon Fuerth, the ideas behind this project were sown in your classrooms and nurtured into fruition by the grace of your patience, support, and insightful questions. Your sympathy for the unconventional, and the dedication with which you approach your respective interests have always been my inspiration.

Abstract of Thesis

Continuity and Change:
Structural Realism and International Stability in the Information Era

Today, the world is in a state of transition and uncertainty abounds. The bipolar Cold War world, which was replaced by an arguably unipolar system after the fall of the Soviet Union, is once again on the verge of being redefined by an emerging balance between nation-states, global businesses, and amorphous clusters of "super-empowered individuals." The technological standards established by the industrial revolutions are being replaced by the "micro-revolutions" that compose the ongoing information revolution. And international relations professionals, both practitioners and academics alike, are faced with the challenge of adapting to the emergent consequences that are borne at the juncture of these geopolitical and technological shifts.

This thesis examines one aspect of the information revolution's impact on international relations by studying the securitization of cyberspace through the structural realist set of optics. The first of the two main questions addressed in this study asks whether or not structural realism, and state-centric theories in general, retain explanatory power in the information age. The purpose of this question is to establish whether structural realism can still be used to explain and anticipate international political phenomena, or if the changes caused by the advent of cyberspace are of the extent that state-centric theories such as structural realism no longer retain sufficient explanatory value. Based on the criteria outlined in a debate between Kenneth Waltz and John Ruggie, I conclude that at the current stage of the information revolution, because the changes to the

international system caused by cyberspace do not transform the defining principles of the international system, structural realism does not need to be overhauled as a tool for studying international phenomena.

Upon establishing the continued relevance of structural realism, I ask in the second question, what the merits and limits of structural realism are in explaining the effects of cyberspace on the international security environment. Here, I assess the potential impact of cyberspace on international stability according to two concepts often used by structural realists—namely, the security dilemma, and system polarity. My analysis indicates that although the security dilemma portrays cyberspace as a potential source of competition and instability, the structural realists' reliance on the number of great powers to anticipate the system's stability dangerously overlooks the possible threats that are created from cyberspace enabling non-state actors, and deteriorating the control states have over their respective security postures. As a result, I conclude in my final assessment that expectations of stability based on the polarity of the system can lead to a false sense of security for states, and that as the information revolution progresses, international political theory will need to reflect the greater roles played by non-state actors in shaping the international security environment.

Table of Contents

Glossary of Terms

ARPANET: Advanced Research Projects Agency Network

C2: Command and Control

CIPAC: Critical Infrastructure Partnership Advisory Council

CNA: Computer-Network Attack

CND: Computer-Network Defense

CNE: Computer-Network Exploitation

CNO: Computer-Network Operations

COTS: Commercial Off the Shelf

CSIS: Center for Strategic and International Studies

CYBERCOM: United States Cyber Command

DDoS: Distributed Denial of Service

DEPSECDEF: Deputy Secretary of Defense

DISA: Defense Information Systems Agency

DoD: United States Department of Defense

DII: Defense Information Infrastructure

ENIAC: Electronic Numerical Integrator and Calculator

EW: Electronic Warfare

GIG: Global Information Grid

IC: Integrated Circuit

ICS: Industrial Control System

ICT: Information and Communications Technology

IDS: Intrusion Detection System

IO: Information Operations

IP: Internet Protocol

IW: Information Warfare

ISP: Internet Service Provider

JCS: Joint Chiefs of Staff

MAD: Mutual Assured Destruction

NIPC: National Information Protection Center

NIAC: National Infrastructure Advisory Council

NIEX: No-Notice Interoperability Exercise

NSA: National Security Agency

NSA/IA: National Security Agency Information Assurance Directorate

NSTAC: National Security Telecommunications Advisory Committee

NSTISSC: National Security Telecommunications and Information Systems Security Committee

P3: Public-Private Partnership

PDF: Portable Document Format

PLAN: People's Liberation Army Navy

SCADA: Supervisory Control and Data Acquisition

SQL: Structured Query Language

STRATCOM: United States Strategic Command

USCC: United States – China Economic and Security Review Commission

Chapter 1: Introduction

"Solar Sunrise": International Security in the Information Age

In February 1998, as the United States was preparing for a major aerial raid of Iraqi facilities suspected of manufacturing chemical, biological, and nuclear weapons, U.S. law enforcement and defense agencies detected numerous sophisticated intrusions into the U.S. Defense Department's (DoD) Defense Information Infrastructure (DII). Forensics indicated that upon probing the DII for vulnerabilities, the assailants had exploited a known vulnerability in computers running the Solaris operating system to gain root access (administrator level access) to several computer systems within the DII, including those operated by the U.S. Air Force, Navy, and Marine Corp.[1] Hundreds of network passwords were stolen by the assailants, and logistical information for the upcoming Iraqi aerial bombing campaign, Operation Desert Fox, had been compromised.

Due to the political circumstances surrounding the penetration, the Pentagon initially believed that the Iraqi government was behind the intrusions.[2] Cyber forensic investigations, which had soon traced the attacks back to an Internet Service Provider (ISP) in Abu Dhabi, further heightened the U.S. defense establishment's concern over Iraqi involvement. Upon receiving permission from the United Arab Emirates (UAE) authorities, the United States responded by sending a strike force to the location where they

[1] Global Security, "Solar Sunrise," *Global Security* (2008), http://www.globalsecurity.org/military/ops/solar-sunrise.htm

believed the Iraqi computer team was operating. However, once entering the building, the strike team only found unmanned computer servers, and no sign of Iraqi infowarriors. The remote servers were only the hop stops used by the assailants, and the actual source of the intrusions that the United States believed were from abroad, were in fact from within the United States.[3]

A multiagency investigation led by the still nascent National Information Protection Center (NIPC) discovered that the intrusions, code-named "Solar Sunrise," had been the work of two sixteen year old teenagers from California, and one Ehud "The Analyzer" Tenenbaum—an eighteen year old hacker from Israel.[4] No state actors were involved in the penetration of U.S. defense networks, and no military-grade hardware was used in the execution of the operations. Three teenage hackers, armed with household computer systems, an Internet connection, and malicious code had successfully infiltrated and exploited a secure federal computer network, and had driven the United States to send a strike force into a foreign country.

The arrest of Tenenbaum and his fellow teenage infowarriors came as a surprise to military analysts and business professionals alike.[5] Nine years after the Morris Worm introduced malicious programs to the still-nascent Internet, the successful provocation and intrusion upon American military, corporate, and university computer networks by

---

[2] Michael A. Vatis, "Trends in Cyber Vulnerabilities, Threats, and Countermeasures," in *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies*, eds. Jacquis S. Gansier (Washington, D.C.: National Defense University Press, 2004), 102-103.

[3] John Adams, "Virtual Defense," *Foreign Affairs* (May/June, 2001), 109-110.

[4] Tenenbaum was arrested after turning himself in to authorities, and was not caught by the NIPC task force. See "The Hacker Who Turned Himself In," *The Guardian* (March 26, 1998)

[5] "White Collar Hackers—A Matter of National Insecurity," *The Guardian* (March 26, 1998)

individuals like Tenenbaum broke with many of the expectations and assumptions both groups of professionals had formerly held about the nature of national security. The sudden realization that individuals, let alone teenagers, were able to remotely penetrate into state information systems led many to question what had changed in the international system in the post-Cold War period, and how these changes were going to alter the concept of security.

In contrast to the high-level of interest initially expressed by the business and military communities over the potential consequences of cyberspace, the reception of cyber-related issues by scholars of international politics remained relatively vapid. Studies regarding the effect of modern information and communications technology (ICT) on international politics continue to be sparse, and even structural realists—who often emphasize the role of military capabilities and technology—have remained relatively silent on the issue. Even those within the realist tradition who have taken up the subject of the information revolution and the Internet have often only discussed them in terms of broader socio-economic issues such as "globalization," or have altogether dismissed the possible significance of modern information and communications technologies on the general dynamics of international politics by considering the potential threats, "overblown."[6]

Thus, the effects of cyberspace on our current theoretical approach to international politics and the expectations we derive from them remain uncertain. Can the world system still be ordered according to the principles of anarchy and power? Should nation-states continue to be used as the base unit of the international system? Does the creation of

[6] See Kenneth Waltz, "Globalization and Governance," *PS: Political Science and Politics* 32:4 (Dec., 1999), and Stephen M. Walt, "Is the Cyber Threat Overblown?" *Foreign Policy Online* (March 30, 2010) http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown

cyberspace promote cooperative or competitive behavior among its users? And is the information revolution a potentially stabilizing or destabilizing factor for the international system? This essay seeks to examine the effects of the information revolution on international political theory by studying the effects of cyberspace on structural realist theories of state behavior and international stability.

Structure and Organization

First, the most fundamental questions for this study are perhaps, what is cyberspace, and why structural realist theory? In the most recent decade, news and media outlets have been full of reports of "cyber-attacks," "cyber-crime," and the so-called "cyber-threat," but many of these reports have come without explaining what these terms describe, and how they are distinguished from each other.[7] No set taxonomy has been established to describe these issues, and as a result, skeptics such as Stephen Walt have been quick to point out that many of these issues are "highly esoteric," and that the rapidly ballooning "cyber-threat" partly stems from the mistaken conclusion that comes from having "lots of different problems…lumped under a single banner."[8]

Walt's warning on the potential dangers of taxonomical ambiguity leading to threat inflation is well taken, and for the purposes of this essay I limit the scope of what is broadly cast as the "information revolution" to narrowly focus on cyberspace, and the

[7] See Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine* 15:09 (Aug. 21, 2007), Kim Zetter, "Computer Malware the New 'Weapon of Mass Destruction'," *Wired: Threat Level* (December 10, 2008), and Conrad Walters, "Cyber Cold War a Threat to All," *The Sydney Morning Herald* (December 24, 2007).

[8] Stephen Walt raises several concerns about the "cyber-threat" and expresses his skepticism regarding the significance of threats unique to cyberspace. See Walt, "Is the Cyber Threat Overblown?" (March 30, 2010)

technologies that helped create it. I draw upon Manuel Castells' history of the information revolution to define cyberspace as the byproduct of three separate "micro-revolutions" that took place in the latter half of the twentieth century within the fields of micro-electronics, computer technology, and telecommunications (opto-electronics).[9] Moreover, functionally, as a man-made virtual medium, I define cyberspace according to three (physical, syntactic, and semantic) interconnected layers, and explain the securitization of the virtual medium by describing the various offensive and defensive computer network operations (CNO) that cyberspace can be used for.

Next, I have chosen to study cyberspace using structural realism because these theories are a prime example of state-centric international relations (IR) theories that also emphasize the role of security in international politics. By using one of the oldest branches of state-centric IR theory as its foundation, this study seeks to show the enduring merits, as well as the emerging limits of state-centric theories in explaining the post-Cold War world.

Moreover, structural realism is an appropriate choice for studying the consequences of cyberspace because, as many observers have already begun asserting, the world is on the precipice of spiraling down into a virtual "arms race."[10] Over 100 states are known to be in possession of some degree of offensive computer network capabilities, and incidents such as "Solar Sunrise" indicate that individuals and non-state actors are also more than capable of harboring malicious programming that can be used to conduct varying levels of destructive activities. Cyberspace has therefore become more than a virtual medium for global communications and financial transactions. It has become

[9] Manuel Castells, *The Rise of the Network Society: The Information Age: Economy, Society and Culture (Volume 1)* (Malden, Massachusetts: Blackwell Publishers, 2000), 38-50.

[10] Bruce Schneier, "It Will Soon be too Late to Stop the Cyberwars," *Financial Times* (December 2, 2010)

securitized to the extent that the United States military recently declared it to be a "new domain of warfare."[11]

For the purpose of this study, I have organized structural realism according to the similarities and differences between the various structural realist theories. In terms of similarities, I explain that most structural realists hold a common worldview that is based on several foundational assumptions about the world—namely, that the system can be separated into the structure and the unit-level processes; that the structure is defined by the ordering principles of anarchy and power distribution; that all units are functionally "alike" under anarchy; and that all state actors are rational actors. In terms of differences, I divide the various strands of structural realist theory according to their views on the question of whether or not the state's thirst for power can ever be satiated. By ordering the theories in this manner, two general groupings are formed. Defensive realists, who believe that power is a means to security and not an end in itself, and offensive realists, who believe that opportunistic power maximization is the only path to guaranteeing security for a state. The former group of theories allows for cooperation between states under certain circumstances, whereas the latter group insists that any semblance of cooperation is temporary, and that states should constantly be looking for opportunities to maximize relative power.

Second, once the theoretical and technical foundations are laid, I approach the two main questions addressed by this study—namely, what type of change does cyberspace

[11] William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89:5 (September/October, 2010): 97-102, 100.

bring to structural realism, and how does cyberspace affect the behavior of states, and the stability of the international system? With the first question, I examine whether the creation of cyberspace produces a change *of* the international system, or a change *within* the international system. In a debate between Kenneth Waltz and John Ruggie, Waltz argues that only the former necessitates a wholesale revision of structural realist theory, and that variables which only produce a change within the system do not require a revision of the theory itself because they only exacerbate or mitigate the structural forces that are inherent to the international system. In other words, according to Waltz, structural realism –or any other state-centric theory for that matter—will only retain its explanatory power if the changes caused by cyberspace upon the international system are changes of magnitude. If a variable such as cyberspace were to transform the world from an international system to a single global government, for instance, then theories of "international" relations, including structural realism, would no longer hold their explanatory value, and moreover, they could not be meaningfully used as the theoretical foundation to examine the effects of cyberspace on the world.

Based on this criteria laid out by Waltz, I argue that at the current stage of the information revolution, cyberspace only produces a change within the international system. Despite arguments by scholars such as Thomas Friedman that claim cyberspace as having transformed the world from an international system to a multi-actor system (including "super-empowered individual" and "electric herds"),[12] I explain that cyberspace has

[12] Thomas Friedman coined the term "super-empowered individuals" to mean individuals that have been empowered by technological developments to act "unmediated by a state." See: Thomas Friedman, *Longitudes and Latitudes: Exploring the World After September 11* (New York, NY: Anchor Books, 2003). Barnett and Hayes expanded upon the concept of super-empowered individuals and argued for a revised three-image system of analysis for the international system. See: Thomas Barnett and Brad Hayes,

changed neither the anarchic nature of the world, nor the dominance of economically and militarily endowed nation-states. However, in addressing this question fully, I also note that the creation of cyberspace has produced a significant change within the system. Much like how the advent of nuclear weapons mitigated some of the deleterious forces within the anarchic system by bringing about the concept of mutual assured destruction (MAD), I argue that cyberspace exacerbates some of the deleterious forces by increasing the level of uncertainty experienced by states. More specifically, I argue that because in the post-industrial era there are more informational assets that need to be protected from computer-based threats, more potential adversaries to protect them from, and more actors involved in the defense of these assets, states (especially heavily networked great powers) are finding great difficulty in adapting to this new, "informationized" security environment.

After establishing the argument that cyberspace does not necessitate a wholesale revision of structural realist theory, I go on to assess how cyberspace affects the behavior of states and the stability of the international system according to structural realist arguments. First, I assess whether cyberspace encourages competitive or cooperative behavior between states according to the material (offense-defense balance, and offense-defense differentiation) and informational (perception of motives and intentions) variables that are used by defensive realists to assess the severity of the security dilemma. From these three criteria, I argue that because cyberspace favors the offensive, can be used to conduct both offensive and defensive operations, and can befog the process of signaling between two

"System Perturbation: Conflict in the Age of Globalization," in *War and Virtual War: The Challenges to Communities* eds. Jones Irwin (New York, NY: Rodopi, 2004).

states, the severity of the security dilemma is increased, and states will find it difficult to defer taking competitive cyber-security strategies.

Second, I assess the impact of cyberspace on the levels of stability that are expected from certain distributions of power. Drawing on the arguments made in the previous section, this section examines whether certain distributions of power (or "polarities") exacerbate or mitigate the level of competition among states, and if bipolar worlds can continue to be more stable than multipolar worlds in the information age. Basing my reasoning on the arguments made by structural realists on why bipolar systems are more stable than multipolar systems, I argue that the creation of a new virtual domain has made it difficult for states to expect stability based on the number of great powers in the system. I explain that compared to prior historical periods when stability, which is often equated with peace or the lack of major shifts in power distribution, was maintained or disturbed by the behavior (often warfare) of major military powers, today, stability is contingent on a greater number of actors. Because technological shifts have altered the nature of conflict, and the ways in which major shifts in relative power can occur, a greater number of less militarily endowed actors can upset the stability of the system by either directly threatening great powers, or altering the distribution of power by indirect, non-violent means. Consequently, expectations of stability based on the polarity of the system can lead to a false sense of security for states, and can lead to states overlooking the dangers within the virtual domain that can threaten a state's power bases irrespective of the system's polarity.

Chapter 2: Structural Realist Theories of International Politics

The information revolution, the creation of cyberspace, and high technology's impact on globalization are often cited in support of liberal arguments that emphasize the role of technologies, such as the Internet, in enabling democratic movements, globalizing financial markets, and sustaining international organizations. The information revolution, however, is seldom referenced by the realist school of thought, or studied according to the assumptions and propositions held by structural realists. The result is a void within the dialogue on international political theory that underemphasizes cyberspace as a domain of warfare, and overlooks the information revolution's impact on the continued viability of state-centric IR theories.

Because any discussion of theory cannot begin without outlining the parameters of the given theory, this chapter begins by providing a working framework of structural realist theory. First, by identifying the common assumptions held by the diverse range of structural realist theories, I develop a general structural realist worldview. This worldview, which was initially developed by Kenneth Waltz in *Theory of International Politics* (1979), emphasizes the separation of the international structure from unit-level processes, and defines the structure according to the principles of anarchy, and the uneven distribution of material capabilities. Furthermore, from these two principles, structural realists derive the assumption that nation-states, which are the base units of the international system, are

rational units that are alike in their common pursuit of self-preservation in the international system.[1]

Second, because there are significant variations within the theories that share this common structural realist worldview, I identify the main propositions and differences articulated by the two major branches of structural realism: defensive and offensive realism.[2] Most importantly, I note that defensive and offensive realists agree that bipolarity is the most stable form of the international structure, and that they disagree on the state's ability to mitigate the deleterious effects of the security dilemma and achieve a satisfactory level of power and security.

The Structural Realist Worldview: Structures, Anarchy, and Power

Despite the rifts that exist within structural realism, at its core, all structural realist theories share several assumptions that develop their common theoretic approach and worldview. First, all structural realist theories are systems-theories of international relations. This means that for structural realists, the international system is functionally divided into two interacting levels: the international structure, and the unit-level processes within the system. In terms of which level of analysis to use, although structural realists concede that neither level of analysis is sufficient to accurately determine the behavior of actors or the outcome of system dynamics, structural realists believe that because systems-

[1] Kenneth Waltz, *Theory of International Politics* (Long Grove, IL: Waveland Press, 1979).

[2] Here, it is important to note that although Kenneth Waltz' neorealism differs significantly from the defensive realist theories of Robert Jervis, Steven Van Evera, and Charles Glaser, because these theories all propose that states can achieve a satisfactory level of security, and that the deleterious effects of the security dilemma are manageable, I refer to them in the aggregate as defensive realists.

level analysis explains the enduring properties, or "a small number of big and important things,"[3] about the international system, and unit-level analysis can only explain the proximate causes of specific events, reductionist methods and unit-level analysis have no place within theories that are concerned with deriving the constant characteristics of the international system.[4]

Second, all structural realists share a common conception of the world system that is defined according to four base assumptions: (1) the "primary political unit of an era" is the base unit of the system; (2) the structure is ordered according to the principle of anarchy and power; (3) the architecture of the system is defined at any given point in time according to the number of great powers that populate the system; and (4) all state actors are rational actors. In terms of the first assumption, while structural realist theories often presume without providing cause that the nation-state is the "primary political unit" of the current era, it is worth noting that the use of the nation-state as the base unit of the system has never been established as an a priori fact, and that "states are not and never have been the only international actors."[5] In defending their state-centric approach, structural realists only raise the argument that "structures are defined not by all the actors that flourish within them but by the major ones."[6] The criteria for what makes one type of international actor

[3] Kenneth Waltz, "Reflections on *Theory of International Politics:* A Response to my Critics" in *Realism and International Politics*, Kenneth Waltz, (New York, NY: Routledge, 2008), 43.

[4] Waltz affirms the view that the unit-level can explain immediate causes of events, and that the structural-level explains the enduring causes of events in an interview with Harry Kreisler. For the transcript of the interview, see: Harry Kreisler and Kenneth Waltz, "Theory and International Politics: A Conversation with Kenneth Waltz," *Conversation with History Series* (University of California, Berkley: Institute of International Studies, February 10, 2003), http://globetrotter.berkeley.edu/people3/Waltz/waltz-con0.html

[5] Waltz (1979), *Theory of International Politics*, 93.

[6] Several scholars such as Robert Gilpin and John Mearsheimer also argue that states (or great powers) are the units of the system because they are the "major ones." Gilpin notes that it is because states are "capable of putting forth demands effectively," whereas Mearsheimer writes that it is because they "dominate and shape international politic." See: Robert Gilpin, *War and Change in World Politics* (New York, N.Y.: Cambridge

"major" are left ambiguous, and one can only infer that determining the "major" players of a system is much like determining the threshold of obscenity—you know it when you see it.

The second assumption that defines the structural realist worldview is that the international political order is an anarchic one. Defined in contrast to a hierarchical domestic political order wherein authority is vertically organized, and the units are differentiated according to function; the international political order lacks any form of a central, supra-national authority, and all the units are "alike" in the functions they perform.[7] In anarchy, because there is no central authority that legislates, regulates, or bestows rights and obligations upon the units, states have no expectation of legal remedy for disputes that arise with other states, and cannot depend upon third parties to intervene to their support. States under these circumstances are left to their own means when faced with such situations, and must provide for their own preservation if all non-violent measures of conflict resolution fail. Political life for states in an anarchic system, therefore, is very much a Melian existence wherein, "the strong will do what they will, and the weak will suffer what they must."[8]

The notion that states are left to their own means to provide for their self-preservation and security further leads structural realists to differentiate units according to power, or in other words, how well or how poorly they can accomplish the tasks common to all. Power, in this sense, can be vaguely understood as the capabilities available to states

---

University Press, 1981), 18; John Mearsheimer, *Tragedy of Great Power Politics* (New York, N.Y.: W.W. Norton & Company, 2001), 17; and Waltz (1979), *Theory of International Politics*, 93.

[7] Waltz (1979), *Theory of International Politics*, 89.

[8] Robert B. Strassler ed., *The Landmark Thucydides* (New York, N.Y: Simon and Schuster Inc., 1996), 352.

including various aspects such as socio-economic, political prestige, resource endowments, technological innovation, and military force. Power, as Joseph Nye eloquently writes, "like love, is easier to experience than to define or measure."[9] Yet, because structural realists believe the ability to forcibly coerce an adversary is the "*ultima ratio"* of international politics, structural realists most often emphasize actionable military capabilities of states to measure the relative power of one state against another.[10]

By differentiating functionally "like-units" according to the principle of power, structural realists derive the third assumption that the architecture of the international system is defined at any given time by the number of great powers that populate it. Great powers, which are considered to be the states with the strongest military force and the most sustainable power bases to support them, are used by structural realists because they assume the behavior and decisions of great powers have the capacity to either maintain or destroy the stability of the international system. Moreover, the architectures that the great powers create, which are cast in terms of "bipolar" and "multipolar" worlds, allows structural realists to make deductive arguments about the durability of some structures over others. (See section on "Polarity")

In addition to these core assumptions, while Waltz does not address the issue directly, structural realists such as Charles Glaser expand the "like-unit" assumption to also include the fourth assumption that all states are rational actors. If all states are assumed to be bound together in their plight for a common objective (security), then, Glaser argues, all

[9] Joseph S. Nye, Jr., "The Changing Nature of World Power," *Political Science Quarterly* 105:2 (Summer, 1990): 177-192, 177.

[10] John Mearsheimer emphasizes the role of the military the most in structural realist theory, however, Waltz, Jervis, and others also emphasize the role of military assets over other power bases such as economic or technological innovation. See: Mearsheimer (2001), *Tragedy of Great Power Politics*, 56.

states must also be "purposive actors" that maintain relatively fixed motives, and "can make at least reasonable efforts to choose the strategy that is best suited to achieving their goals."[11] Borrowing heavily from Jon Elster's work on rational choice theory, as rational actors, states are assumed to have an objective, and an ability to discern a feasible set of options to achieve the objective. They are assumed to base their decisions on an understanding of constraints, a belief in causation, and the subsequent ability to prioritize the feasible set of options in a way that is consistent with the actor's beliefs, objectives, and understanding of its constraints.[12] Thus, this belief that all states are functionally alike, and that they are able to create and follow a logical progression that is internally consistent, and can be externally observed, allows structural realists to make normative judgments (e.g., optimal versus suboptimal policies) and prescriptive conclusions about international politics.

Two Branches of Structural Realism: Defensive and Offensive Realism

The large array of theories broadly cast as "structural realist" vary in their purpose, the independent variables they include, and the deductions that they derive from their commonly held worldview. Even though Kenneth Waltz, who initially conceived the structural realist worldview, is often recognized as the originator of the systems-approach to realism in international politics, subsequent theories such as John Mearsheimer's offensive realism, and Charles Glaser's strategic choice theory draw competing conclusions

[11] Charles Glaser, *Rational Theory of International Politics* (Princeton, NJ: Princeton University Press, 2010), 31.

[12] Jon Elster, *Rational Choice* (Oxford, London: Basil Blackwell, 1986)

from the foundation established by Waltz's neorealist theory. Organizationally, this means that there are various ways to organize and group the diverse set of structural realist theories, and that all the theories do not fall between the two poles of a given linear diagram.

For the purposes of this study, I have loosely organized some of the salient theories of structural realism according to where they stand on the question of how much power states desire. Organizing structural realism in this fashion creates two broad groups of theories—defensive realists, who believe that a state's desire for power is satiable, and offensive realists, who believe that a state's desire for power can only be satiated when no other actors can challenge its security. The following discusses differences between these two groups, as well as similarities in their deductive conclusions.

Defensive Realism

The term defensive realism is often used to describe the group of structural realist theories that focus on the security dilemma to argue that non-structural variables (such as threat perceptions, and offense-defense variables) can lead security-seeking states to achieve their objective through non-competitive means. This conventional definition of defensive realism is a much more restrictive definition of the sub-group of structural realists—it excludes theories such as Kenneth Waltz' neorealism because neorealists deduce from the anarchic nature of the system that international politics is an inherently "competitive realm";[13] and it also excludes Charles Glaser's strategic choice approach

[13] Waltz (1979), *Theory of International Politics*, 179.

because Glaser's theory breaks with the assumption that all states are motivated by the pursuit of security.[14] Organizing structural realism in the conventional manner would require an explication of structural realism that is tangential to the purpose of this study.

Here, since the focus is on the role of power in structural realism, and how the information revolution influences it, the individual theory's perspective on power is the discerning criteria in grouping the theories. Defensive realists, in this sense, are the theories that accept the view that a state's power does not necessarily correlate with its level of security, and that more power does not lead to more security. Defensive realists find that security, which is the ultimate end most states seek, is achieved by pursuing optimal strategies that maximize security, not the relative share of power a state holds.

Proponents of this view include Kenneth Waltz, Robert Jervis, Stephen Walt, Charles Glaser, and others. Waltz, despite finding international politics as an inherently competitive realm, believes that "[states] cannot let power, a possibly useful means, become the end they pursue."[15] Based on the assumptions that the paramount interest of states is to achieve security, and also that power follows the economic law of diminishing marginal returns, Waltz draws the conclusion that states are better off balancing the power of others (and maintaining the status quo) rather than endlessly maximizing it.[16] For Waltz, therefore, pursuing a policy of restraint whereby the equilibrium at the point of constant returns is maintained (cost of one unit of power equals a return of one unit of security) is the optimal policy for security-seeking states.

---

[14] Charles Glaser organizes structural realist theories in this fashion, and places neorealists, offensive realists, defensive realists, and his own theory into four distinct categories of structural realism. See: Glaser (2010), *Rational Theory of International Politics*, 148-158.

[15] Waltz (1979), *Theory of International Politics*, 126.

[16] Glaser (2010), *Rational Theory of International Politics*,126.

Jervis, Walt, and Glaser agree with Waltz in his assertion that "powers is a means not an end," and that power maximization is not always the optimal approach to seeking security.[17] However, the fundamental difference between Waltz and the latter group of structural realists is that they arrive at this conclusion using various unit-level theories (offense-defense theory; balance of threat; strategic choice theory) that fall beyond the scope of neorealism. This latter group believes that the security dilemma—the idea that states arming with the intention of increasing its own security, inadvertently decreases the security of other states, which in turn leads to a positive feedback loop of increasing insecurity—is not a path dependency for international politics. They believe that if the defense has the advantage over the offensive, if the motives and intentions of a potential adversary are neither greedy nor revisionist, and if the motives and intentions of states are successfully communicated and perceived, then neither competition nor power maximization are the optimal policies for a security-seeking, status-quo state. Instead, they believe that cooperative strategies consisting of arms control and arms reduction agreements could mitigate the deleterious effects of anarchy and the security dilemma.

However, the caveat that these defensive realists attach to this proposition is that offensive and defensive variables (e.g., geography, technology) must be distinguishable and favor the defensive, that the motives of the state must be relatively constant, and that a state's perception of another based on signaling must reflect the actual benign motives and intentions of the state. Without satisfying these conditions, defensive realists generally agree that security-seeking states must sometimes act as aggressors, or that competition and conflict are unintentionally caused by the miscalculation of states. In sum, while states are

[17] Waltz (1979), *Theory of International Politics*, 126.

generally assumed to be rational actors within defensive realism, in reality we find too often that being rational and always being capable of acting rational are two completely different matters.[18]

Offensive Realism

Although offensive realism, which was articulated by John Mearsheimer in the seminal piece, *Tragedy of Great Power Politics* (2001), accepts most of the assumptions and propositions held by defensive realists, these two groups differ in their fundamental view of how states should pursue security. More specifically, in contrast to defensive realists, offensive realists take the view that opportunistic power maximization, and the pursuit of hegemony, are the only ways a state can guarantee security for itself within the anarchic system. From this rather paranoid perspective, states are assumed to be motivated by an underlying desire to seek security, but in doing so are assumed to lack any intention of merely maintaining its position within the international system, or giving other states the benefit of the doubt.

For offensive realists, all great powers harbor some degree of revisionist intent because unless they have achieved global hegemony, which Mearsheimer says is unlikely, they can never be assured of the permanence of their great power status, or that they will not be conquered by other aspiring powers in the future. Whatever modicum of security that great powers can enjoy in the short-run is seen as ephemeral, and states cannot expect

[18] In fact, even Glaser admits that states often do not behave rationally in practice. But he notes his theory is not meant to explain the actual behavior of states, but rather what states "should" do. See Glaser (2010), "Chapter Seven: Evaluating the Theory from Within."

it to last unless they can eliminate all other competition and dominate the system. In this sense, "states are almost always better off with more rather than less power," and maximizing power is like a hedge against the threats of today, and the uncertainties of tomorrow.[19]

Despite the difference in interpretation, the logic behind Mearsheimer's arguments also stem from the security dilemma concept. Mearsheimer, however, finds that even if offense-defense variables, and threat perception indicate a non-threatening environment, because states can often change their intentions, states are better off amassing as much power as they can, whenever they can. As evidence of this type of behavior, Mearsheimer notes that throughout history even when geographic and technological conditions favored the defense, and narrowed the window of opportunity for great powers to pursue power, great powers have continued to compete with other great powers over gains in relative power, and have found success in taking expansionist policies.[20]

Polarity

In addition to using material and information variables to explain the optimal and suboptimal security policies of states, structural realist theories also use the international structure to generate general assertions about the stability of certain balances of power over others. In this regard, defensive and offensive realists both agree that bipolarity is more stable than multipolarity. The notion that an international system with two dominant

[19] Mearsheimer (2010), *Tragedy of Great Power Politics*, 35.

[20] Ibid., 38-39.

powers is more stable than a system with multiple great powers stems from the structural realists' belief that a system with fewer moving parts is easier to manage than a system with many moving parts—especially if the parts are armed with weapons of mass destruction.

First, with fewer great powers in the system structural realists find that there are fewer potential "conflict dyads" within the system, that there is a lesser likelihood of unintended wars erupting from miscalculations by states, and that the distribution of power is more likely to be balanced. In terms of potential conflicts involving great powers, Mearsheimer asserts that whether one focuses on "great-great" conflict dyads or "great-minor" conflict dyads, smaller numbers of great powers are better because it simply reduces the potential number of conflicts that would involve a great power. [21] For example, during the Cold War, since there were only two great powers in the system, the number of potential "great-great" conflict dyads was one. If, hypothetically, China was also a great power at the time, the number of "great-great" conflict dyads would have increased to six. As a matter of probabilities, Mearsheimer argues that a system with more opportunities for great power war is less stable than a system with fewer opportunities.

In addition, fewer great powers also reduce the likelihood of states miscalculating the capability and resolve of its potential adversaries, and waging unnecessary conflicts. For example, in a bipolar system, state *X* assesses and calculates the intentions and capabilities of state *D* to understand the ramifications of its action *Z*. In a multipolar world with five actors, state *X* would have to consider the intentions and capabilities of states *A…D*, the alliances that may exist between all the great powers, and how action *Z* would

[21] Ibid., 338.

influence all possible combinations of actors before deciding whether or not to follow through with the action. Because of the number of complex calculations involved in the strategic decision making of states in a multipolar world, the likelihood of accidents occurring from misperceiving things such as intent, power advantages, and alliances is much higher.

Furthermore, according to Mearsheimer, "the more great powers there are in a system, the more likely it is that wealth and population size, the building blocks of military power, will be distributed unevenly among them." If these "power asymmetries" are created in a territorially contiguous region like Europe, for example, then Mearsheimer warns that the power imbalance could create a potential hegemon that could aggressively pursue expansionist policies within the region.[22] In contrast, Mearsheimer and Waltz both agree that when power is more evenly distributed among fewer states, each of the great powers are less likely to perceive a swift victory, and are more likely to follow conservative policies.

However, while fewer is definitely better than more, structural realists agree that the decisive advantages of having only two great powers makes bipolarity the most favorable system of all. Leaving conflict dyads, miscalculation, and power distribution aside. In contrast to multipolar systems, bipolar systems allow great powers to have the greatest amount of control over their own security and also over the stability of the system. Whereas in multipolar systems states may form alliances and coalitions to balance against perceived threats, in a bipolar system each of the great powers can only rely upon internal

[22] Ibid., 344-345.

efforts to check the other. Shifts in alliances of minor powers do not create a significant asymmetry of power between the two poles, and the risk of either one of the great powers being dragged into a conflict between minor powers is less.[23] Although the danger of having either of the great powers overreacting to unwanted incidents (e.g., Cuban Missile Crisis) remains, Waltz argues that as bipolar systems "mature," power tends to become more evenly distributed between the two great powers, and the states themselves begin to act as "duopolists"—meaning, they both strive to moderate the intensity of competition to promote domestic prosperity, while still remaining cautious of the other.[24] In bipolarity, therefore, because great powers have the knowledge that what they have is the lesser of two evils, they are better able to live with the other and promote stability.

[23] Ibid., 169-170.

[24] Waltz (1978), *Theory of International Politics*, 203.

Chapter 3: Defining the Virtual Domain

The Information Revolution: Which Revolution?[1]

The information revolution, like the industrial revolution before it, is a cumulative process that follows the law of increasing returns. Technological innovations in one field interact with innovations occurring in other fields, and soon, the mutually reinforcing effects of these "micro-revolutions" result in what is retrospectively recognized as a technological "revolution."[2] For the industrial revolution, individual technological breakthroughs that came between the end of the eighteenth and nineteenth centuries, such as the steam engine, the spinning jenny, electricity, and the internal combustion engine, led to the overall industrial revolution that is now recognized as the technological revolution that replaced hand-tools with machines, and vastly increased the rate and scale of production.

Although the revolution in information and communications technology (ICT) is still in its nascent stages, the technological breakthroughs that have thus far defined this revolution can be found in the fields of microelectronics, computers, and telecommunications. In microelectronics, the invention of the transistor in 1947, which allowed for information to be coded and processed using electric impulses, began one leg of the information revolution. Transistors, semiconductors, and the integrated circuit (IC)

[1] The task of dividing a major technological revolution into component "micro-revolutions" and asking the question of "which revolution?" is largely taken from Castells history of the information revolution. See: Castells (2000), *The Rise of the Network Society*, 29-76.

[2] Ibid., 33-35.

that followed in 1957, culminated with the invention in 1971 of the microprocessor. The invention of microprocessors, which essentially placed all of the information processing capabilities of transistors on one chip, allowed for information processing capabilities to be fabricated in very small, even portable devices.[3]

In the field of computers, the first computer, "ENIAC" (electronic numerical integrator and calculator) was produced in 1946 by the U.S. army to process massive amounts of computations. Weighing in at over thirty tons, ENIAC was built upon "19,000 vacuum tubes, 1,500 relays, and hundreds of thousands of resistors, capacitors, and inductors" that altogether consumed almost 200 kilowatts of electrical power.[4] These initial computers, even the vastly smaller 701 vacuum tube machines created by IBM in 1953, physically took up entire rooms and were far from the commercially available computers that we are used to using today.

In 1975, the technological breakthroughs in microelectronics and computers converged to produce, "Altair," one of the first microcomputers that were based on microprocessor technology.[5] Altair, and other early microcomputers such as Apple I, Apple II, IBM 5100, etc, were one of the early "micro-revolutions" that brought advanced information processing capabilities down from the realm of military-grade hardware, and made computers user-friendly. Microcomputers, as the name suggests, were much smaller

---

[3] Ibid., 39-41.

[4] Martin H. Weik, "The ENIAC Story," *ORDNANCE* (January/February, 1961), http://ftp.arl.army.mil/~mike/comphist/eniac-story.html

[5] Castells (2000), *The Rise of the Network Society*, 42-43.

than their gargantuan predecessors, and their relatively cheap pricing made them more affordable for the common business or household.[6]

The second of these "micro-revolutions," and the main subject of this study, was derived when advances in microelectronics and computer technology met technological breakthroughs that were being made in the telecommunications field. In the 1960s, when the United States and the Soviet Union were in the midst of the Cold War, scientists including J.C.R. Licklider, Leonard Kleinrock, and Lawrence Roberts were tasked with designing a communications system that was independent of nodular command and control centers, and would endure nodal losses due to nuclear strikes. Their answer to the challenge Licklider and others produced was packet-switching technology. In contrast to circuit-switching methods of communications of the past, wherein the data's path is fixed and predetermined, packet-switching allowed for segments of data (called "packets") to follow a path of least resistance along a network of computers between two points. With this latter technology, even if some of the nodes between the sender and the receiver were damaged, the packets could take alternate routes to eventually reach the destination.[7]

In 1966, Roberts, Kleinrock and others took the concepts of packet-switching and computer networks and began working on constructing the first nodes that would be a part of, "ARPANET" (Advanced Research Projects Agency Network), the world's first major packet-switching based computer network. Within three years, the "budding Internet was off the ground"[8] and ARPANET had four networked host computers between the

[6] Images of early microcomputers as well as prices can be seen on an online archive chronicling the work of Stan Veit. See: Stan Veit, *PC-History* accessible online at: http://www.pc-history.org/

[7] Barry M. Leiner et al., "A Brief History of the Internet V.3.32," *The Internet Society* (December 10, 2003), http://www.isoc.org/internet/history/brief.shtml.

[8] Ibid.

University of California, Los Angeles (UCLA), Stanford Research Institute (SRI), University of California, Santa Barbara (UCSB), and the University of Utah.

Today, with over 1.9 billion users online, the global, open-architecture computer network most often referred to as the "Internet," has become one of the most salient byproducts of the ICT revolutions thus far.[9] Computer networks have permeated almost every facet of modern life in post-industrial societies, and functionally, they have significantly altered the speed and volume at which information is created, processed, disseminated, and destroyed. The following sections discuss how computers, and more specifically, how computer networks have created a new virtual domain of existence for networked individuals and states, and how this domain can be used to conduct a variety of offensive and defensive operations.

The Three Layers of Cyberspace

In contrast to the pre-information age that only existed in one, physical domain, the information revolution has created a new, man-made virtual domain of existence. This domain, which is often referred to as "cyberspace," is comprised of three interacting layers, which I explain below as being: the physical layer, the syntactic layer, and the semantic layer.[10]

First, at its foundation, the physical layer integrates several independent components such as computers, hard drives, servers, routers, sensors, and various wires.

[9] Internet World Stats: Usage and Population Statistics, "World Internet Users and Statistics," *Internet World Stats* (June 30, 2010), http://www.internetworldstats.com/stats.htm

Much like the vital organs and the bodily systems that sustain life, and allow the brain to receive and communicate information with other parts of the body, the physical layer of cyberspace shoulders the existence of the virtual domain. In essence, the existence of the virtual domain depends upon the healthy function of its physical foundation—and the removal or the destruction thereof would be analogous to removing or destroying the life sustaining vital organs of a human being.

Second, the layer that sits above the physical layer is the syntactic layer. Mainly consisting of code written in programming languages expressed in text or graphics, the syntactic layer contains instructions for computers and machines to perform various computations and protocols that are used by machines to interact with one another. To extend the human analogy, the syntactic layer of cyberspace is similar to human cognition: it brings meaning to inputs and processes them in a way that produces outputs. For example, why do children pull their hands away from a scalding skillet? It is because certain areas of the brain are able to receive the sensation experienced at the hand, process it as pain, and instruct the hand to pull away from the source of pain. In a similar sense, computers have the potential to communicate with one another because network protocols allow computers to recognize external inputs (requests), process them as instructions, and follow the instructions to produce an output.

Third, the final layer that sits above the physical layer is the semantic layer. Libicki explains that the semantic layer consists of the information or the data that a machine contains. This definition diverges slightly from the traditional notion of computer

[10] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Project AIR FORCE Monograph, 2009)

semantics, which refers to semantics as the meaning given to programming languages that are used to manipulate machinery and communicate between computer systems. Libicki's definition incorporates this traditional interpretation of semantics and widens it to include types of information such as digitally stored documents written in natural language, data sets, and images.[11] At the risk of overextending the human analogy, we can perhaps understand Libicki's definition of semantics as the computer equivalent for human language and memories. As the terminology clearly indicates, natural language, which is essentially a set of meaningless symbols that are given meaning through human cognition, is a parallel to programming language; and memories, which are the experiences, information, and stimuli stored in the human brain, are analogous to data files stored within a computer's data storage unit (also known as, "computer memory").

Computer Networked Operations (CNO): Attack, Defense, and Exploitation

The creation of the virtual domain gives rise to a new set of interactions between humans. Just as space transportation systems (STS) opened up the physical domain of space to humans, microelectronics, computers, and opto-electronics have opened up an entirely new domain for humans to create, cooperate and compete. In this latter regard, while cyberspace has had game-changing effects on post-industrial society, and on the information economy, it has had an especially significant impact on war and military affairs. The virtual domain has produced a new arena in which stakeholders must defend

[11] Libicki, *Cyberdeterrence and Cyberwar*, 12.

their electronic and informational assets, as well as new means by which actors can defend their own, or threaten the "digital homeland" of others.

Although cyberspace has been around the military establishment since the creation of the U.S. Department of Defense's (DoD) advanced research projects network (ARPANET) around 1969[12], cyberspace is still a relatively new concept within both civilian and military affairs; and the operations within cyberspace are taxonomically subject to a variety of names and definitions. Information warfare (IW), cyber-war, cybercrime, information operations (IO), and computer-network operations (CNO) are all terms that are often interchangeably used to describe different segments of what is essentially the use of electronic and information systems to deny, exploit, corrupt, deceive, or destroy another user's computer networks, information systems, or information, while defending one's own.[13] For the purpose of consistency within this study, I use the concept of computer-network operations (CNO) to organize and discuss the offensive and defensive applications of cyberspace.

From an American military perspective, CNO are considered as one of the five core capabilities that fall within the broader scope of information operations (IO). While the concept of IO is neither new nor revolutionary within military affairs, electronic warfare (EW) and CNO are recent additions that were established due to "the increase[ed] use of networked computers and supporting IT infrastructure systems by military and civilian

[12] Leiner et al., "A Brief History of the Internet"

[13] See Michael A. Vatis, "Trends in Cyber Vulnerabilities, Threats, and Countermeasures" in *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies* eds., Jacques S. Gansler and Hans Binnendijk, (Washington, DC: National Defense University, 2004), 101; and United States Joint Chiefs of Staff (JCS), *Joint Publication 3-13: Information Operations* (February 13, 2006), II-4.

organizations."[14] CNO are broadly defined by the Joint Chiefs of Staff (JCS) as the use of information systems to attack and exploit adversarial information systems and networks while protecting one's own, and are organized into three sub-categories consisting of: computer-network attack (CNA), computer-network exploitation (CNE), and computer-network defense (CND).

On the offensive side, there are two types of operations: CNA and CNE. Whereas computer-network attacks, which are sometimes referred to as "cyber-attacks," are deliberate acts within cyberspace by one entity to corrupt (degrade), destroy, or disrupt the information and computer-network systems of another entity.[15] Computer-network exploitations are "enabling operations and intelligence collection capabilities conducted through the use of computer networks."[16] A key theoretical distinction between the two types of offensive operations is the intended effect; CNA is intended to directly or indirectly deprive the user of the full functionality of the target system or network, whereas CNE is not intended to directly influence the target system itself, or cause any direct harm.

While on paper, the distinctions are clearly drawn between CNA and CNE, making an operational distinction is extremely difficult. Since, as Libicki points out, "an implant designed to purloin information may be indistinguishable from an implant designed to disrupt systems or corrupt information,"[17] malignant code that was implanted

[14] JCS, *Joint Publication 3-13*, II-4.

[15] Libicki, *Cyberdeterrence and Cyberwar*, 23.

[16] JCS, *Joint Publication 3-13*, II-5.

[17] See Libicki, *Cyberdeterrence and Cyberwar*, 24 and Melissa E. Hathaway, "Cyber Security: An Economic and National Security Crisis," *The Intelligencer: Journal of U.S. Intelligence Studies* 16:2 (Fall, 2008)

in an industry control system (ICS) during peacetime to extract information could potentially be used to disrupt or destroy the system during a time of conflict.

To further add to the confusion, the dual-use of CNE techniques may not even be intentional. Since understanding the total effect of a given intrusion into a target system is only possible with a complete understanding of the target system, most intrusions into foreign systems are prone to unintended consequences.[18] The first recorded computer worm (a self-replicating type of malware) that was distributed in 1988 is an example of this dynamic. The "Morris Worm," which was designed and distributed by the then-Cornell University student Robert Morris, was initially programmed with the intention of determining the size of the ARPANET. In design, by exploiting vulnerabilities in systems connected to the ARPANET, the worm was intended to copy itself indefinitely from one system to the next until it had reached the outer contours of the network and had indicated how large ARPANET had become. The unintended consequence of the experiment was that the worm took up such a large proportion of the available resources within a given system due to over-replication, that eventually infected systems would become unable to function. Within months, the Morris Worm became so virulent that it temporarily brought down the U.S. Department of Defense's nascent version of the Internet, and debilitated a known ten percent of the 88,000 computers connected to ARPANET.[19]

On the defensive side, computer-network defense (CND) or "cyber-defense," is a category of operations in cyberspace that is intended to "protect, monitor, analyze, detect,

[18] Libicki, *Cyberdeterrence and Cyberwar*, 76.

[19] Thomas A. Longstaff et al., "Security of the Internet," in *The Froehlich/Kent Encyclopedia of Telecommunications vol. 15* eds., Fritz E. Froehlich and Allen Kent (New York, NY: Marcel Dekker, 1997)

and respond to unauthorized activity."[20] As in the physical domain, the various methods of defending electronic and information assets within cyberspace can be organized into two types of capabilities: (1) purely defensive capabilities, and (2) offensive capabilities that are intended to serve a defensive purpose by deterring attacks with the threat of retaliation.

Purely defensive capabilities are techniques that do not impede upon a foreign network. They are passive defenses that absorb unauthorized activity, alert users of the intrusion, and mitigate the attack's effect. Purely defensive measures generally include techniques such as air gapping (isolating) sensitive and confidential networks and systems, implementing digital authentication for hardware and software, setting up firewalls, intrusion detection systems (IDS), and *honeypots*[21], and enforcing physical restrictions to system access. The dynamic use of these techniques can deter an adversary by raising the cost (time, effort, risk of detection, etc.) of waging an attack upon the defended system, and denying access in the first place.[22]

Offensive capabilities used for defensive purposes, on the other hand, deter by threatening the adversary with retaliation in kind, or through escalation.[23] They typically include techniques such as threatening distributed denial-of-service (DDoS) attacks with "botnets," [24] unleashing accumulated system exploits, and kinetically attacking key

---

[20] JCS, *Joint Publication 3-13*, II-5

[21] Honeypots are functionally useless decoys that are used to bait potential attackers and monitor their activity. Honeynet Project, "Know Your Enemy: GenII Honeynets," *Honeynet Project* (May 12, 2005) http://old.honeynet.org/papers/gen2/

[22] Libicki, *Cyberdeterrence and Cyberwar*, 170-172.

[23] Ibid., 28.

[24] Botnets are computer systems that have been compromised by a single command and control system that can be used to overwhelm a target system with the distribution of spam. See Randy Abrams, "The Biggest Botnet in the World," *ESET Threat Blog* (March 4, 2010), http://blog.eset.com/2010/03/04/the-biggest-botnet-in-the-world

information nodes of the potential assailant. Similar to nuclear deterrence, since offensively oriented "cyber deterrence" is only as effective as the threat is credible within the mind of the adversary, the technique of "deterrence in kind" can only work if several conditional factors are met. These factors include: the ability to attribute an attack to its source, prove the effects were a consequence of the attack, the ability to absorb the first strike, hold the adversary's assets in check, and still maintain the capabilities to strike back (second-strike capability). While for nuclear deterrence, many of these conditions can be met; in cyberspace, since it is still doubtful that even the most fundamental of conditions such as attribution can be achieved, many scholars and practitioners such as Martin Libicki and Deputy Secretary of Defense (DEPSECDEF) William Lynn doubt the ability for states to deter attacks against them by pursuing a retaliatory strategy.[25]

Why is Cyberspace Different?

As the difference in deterrence strategies demonstrated, even though the underlying principles of attacking, exploiting, and defending are common throughout both the physical and virtual domains, there are attributes of cyberspace that are unique to the virtual domain. Four such attributes (number of vulnerabilities, attribution, damage assessment, and cost variables) are discussed below.

[25] Libicki, *Cyberdeterrence and Cyberwar*, 159.

Vulnerabilities

Compared to physical assets that can only be attacked within one domain, information assets that exist within cyberspace can be attacked or exploited through any combination of kinetic and virtual means. For example, the tangible components of cyberspace such as computers, hard drives, servers, and sensors—much like a group of bunkers or barracks—are only prone to kinetic strikes. However, operating software, communications platforms, digital documents, and other types of digitally stored information on the hardware can be destroyed, compromised, or stolen using a variety of non-tangible techniques.

The number of vulnerabilities within cyberspace is further expanded by the fact that there is a positive correlation between the sophistication of the system and the number of potential exploits that could exist. As Libicki states, "the more complex the system…the more places there are in which errors can hide."[26] A system that consists of two cups connected by a piece of string, for instance, has far fewer potential exploits than a computer system that is connected wirelessly to a global network of other computer systems. Whereas information passed between the two cups could only be intercepted or exploited in two or three ways, the number of ways in which an adversary could attack or exploit the information passed between computer systems is only a matter of creativity.

[26] Libicki, *Cyberdeterrence and Cyberwar*, 18.

Attribution and Damage Assessment

There are at least two important questions that come with every act of offensive behavior in the international system: "who did it" and "what did it do?" The former question attributes an intrusion to an actor, establishes culpability, and helps the victim decide the course of action to take in response to the intrusion. The latter question, on the other hand, gauges the direct and indirect effects of the given attack, determines the appropriate response to the attack, and provides moral and legal justification for a response.

In the physical domain, answering these questions is relatively straightforward. Take for example the invasion of Poland by Nazi Germany on September 1, 1939. Using the advantages of mechanized military technology, the Germans invaded Polish territory from the Northern and Eastern borders, and swiftly led the Polish to surrender on September 27, 1939. There is no ambiguity in identifying who was involved, and directing culpability against the perpetrator.

In terms of the latter question of "what did it do," the effects of the incident were immediately visible. As an example of total war, the German and subsequent Soviet invasion of Poland led to the destruction of Polish towns and cities, and the casualties of soldiers and civilians. The British and French declared war on Germany two days after the beginning of the campaign, and the invasion is considered to be one of the first major battles of World War II.

Without the ability to answer these fundamental questions of attribution and effect, the outcome of the "September Campaign" could have been very different. Imagine, for example, the difference in response if the Polish, the British, or the French could not

determine if the invasion was by the Germans, the Hungarians, or the Romanians? Or, alternatively, imagine if the effects of the attack were not immediately visible, and the Polish were unable to determine the extent of the damage. Although these scenarios require a stretch of the imagination, the confusion that would ensue if actors were unable to attribute, or even assess the damage from an intrusion is the current state of cyberspace.

First, in terms of attribution, technical and legal difficulties often stand in the way of cyber-forensic experts. On the technical front, the relatively minimal fixed infrastructure requirements for CNA and CNE, as well as the unregulated nature of the Internet makes it extremely easy for actors to work anonymously, and to conduct offensive operations from the rear. Unlike physical capabilities that require large and often costly infrastructure, remote servers, anonymity networks (such as Tor)[27], and other publicly available online tools generally allow users to conduct operations relatively cheaply from any mobile location with a connection to the Internet.

From a legal standpoint, attributing an attack is also difficult because investigators require jurisdiction to conduct investigations within foreign networks. Users that seek to exploit or attack foreign networks can often hide behind lax domestic cyber-law, and avoid being charged by the authorities of another country. As illustrated in the 1998 "Solar Sunrise" example, even if investigators were able to track an attack back to an IP addressed associated with a foreign government, without further cooperation with local authorities to pursue the lead, investigators cannot gather direct evidence that would attribute the attack to a source. These technical and legal obstructions to attribution raise one of the greatest

[27] Tor (formerly known as, The Onion Routing Project) is a free, client software based virtual network that provides anonymity to Internet users from various traffic analysis techniques. For more on Tor and other

challenges to international politics, which is that victims of CNA or CNE are unable to distinguish between state-sanctioned activity and non-state activity. State actors that seek to gain from online espionage, for example, could hire third-party hackers from another state to exploit the target systems, and plausibly deny any allegations that tie the intrusions to their government. Victims of the intrusion would be left with either escalating the situation by taking the risk and assuming that the illicit connection exists, retaliating in private, or simply condemning the action and abstaining from any further response.

Second, another point of uncertainty inherent to cyberspace is the difficulty of assessing the purpose and the full effect of a given act. Often times due to the complexity of a target system or network, the outcome of a given act may differ greatly from the intended purpose. The unexpected interaction between multiple low-level intrusions upon the systems on a common network, for instance, may have the emergent effect of causing network-wide damage. Or alternatively, a potential attacker testing the threshold of a target system may unexpectedly engage a trip wire and cause a defensive maneuver of the system, which incapacitates the users of the system and is consequently perceived as an actual attack.[28]

Thus, because actors find difficulty in assessing the full extent of damage directly (or indirectly) caused by any given intrusion, establishing a proportional response is likewise challenging. Even if the attribution to the source is correct, without being able to distinguish an accident from an attack, or an intended consequence from an unintended

---

online tools, see: The Tor Project, *About: Tor* (September 15, 2010), https://www.torproject.org/index.html.en

[28] Libicki, *Cyberdeterrence and Cyberwar*, 75-77.

one, victims run the risk of either under-reacting and encouraging other intrusions, or over-reacting and unnecessarily escalating the situation.

Cost-Effect Ratios (Low Cost Barriers to Entry)

Another aspect unique to cyberspace is the relatively low costs associated with conducting an offensive operation. Compared to the costs associated with maintaining and deploying the capabilities required to conduct an offensive strike within the physical domain, the costs for conducting a cyber-attack are miniscule. Consider, for instance, the costs associated with maintaining a bomber squadron required to destroy a strategic power plant against the costs associated with launching a cyber-attack on the supervisory control and data acquisition (SCADA) systems that operate the power plant. Whereas the maintenance of the bomber squadron would require anything ranging from the barracks housing the aircrafts to the manufacturing of the munitions and the target acquisition systems, coordinating the cyber-attack to overrun SCADA system could potentially be done by only using publicly available equipment and information.[29] In comparison to its physical counterpart, offensive CNO are thus theoretically more cost-effective, and have a lower cost-barrier to entry for potential attackers.

[29] In June 1997, the JCS and the National Security Agency (NSA) launched a No-Notice Interoperability Exercise (NIEX) called "Eligible Received" to test the resilience of U.S. cybersecurity mechanisms against external attack. In a scenario that envisioned a crisis on the Korean Peninsula that required U.S. engagement, thirty-five NSA agents were given two weeks, and access to publicly available equipment and information to test U.S. civilian and military infrastructure. The thirty-five members were able to break into nine power grids for American cities, gain access to emergency response infrastructure, and attack 41,000 of the 100,000 Department of Defense (DoD) computer systems. See: John Adams, "Virtual Defense" *Foreign Affairs* 80:3 (May/June, 2001) and Global Security, *Eligible Receiver* (April 27, 2005), http://www.globalsecurity.org/military/ops/eligible-receiver.htm

Chapter 4: Cyberspace and the International System

Changes of and Changes within the International System

In "Continuity and Transformation in the World Polity: Toward a Neorealist Synthesis" John Ruggie criticizes Waltzian structural realism for assuming the continuity of the international system, and neglecting the Durkheimian concept of dynamic density as a potential source of system-wide change.[1] In his argument, Ruggie refers to the modern notion of sovereignty, and the redefinition of property relations within the international system as an example to demonstrate the ability of a non-structural variable to produce changes in the interaction between states. He argues that by discounting variables such as sovereignty, which is neither a unit- nor a structure-level variable, Waltz "goes too far" in his separation of unit-level processes from systems theory, and leaves nothing endogenous to the theory that accounts for changes to the international system.[2]

Waltz responds to Ruggie's argument by reiterating the purpose of structure—"to tell us a small number of big and important things"[3]—and by emphasizing the difference between two types of change: a change *within* the international system, and a change *of* the international structure itself. Waltz points out that while he agrees with Ruggie in the

[1] Ruggie refers to Emile Durkheim's concept of 'dynamic density' to show that "quantitative as well as qualitative changes" in certain unit-level elements are relevant to explaining the overall nature of a system. See, John G. Ruggie, "Continuity and Transformation in the World Polity: Toward a Neorealist Synthesis," *World Politics* 35:2 (Jan., 1983), 283-4.

[2] Ibid., 285.

latter's assertion that anarchy and power are insufficient to derive a generative theory of international politics, he still finds that Ruggie's critique is flawed because Ruggie does not discern between changes within and changes of the international system. Specifically, Waltz argues that despite its far-reaching effects, the redefinition of property relations—much like the "nuclear revolution" in military weaponry—only altered the quality of the relations between states, and not the actual substance of the relations themselves. Nuclear weapons, "reduc[ed] the odds that war will occur among the great and major powers,"[4] yet they left the enduring principles by which the structure is defined (anarchy and power) relatively unchanged. Because states continued to help themselves, and compete in the process of doing so, Waltz maintains that his structurally driven theory remains feasible.

While mediating the debate between Ruggie and Waltz over the exclusivity of structural realism is a task far beyond the scope of this study, referencing the debate itself is useful to highlight the importance of distinguishing between the types of effect a unit-level change can have upon the system. By clarifying whether the emergence of cyberspace produces a system-wide change, or a transformation of the structure itself, one can avoid the reductionist pitfall of over-emphasizing the significance of the digital medium, and specify the degree to which cyberspace will impact structural realist theory.

In this chapter, I argue that although at the current stage of the information revolution cyberspace has yet to alter the structural realist's conception of the international system, the technology's permeation into almost every facet of modern society has allowed

[3] Kenneth Waltz, "Reflections on *Theory of International Politics*" in *Realism and International Politics* Kenneth Waltz (New York, NY: Routledge, 2008), 45. Waltz also reiterates this distinction in, Kenneth Waltz, "Structural Realism after the Cold War," *International Security* 25:1 (Summer, 2000): 5-41.

[4] Waltz, "Structural Realism after the Cold War," 41.

it to still have a systemic effect. Most importantly, I argue that due to the increase in the number of vulnerabilities, and the increase in the number of potential adversaries that states could face within the virtual domain, cyberspace can effectively increase the level of uncertainty within the international system, and ceteris paribus—decrease the level of security enjoyed by great powers.

Does Cyberspace Transform the International System?

Today, the short answer to this is still no. The continuity of the structural realists' conception of the international system is maintained: the enduring dynamics of the system are still driven by the interaction of the units and its structure, and the latter is still defined by the principles of anarchy and the uneven distribution of material capabilities. States continue to be concerned (if not more so) of their need to secure their own assets and interests; and the system, moreover, continues to lack a supranational sovereign that alleviates any of the deleterious effects of the anarchic structure.

The international structure defined by anarchy, power, and the 'self-help' imperative have thus endured the technological shift into the information age; and structural realists would argue that their theories (derived primarily from the international structure) likewise remain intact and relevant. Yet, to acknowledge some counterarguments, some scholars such as Thomas Friedman, Bradd Hayes, and Thomas Barnett disagree. They emphasize the empowering capabilities of computer networks upon non-state actors and cast into question the enduring role of the nation-state as the base unit of the international system. Friedman, who coined the term "super-empowered

individuals," observes that the emergence of computer networks has transformed the world from a nation-state based "cold war system" to an interconnected "globalization system." He notes, "the world has become an increasingly interwoven place, and today…in the broadest sense we have gone from an international system built around division and walls to a system increasingly built around integration and webs."[5]

Although Friedman recognizes that nation-states will continue to play a major role in the international system, he describes the forthcoming world system as being less defined by states, and more so by the balance between states, global markets, and "super-empowered individuals." By connecting into the global network of states, multinational firms, transnational organizations, and individuals, Friedman argues that individuals and non-state groups as diverse as Osama bin Laden and the International Campaign to Ban Landmines (ICBL) will be able to act more autonomously, and unmediated by the state.

Hayes and Barnett further this argument by suggesting "system perturbation" as an alternative to the state-centric paradigm of great power conflict that dominated prior generations of thought on international conflict. In contrast to a system defined by great powers, Hayes and Barnett argue that system perturbations, or the enduring horizontal effects of pivotal events caused by non-great powers, are much more representative of post-Cold War international dynamics. By referencing the economic, political, and security-related ramifications of the September 11, 2010 terrorist attacks, Hayes and Barnett note that unlike prior forms of international conflict, which had clear adversaries and time frames, conflict in the globalized world is far more uncertain: "super-empowered

[5] Thomas Friedman, "Prologue: The Super Story," *Longitudes and Attitudes: Exploring the World after 9/11* (New York, NY: Farrar, Straus, and Giroux, 2002)

individuals" and online memes such as "Anonymous," [6] can cause wide-spread "perturbations" of the global system, and the conflicts themselves can be much less spectacular and more amorphous than the great power wars of the past.[7]

If the critics of the state-centric worldview, such as Friedman, Hayes, and Barnett, are correct in asserting that the information revolution is replacing the nation-state dominant system with a multi-actor system, then the change caused by contemporary information technologies is indeed transformative. By adding non-state actors such as the "electric herd" and "super-empowered individuals" into the fray of major international actors, the structural realists' assumption that all international actors are "like-units" is challenged. Units are no longer similar in the tasks they perform or the ends that they aspire to achieve.[8] The priority placed on security, for instance, will be largely different between a "super-empowered individual" that can hide behind domestic law, and states, which have no higher authority to make their plea. This variation in motives among state and non-state actors, then, would lead to a world system that is populated by more than just security-seeking states.

Although the possible ramifications of a change in the composition of the structural realists' conception of the international system would be quite momentous for the study of world politics, at the current stage of the information revolution, I return to the initial conclusion that the ramifications are only possibilities—nothing more. Anarchy and

[6] Chris Cox uses the group 'Anonymous' to describe an emerging type of amorphous online citizen activism that targets computer systems and networks with offensive CNO. See Chris Cox, "Anonymous 4GW (Fourth Generation Warfare)," *Campaign Reboot* (October 5, 2010), http://recampaign.blogspot.com/2010/10/anonymous-4gw.html

[7] Bradd C. Hayes and Thomas P.M. Barnett, "System Perturbation: Conflict in the Age of Globalization," in *War and Virtual War: The Challenges to Communities* ed., Jones Irwin (New York, NY: Rodopi, 2004)

[8] Waltz (1979), *Theory of International Politics*, 93.

the so-called "law of the jungle" continue to define the structure of the international system, and despite the unprecedented empowerment of non-state entities over the past several decades, no other actor in the international system has thus far been able provide a substitute for the various "political social-economic functions" currently served by nation-states, and "foster the institutions that make…peace and prosperity possible."[9] Therefore, while scholars such as David Betz may be correct in suggesting that borderless online meme's such as "Anonymous" and "4Chan"[10] are harbingers of a prospective world system described by Friedman and others, today, the structural realists' state-centric worldview has endured, and the technologies of the information revolution have not transformed the international system.

The System-Wide Effects of Cyberspace

Although cyberspace and the technologies of the information revolution have not transformed the international system, the creation of the virtual medium has had a multiplicative effect on pre-existing dynamics within the system. While the deleterious effects of the anarchic structure on state security remain unchanged, the scale of these effects has been significantly amplified because there is simply *more* of everything. There are more assets for the state to protect, more threats from which to protect them from, and more actors that are involved in the protection thereof. The following section demonstrates

[9] Kenneth Waltz, "Globalization and Governance," *PS: Political Science and Politics* 32:4 (December, 1999): 693-700, reprinted in Kenneth Waltz, *Realism and International Politics* (New York, NY: Routledge, 2008), 238.

[10] David Betz, *The Malevolence of Crowds*, http://kingsofwar.org.uk/2010/10/the-malevolence-of-crowds/.

how this increase in the sheer number of variables has increased the level of uncertainty for national security.

More to Protect. The emergence of cyberspace, and the creation of value therein, have expanded the scope of national security for heavily networked states. Because states have a vested interest to protect not only the physical integrity of the nation-state, but also the interests and welfare of its citizens, the creation of electronic and digital assets have also altered the concept of national security in both the traditional and non-traditional sense. States simply have more to protect. Whether it is the nebulous web of computer systems that support the armed forces, or those that sustain the nation's economy, the technologies that created substantial gains in efficiency and productivity are ironically the same technologies that have created a new frontier of vulnerabilities.

From the traditional security perspective, the effects of cyberspace can be seen in the newly formed agencies devoted to the maintenance of information infrastructures, and the execution of offensive and defensive missions within cyberspace. In the United States, the four individual armed service elements tasked with missions within cyberspace[11] were merged in 2009 to form U.S. Cyber Command (CYBERCOM), a new sub-unified command under U.S. Strategic Command (STRATCOM). [12] CYBERCOM, which coordinates with other defense agencies such as the Defense Information Systems Agency (DISA), coordinates U.S. military operations within cyberspace, and oversees the 15,000

[11] The four service elements include: Army Forces Cyber Command (ARFORCYBER); 24th United States Air Force; Fleet Cyber Command (FLTCYBERCOM); and Marine Forces Cyber Command (MARFORCYBER).

[12] United States Strategic Command, *United States Cyber Command: Fact Sheet* (October, 2010), http://www.stratcom.mil/factsheets/cc/.

military networks and over 7 million computer systems that the U.S. military relies on to retain the full operability of its conventional armed forces. As emphasized by the U.S. Deputy Secretary of Defense (DEPSECDEF) William Lynn, the establishment of a new four-star command is a testament to the fact that "cyberspace is a source of potential vulnerability" for the United States, that the military needs to move toward a layered defense posture within cyberspace, and that cyberspace itself has become a new domain of warfare for the U.S. military.[13]

On the government side, following the issuance of National Security Directive 42 on July 5, 1990, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established, and the Information Assurance Directorate (IA) of the National Security Agency (NSA) was tasked with the protection of the U.S. government's national security systems.[14] According to the Directive, the increase in the volume of information assets, and the emerging threats against these assets, created the need to coordinate the protection of key national security information systems.

> "Continuing advances in microelectronics technology have stimulated an unprecedented growth in the demand for and supply of telecommunications and information processing services…Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation…[and] a comprehensive and coordinated approach must be taken to protect the government's national security telecommunications and information systems against current and projected threats."[15]

[13] William J. Lynn III, "Remarks at Stratcom Cyber Symposium," *Stratcom Cyber Symposium* (Omaha, NE, May 26, 2010) Transcript available online at, http://www.defense.gov/speeches/speech.aspx?speechid=1477.

[14] National Security Directive No. 42 (July 5, 1990) Partially declassified on November 22, 1996.

[15] Ibid.

The Directive, and the tasking of NSA/IA with the exclusive protection of government networks ([dot]gov versus [dot]mil) are further indications of the expansive scope of cybersecurity. These developments corroborate the assertion that the potential threats within cyberspace are unique from prior forms of national information security, and that new, broader approaches must be taken to protect the integrity of the so called, "digital homeland."

From the non-traditional security perspective, the volume of goods to protect has also increased with the creation of the virtual domain. Economic performance, which sustains and limits a state's politico-military initiatives, has become increasingly contingent upon the performance of the various information and communications systems that underlie a country's economy. Computer systems and networks have increased the speed and volume of information that companies can process; and regardless of where one stands on the "global economy" debate, all parties can agree that information and communication systems have allowed for financial markets to be globalized, and for capital to exchange hands in near real-time speeds across the world. While some argue that these developments have merely exacerbated a preexisting international condition, the unprecedented increase in productivity, and emergence of globalized financial markets have translated into much larger profit margins for some businesses, which in turn has been crucial for the continued growth of post-industrial national economies.

In addition, the informationization of the critical infrastructure that supports human welfare has also increased the volume of assets at stake. By networking national

critical infrastructure, which often includes public utilities (electricity, water, telecommunications), emergency response services, and transportation, computer-based industrial control and supervisory control and data acquisition (SCADA/ICS) systems have become a new segment of online assets for the state to protect.[16] As simulated exercises such as "Eligible Receiver," and real-world threats such as the Conficker and Stuxnet worms indicate[17], the networking of SCADA/ICS systems onto open IP networks has opened up the state's critical infrastructure to an entirely new scale of attacks and exploits.

More Threats. Not only has cyberspace expanded the scope of national security by increasing the number of electronic and digital assets to protect; it has also had the effect of increasing the number of threats in general by providing old and new adversaries with a cost effective method of conducting offensive operations both within and outside of the virtual domain. This means that not only do states need to be continually aware of the intentions and actions of foreign state adversaries, they now need to have a defensive strategy against the myriad of potential non-state adversaries that can jeopardize national security, and who each harbor divergent motives, intents, and interests.

---

[16] According to a survey of 600 IT executives conducted by Vanson Bourne Limited in 2009, eighty percent of the respondents claimed that their SCADA/ICS systems were connected to IP networks. See: Stewart Baker, Shaun Waterman, and George Ivanov, *Into the Crossfire: Critical Infrastructure in the Age of Cyber War* (London: McAfee, 2010).

[17] The Conficker Worm was reported to have infected and impaired several hundred critical medical equipment, and the control systems of undisclosed critical infrastructure providers within the United States. More recently, the Stuxnet Worm was reported to have infected and impaired over 30,000 Windows PCs in Iran, some of which were in use at the Bushehr nuclear power plant. See: Elinor Mills, "Conficker Infected Critical Hospital Systems, Experts Say," *CNET News: Security* (April 23, 2009), http://news.cnet.com/8301-1009_3-10226448-83.html, and Harry Sverdlove, "Stuxnet Worms Shows Critical Infrastructure Attacks No Longer Just Hollywood Hype," *SC Magazine* (October 18, 2010), http://www.scmagazineus.com/stuxnet-worm-shows-critical-infrastructure-attacks-no-longer-just-hollywood-hype/article/181212/.

Because the nature of CNO complicates the process of attribution, favors the offensive, and is relatively cheap, computer-based methods of conducting offensive operations is attractive to a wide range of actors. As Michael Vatis delineated in a 2002 report on the state of U.S. national cybersecurity, the range of state and non-state "cyber attackers" includes: organizational insiders, transnational criminal groups, virus writers, foreign intelligence services, professional militaries, terrorists, ultra-nationalist hackers ("hacktivists"), and recreational hackers.[18]

For state-actors, open-source media reports documenting instances of offensive CNO suggest that while state actors have conducted actual cyber-attacks, the majority of state-based offensive operations are currently intelligence gathering efforts and probes to uncover system vulnerabilities. In the twenty year period (1990-2010) since the initial use of cyberspace for offensive operations, while examples of state-sanctioned CNA exist—the use of "electronic attacks" by the U.S. against the financial assets of Slobodan Milosevic during the 1999 Kosovo Air War[19], and the alleged Russian cyber-attacks against Estonia and Georgia in 2008[20]—the majority of reports indicate that state-based offensive CNO has been largely limited to information gathering efforts (CNE). In the September/October

[18] Michael Vatis, "Cyber Attacks: Protecting America's Security against Digital Threats," *Executive Session on Domestic Preparedness (ESDP) Discussion Paper* (Cambridge, Massachusetts: John F. Kennedy School of Government, Harvard University, June 2002), 2-10.

[19] Examples of state-sanctioned CNA are extremely limited. In October 1999, chairman of the U.S. Joint Chiefs of Staff, Gen. Henry Shelton, openly acknowledged that the U.S. had used "very limited" electronic attacks against Serbian computer networks during the air campaign. See: Elizabeth Becker, "Pengaton Sets Up New Center for Waging Cyberwarfare," *The New York Times* (October 8, 1999), and John Markoff, "Cyberwarfare Breaks the Rules of Military Engagement," *The New York Times* (October 17, 1999).

[20] Project Grey Goose, which is an open-source intelligence project organized by Jeff Carr (IntelFusion), conducted research on the Kremlin's involvement in the 2008 Russia-Georgia "cyberwar." In the two reports published by the group in 2008 and 2009, the contributors assessed that the Russian government discretely supported nationalist Russian hackers in 2008, while maintaining plausible deniability for the hacker's actions. See: Jeff Carr et al., "Project Grey Goose: Phase 1 Report" *Project Grey Goose* (October 17, 2008) and Jeff Carr et al., "Project Grey Goose Phase 2 Report: The Evolving State of Cyber Warfare," *GreyLogic* (March 20, 2009).

2010 edition in *Foreign Affairs*, DEPSECDEF Lynn noted, "more than 100 foreign intelligence organizations are trying to break into U.S. networks."[21] Annual reports by the U.S.-China Economic and Security Review Commission (USCC) going as far back as 2002 note that the People's Republic of China (PRC) has been aggressively investing in the development of offensive CNO capabilities; and in the most recent 2009 report, the USCC alleges that large bodies of circumstantial and forensic evidence indicates Chinese state involvement in the theft of "terabytes of data" from U.S. government and defense contractor systems.[22]

While for state actors, the majority of offensive CNO are currently for intelligence gathering operations that mainly target government documents, weapon systems design, and potential system and network exploits, the offensive operations of non-state actors are much more of a mixed bag. Because of the wide range in motives and interests of these non-state actors, there is similarly a wide variety in the types of offensive CNO conducted by these entities within cyberspace. Hacktivists in the PRC, for instance, have been attributed to a variety of politically motivated CNO, including: "web defacement and distributed denial-of-service attacks…[against] the United States, Japan, Taiwan, Indonesia, and South Korea"; directly attacking U.S. commercial firms with zero-day exploits and spear-phishing tactics; recruiting hackers for Chinese government agencies through online hacker forums; and proliferating malicious code to individuals and groups targeting U.S. companies.

---

[21] William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89:5 (September/October, 2010): 97-102, 99.

[22] Archived digital copies of USCC annual reports can be accessed online at: http://www.uscc.gov/index.php.

In contrast to hacktivists—whose motives and targets are politically derived—transnational crime groups that are motivated by financial gain have a different, yet similarly threatening, modus operandi within cyberspace. Albert Gonzales (28) from Florida, and his two Russian co-conspirators, for example, used a method called Structured Query Language (SQL) injections to hack into Heartland Payment Systems (NYSE: HPY), a digital payment processing company, to steal over 130 million credit card numbers.[23] While the total financial ramifications of the "biggest online theft case" has not been calculated, by factoring in fluctuations in stock price, the four million dollars stolen by Gonzales and his fellow conspirators, and the damages paid by Heartland in litigation, one can safely assume that the financial damages caused by the three individuals amount to well over ten million dollars.

Just as the increase in the volume of virtual assets decreased the overall level of certainty surrounding the efficacy of national security measures, the increase in both the number of adversarial actors, and the methods of conducting offensive operations, also decreases the confidence that states can place upon their national security policies. In both cases, the effects of cyberspace shift the threat from fearing one great attack, to what some call, "death by a thousand cuts." Stuck between defending against all possible "cuts," and having to prioritize some threats over others, states have a more difficult time knowing the effectiveness of their national cybersecurity policies, and ascertaining whether or not it is indeed sufficient.

[23] Chloe Albanesius and Erik Rhey, "Inside the Biggest Online Theft Case," *PC Magazine* 29:5 (May, 2010): 1-1, 1.

More Actors Involved. A third factor that further adds to the increased level of uncertainty is the difficulty in coordinating the cybersecurity strategies of the various actors involved in the defense of vital computer systems and networks. Because the use of a common, open-architecture IP network by a wide range of personal, commercial, governmental, and military users opens up the possibility for threats to easily pass through one sector and contaminate all sectors, the burden of securing the cyber-infrastructure of a country is distributed among all social sectors that use the Internet. Unsecure computer systems for business or general household use, for instance, can be compromised by malware such as the so-called "Storm Trojan" (Trojan.peacomm), which will recruit the system into a larger botnet that can be controlled by a centralized command-and-control system to further distribute spam and malware, conduct distributed denial-of-service (DDoS) attacks, and even harvest proprietary information.[24]

The widespread use of commercial-off-the-shelf (COTS) hardware and software in many business, government, and military systems also creates a similar problem. By having these sectors use commercially available hardware and software, the security of privileged information stored on these systems becomes contingent upon the integrity of the vendor. Take, for example, the operating systems and office productivity suites produced by Microsoft and Adobe. Because products offered by these two companies such as Microsoft Windows, Microsoft Office, and Adobe Reader/Acrobat have penetrated into almost all market sectors, and have dominated the share of each market[25], these items

[24] For details on one of the larger botnets and its infiltration methods, see: Symantec Corporation, "Outbreak Alert "Storm Trojan," *Threat Advisory Center* *http://www.symantec.com/outbreak/storm_trojan.html*

[25] According to *Net Market Share* (www.netmarketshare.com), the Microsoft Windows operating system has held over 90 percent market share in operating systems since at least January, 2009. The second ranked operating system, Mac OS, has held approximately 5 percent during the same time range.

become highly attractive targets for adversaries looking to reap the largest return on their time and investments spent searching for vulnerabilities. By having multinational corporations, governments, militaries, and civilian defense industrial bases use software such as PowerPoint and Portable Document Format (PDF), the vulnerabilities in these programs become relevant to the security of not only the documents themselves, but of the computer systems using them as well.

Some argue that COTS software is more secure than custom designed government and military software because compared to the latter, COTS software is tested by a larger group of users for flaws and threats, can adapt faster to known vulnerabilities with patches, and can cost significantly less to field. However, although this may be true, the point remains that by fielding COTS software in government and military establishments, private-sector companies carry part of the burden of securing vital systems and networks, and conversely, the public sector becomes invested in the security of their commercial hardware and software suppliers. As one publicly distributed U.S. DoD poster states, the protection of the nation's networks has become, "everyone's business."

The increase in the number of active participants in the maintenance and defense of national cyber-infrastructure leads to difficulties in coordination and cooperation. As one report by the Center for Strategic and International Studies (CSIS) cogently points out, because of the "bifurcation of responsibility (the government must protect national security) and control (it does not manage the asset or provide the function that must be

protected)" the burden of national cybersecurity became distributed, and the need for a public-private partnership (P3) to protect critical infrastructure arose.[26]

While P3 initiatives such as the National Security Telecommunications Advisory Committee (NSTAC), the National Infrastructure Advisory Council (NIAC), and the Critical Infrastructure Partnership Advisory Council (CIPAC) have all been active in the coordination of detection, protection, and response to threats in cyberspace, these initiatives have faced significant difficulties in achieving sufficient levels of coordination and cooperation.[27] Among these, the most important is the difficulty of establishing trust, and developing a willingness among participants to share information. Intelligence and defense agencies are wary of disclosing classified information that may jeopardize national security; corporations are unwilling to sacrifice their reputations by admitting to security breaches; and household users are mistrustful of the government monitoring their systems and networks. Thus, although the dissemination of known vulnerabilities and attacks are key in developing the resilience of critical systems and networks, conflicting interests between stakeholders and barriers to cooperation jeopardize the timely protection and security of these digital assets.

[26] James A. Lewis et al, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C.: Center for Strategic and International Studies, December, 2008), 43.

[27] In addition to the CSIS report, the Intelligence and National Security Alliance (INSA) have released a report on the challenges facing a cybersecurity P3. See, Joseph Mazzafro ed., *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models* (Arlington, VA: Intelligence and National Security Alliance, November, 2009).

Chapter 5: Cyberspace and Structural Realist Theory

In the previous chapter, I explained the difference between a variable causing a change of the system, and a change within the system. I determined that while the creation of cyberspace has not caused a transformation of the system, the several changes that cyberspace caused within the system raised the overall level of uncertainty that states face in pursuing security. I argued that because in the post-industrial era there are more informational assets that need to be protected from computer-based threats, more potential adversaries to protect them from, and more actors involved in the defense of these assets, states (especially heavily networked great powers) are finding difficulty in adapting to this new, informationized security environment. Under these conditions, state security agencies are confronted with the challenge of finding a balance between depending on deterring known adversaries, and defending against amorphous threats and faceless adversaries in the virtual domain.

This chapter goes on to chart the limits of structural realism by assessing how cyberspace affects the behavior of states and the stability of the international system according to arguments made by structural realists. First, structural realist arguments grounded in the security dilemma are used to understand whether cyberspace encourages competitive or cooperative behavior between states. The uses of cyberspace are analyzed according to the offense-defense balance, offense-defense differentiation, and the ability for states to perceive the motives and intents of other states. From these three criteria, I argue that because cyberspace favors the offensive, can be used to conduct both offensive and defensive operations, and can befog the process of signaling between two states, the

severity of the security dilemma is increased, and states will find it more difficult to discern optimal cybersecurity policies from suboptimal ones. Even if cooperative behavior, such as the drafting and ratification of the Convention on Cybercrime, is undertaken by states with one hand, the dangers of relying on passive defenses will lead states to develop and refine offensive computer-network capabilities with the other.

Second, I assess the impact of cyberspace on the stability of the international system from a structural perspective. Drawing on the arguments made in the previous section, this section examines whether certain polarities exacerbate or mitigate the level of competition among states, and if bipolar worlds can continue to be more stable than multipolar worlds in the information age. Basing my reasoning on the arguments made by structural realists on why bipolar systems are more stable than multipolar systems, I argue that the creation of a new virtual domain has made it difficult for states to expect stability based on the number of great powers in the system. I explain that compared to prior historical periods when stability, which is often equated with peace or the lack of major shifts in power distribution, was maintained or disturbed by the behavior (often warfare) of major military powers, today, stability is contingent on a greater number of actors. Because technological shifts have altered the nature of conflict, and the ways in which major shifts in relative power can occur, a greater number of less militarily endowed actors can upset the stability of the system by either directly threatening great powers, or altering the distribution of power by indirect, non-violent means.

Competition Under the Security Dilemma

Despite their differences, defensive and offensive realists agree on the optimal strategy of security-seeking states when the "security dilemma is at its most vicious…[and] the only route to security lies through expansion."[1] Defensive realists find that when the offense has the advantage, offensive and defensive capabilities can be distinguished, and when states believe that their adversaries are "greedy" (prioritizing non-security interests over security interests), security-seeking states should act like an aggressor and pursue competitive policies.[2] While the creation of the virtual domain does not immediately shift the security dilemma into overdrive and prescribe aggressor-like behavior to security-seeking states, I argue that the creation of cyberspace increases the severity of the security dilemma, which in turn increases the likelihood of states to pursue competitive policies by acquiring offensive capabilities within cyberspace.

Offense-Defense Balance

My argument that cyberspace increases the severity of the security dilemma can be derived by assessing three variables: offense-defense balance, offense-defense differentiation, and perceived motives. First, one method of measuring the offense-defense

[1] Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30:2 (January, 1978): 167-214, 187.

[2] Charles Glaser introduced information variables (e.g., motives and intentions) to assessing the severity of the security dilemma. He argued that a dilemma would not exist unless some states were indeed greedy states, and security-seeking states exhibiting greedy behavior were misperceived as actually being greedy states. See: Charles Glaser, *Rational Theory of International Politics,* (2010).

balance is by determining "the cost ratio of attacker forces to defender forces."[3] For every dollar that attacking state *X* spends on "conquering" a system or network of state *Y*, how much more or less does state *Y* need to invest in securing these assets? According to this approach, assuming that all other factors are relatively equal[4], if the cost of defense for state *Y* is less than the costs incurred by state *X*, then the offense-defense balance favors the defense, and the severity of the security dilemma is mitigated. Contrarily, if the costs of state *Y* are greater than those of state *X*, then the opposite is true, and the offensive has the advantage.

In cyberspace, the latter scenario often holds true and the cost of defending far exceeds the cost of exploiting or attacking a system. As DEPSECDEF Lynn explains, cost variables in cyberspace asymmetrically favor the offensive because attacking forces do not need to develop their own expensive weapon systems to launch offensive operations against another country.[5] For the price of a household computer system and access to the Internet, attacking forces can educate themselves on how to conduct offensive CNO, search target systems and networks for vulnerabilities, and use either pre-authored or self-authored malicious programming to launch attacks.[6]

Moreover, Lynn also adds that "the…ability to defend…networks always lags behind [the] adversary's ability to exploit…weaknesses" because "security and identity

---

[3] Glaser and Kaufmann note that there are several competing definitions of offense-defense balance among defensive realists. See: Charles Glaser and Chaim Kaufmann, "What is the Offense-Defense Balance and can We Measure It?" *International Security* 22:4 (Spring, 1998): 44-82, 50.

[4] A caveat that offense-defense theory holds is that vast discrepancies in power, skill, or size between two opposing sides could alter the balance measured in terms of cost ratios.

[5] William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89:5 (September/October, 2010): 97-102, 98.

[6] An example is the 1997 "Eligible Receiver" NIEX conducted by the JCS and the NSA. (See Chapter 3, FN-21)

management were lower priorities" in the creation of the Internet.[7] The barriers to entry were deliberately set low in cyberspace in order to facilitate collaboration and innovation, and as a result, defending forces constantly play a game of catch-up with the plethora of potential adversaries by scouring millions of lines of code for flaws and potential vulnerabilities in programs running on their systems, and trying to prevent attacks and exploitations before they occur. Thus, defending forces incur the various costs associated with defensive measures, including: only procuring hardware and software from authenticated domestic sources[8], maintaining skilled technicians to locate and patch vulnerabilities before the adversaries, constantly monitoring critical systems, and fielding defensive mechanisms such as firewalls, honeypots, and anti-virus software.

Offense-Defense Differentiation

A second variable in assessing cyberspace's effect on the security dilemma is whether or not offensive and defensive capabilities can be distinguished from one another, and whether defensive capabilities also have the ability to conduct offensive operations. In this approach, if offensive and defensive measures can be differentiated, then as Jervis argues, "the basic postulate of the security dilemma no longer applies…[and] a state can increase its own security without decreasing that of others."[9] Although Jervis adds the caveat that states may still choose to procure offensive capabilities at the detriment of the

[7] Ibid2.

[8] The cost here is having to procure domestically manufactured and authenticated products instead of COTS hardware and software produced abroad.

[9] Jervis (1978), "Cooperation Under the Security Dilemma," 199.

security of others if the offensive advantage is great enough; competition over offensive capabilities can still be mitigated if states could differentiate between another state's offensive and defensive measures.

For example, a country could increase its own security without undermining the security of its neighbor by procuring passive defense measures such as the hardening of key critical infrastructure and military installations. Although in a nuclear age, one could argue that defensive maneuvers such as the hardening of silos exacerbates the severity of the security dilemma by risking the value of the opponent's nuclear arsenal, in a conventional sense fortification is an example of a clear offense-defense differentiation because hardened facilities are immobile, cannot be used as part of an offensive operation, and because these facilities diminish the opponent's expectations of a swift victory.[10]

In cyberspace, the differentiation between offensive and defensive capabilities is quite weak. While the digital equivalent to fortifications and hardened facilities exist (e.g., firewalls, air gapped systems), many of the passive defenses are developed by programmers that straddle a very fine line between being a security researcher ("white hat") and a hacker with offensive motives ("black hat"). Consider, for instance, Ehud "The Analyzer" Tenenbaum, the teenager that hacked into the Pentagon's Defense Information Infrastructure in 1998, and Kevin Poulsen, a former black hat who infiltrated federal networks and exposed front companies run by the U.S. Federal Bureau of Investigations

[10] Jervis distinguishes between offense-defense differentiation in pre-nuclear and in nuclear periods. In pre-nuclear periods, fortifications could be considered purely defensive because it served no other purpose other than keeping the adversary out. In the nuclear period, because retaliatory deterrence relied upon the credible threat that one's population was constantly held hostage by the other's nuclear forces, fortifications could detract from the stalemate and provoke one side to preemptively strike the other—thereby taking a purely defensive maneuver and having it favor the offensive. See, Jervis (1978), "Cooperation Under the Security Dilemma," 206.

(FBI). Tenenbaum, who was sentenced to six months of community service in Israel, temporarily switched over to "white hat" activities by becoming a director of the Canadian computer-security consulting firm, Internet Labs Secure.[11] Poulsen, on the other hand, who is currently a senior editor at *Wired* magazine, switched between white and black hat activities on a daily basis before his indictment. By day, Poulsen worked as a consultant to test the security of computer systems at the Pentagon and worked as a computer security researcher for SRI International and Sun Microsystems. By night, Poulsen allegedly hacked into FBI and military computer systems to reveal details of ongoing FBI investigations, expose front companies used by the FBI, and steal military documents.[12]

The ability for hackers and computer programmers to easily switch between benign and malign activities, and the difficulty of determining whether an individual is involved with white or black hat activities leads to the inability of states to differentiate between the offensive and defensive intentions of another state's cybersecurity posture. Even if states employ "ethical hackers" to test the resilience of their own systems, the same individuals that can be tasked to carry out defensive missions can just as easily be tasked to carry out offensive operations against foreign systems and networks.[13] As a result, because of the inability for states to distinguish between offensive and defensive capabilities of

[11] Kim Zetter, ""The Analyzer' Hack Probe Widens; $10 Million Allegedly Stolen from U.S. Banks," *Wired: Threat Level* (March 24, 2009), http://www.wired.com/threatlevel/2009/03/the-analyzer-ha/?intcid=postnav.

[12] John Enders, "California Computer Whiz is First Alleged Hacker Charges with Espionage," *The Associate Press* (December 10, 1992).

[13] For dangers on hiring so-called "reformed hackers," see: M.E. Kabay, "Hiring Hackers (Parts 1 & 2): Verify, then Trust, then Verify," *Network World* (August 17, 2009) and Vito Pilieci, "For Security, Hire Hackers: Insistence on Certificates Overlooks Real Experience, Consultant Says," *National Post* (November 11, 2009).

other states within cyberspace, CNO exacerbates the severity of the security dilemma, and decreases the level of security experienced by states.

Information Variables: Perceiving the Motives and Intents of Others

A third variable in assessing the severity of the security dilemma is the information that states have of the motives and resolve of other states. In other words, how states perceive the motives of another state can influence their decision to take a competitive or a cooperative approach in interacting with the state. For instance, through mutual interaction preceding a crisis, if state *X* believes that state *Y* is a greedy state because of its acquisition of purely offensive weapon systems, then depending on the material wellbeing of state *Y*, state *X* may either opt to pursue a competitive policy of engaging in an arms race with state *Y* or try to avoid confrontation by brokering an arms limitation agreement with state *Y*.[14]

Outwardly observable actions that states take in both peacetime and wartime can therefore influence the perception adversaries have of a state's motives and immediate intentions. While as critics are correct in pointing out, the intentions of states often change, and the actions of states are sometimes reflections of the ends they desire and not based on the information they perceive (e.g., appeasement preceding World War II out of a desire to avoid war at all costs); states nevertheless continue to invest heavily in deciphering the motives and intentions of other states to inform their own actions. The information they gather by reading into costly signals is often used to weigh the potential costs and benefits

[14] Glaser (2010), *Rational Theory of International Relations*, 81-85.

of pursuing either a competitive or a cooperative policy.[15] If states are unable to communicate their motives and intentions with other states, then the uncertainty and risk that the state incurs by taking cooperative strategies is increased.

As a medium that can be used for offensive and defensive operations, cyberspace can take on the function of transmitting and receiving costly signals that can be used to indicate a state's motives and intentions. If the acquisition of long-range heavy-bombers is an indication of a state's intention of carrying out offensive operations in the physical domain, then the overt development of a highly sophisticated computer worm, or the probing of foreign networks during peacetime are indications of a state's intentions of carrying out offensive operations within the virtual domain. The perceived actions of states within cyberspace are thus just as important as their actions within the physical domain in shaping how other states interact with it.

Cyberspace, however, is a unique virtual medium, and while it is how states make use of the medium that determines how others perceive it, cyberspace is unique in that states do not have complete control over how they signal their intentions to other states. As "Solar Sunrise," the "Russia-Estonian Cyber War" and other cases of "hacktivism" illustrate, cyberspace enables users other than the state to impersonate state-sanctioned activity within cyberspace. Although states are traditionally responsible for communicating their motives and intentions to others through their words and deeds, cyberspace creates another "bifurcation of responsibility and control" wherein states are unable to verify and trust the signals that are allegedly transmitted by another state. For

[15] David M. Edelstein, "Managing Uncertainty: Beliefs about Intentions and the Rise of Great Powers," *Security Studies* 12:1 (Autumn, 2002): 1-40.

example, hypothetically, even if countries like China and the United States were to denounce the further securitization of cyberspace officially by signing onto the equivalent of an arms control treaty, if these countries were unable to control how domestic users decided to use the Internet, or more importantly, if they could plausibly deny their connection to offensive CNO emanating from within their national IP ranges, then there would be little reason for these countries not to cheat and develop offensive cyber-capabilities as a hedge against others cheating as well.

In short, because cyberspace favors the offensive and incentivizes competitive behavior, the intensity of the security dilemma is increased. Today, although countries like the United States have publicly emphasized the development of their defense focused strategy (instead of a retaliatory deterrence strategy)[16], these states are also simultaneously engaged in developing and constantly updating offensive capabilities that will enable them to penetrate foreign networks to attribute attacks, monitor the offensive capabilities of other states, and in some cases, to launch a cyber-offensive to gain information superiority in times of conflict.[17] Moreover, because the life-cycle of offensive cyber-capabilities are

[16] Despite the acknowledgment by military personnel of the U.S. military's offensive cyber-capabilities and missions, DEPSECDEF Lynn's explication on CYBERCOM and the U.S. military's cybersecurity posture focused almost entirely on defensive measures. See: Keith B. Alexander, "Advanced Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command: Section 7," *United States Senate Armed Services Committee Hearing* (April 15, 2010) and William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89:5 (September/October, 2010): 97-102.

[17] While direct details are rarely revealed, the development of offensive capabilities by countries such as the United States and China are often implied by government and military insiders. See: John Markoff, David E. Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *The New York Times* (January 26, 2010) and John J. Tkacik, Jr. "Trojan Dragon: China's Cyber Threat," *The Heritage Foundation Backgrounder* (February 8, 2008) http://www.heritage.org/research/AsiaandthePacific/bg2106.cfm, Elizabeth Becker, "Pentagon Sets Up New Center for Waging Cyberwarfare," *New York Times* (October 8, 1999), and Timothy Thomas, *Decoding the Virtual Dragon* (Fort Leavenworth, KS: Foreign Military Studies Office, 2007).

shorter than physical weapon systems, the competition to constantly maintain the newest arsenal of exploits is likely to be faster paced and continuous.

The Evolution of Warfare, Polarity, and Structural Stability

Most structural realist theories are descriptive theories that describe the behavior of states according to the conditions and constraints exerted on them by the various independent variables within the international system. The assessment of a system's polarity, as well as variables such as offense-defense balance, offense-defense differentiation, and the perception of motives and intentions lead structural realists to make deductive assertions about the severity of security competition between states, and whether the objectives of states are best served by engaging in competitive or cooperative policies. The assessment of the variables, moreover, lead structural realists such as Waltz and Mearsheimer to make predictive assertions about the stability of some configurations of the world (e.g., balanced bipolar, unbalanced multipolar) over others.

In the previous section, I examined the effects of cyberspace on the severity of the security dilemma by assessing its effect on offense-defense variables, as well as the ability of states to communicate their motives and intentions to other potential rivals. According to these material and informational concepts, I argued that the complex, offensive-favoring nature of cyberspace increases the uncertainty experienced by state-actors, which in turn decreases their perceived level of security, and leads states to pursue competitive behavior.

In this section, I turn to the structure of the international system, or arguments based on the distribution of power ("polarity") to further examine the effects of cyberspace on the

severity of security competition between states. I argue that, first, structural realist arguments that stem from the distribution of power are constrained by the technological frontiers of the times. The structural realists' interpretation of capabilities and power emphasize conventional and strategic nuclear military assets because shifts in relative power have usually occurred historically by way of physical, "trinitarian" warfare. Arguments that bipolar systems can mitigate the deleterious effects of the international system, and increase the stability thereof, are thus built upon the underlying assumption that (1) great powers are those with the power bases to support their hulking militaries, (2) that the stability of the system primarily depends on the behavior of these great powers, and (3) that consequential shifts of relative power usually occur by way of security competition, or warfare.

Next, I argue that because the underlying assumptions on security competition between states have changed due to the information revolution, the argument that some distributions of power are more stable than others is less relevant. In making this final argument, I rely on the literature of military theorists to explain that today the nature of warfare has changed to include a supplementary layer of non-violent warfare that involves more actors, is less defined, and has a global reach. In this "networked" security environment, where the interconnectivity between private citizens, businesses, governments, and militaries allow a variety of actors to directly or indirectly threaten the security of states, the notion that a world defined by two preeminent superpowers is more stable than other worlds creates a false sense of security, and overlooks a reality wherein even superpowers can become victim to significant losses in relative power through this nascent, yet rapidly developing layer of non-violent warfare.

Technological Frontiers and Structural Realist Theories

First, the structural realists' interpretation of power and conflict are bound by the limits of technological possibility. Just as the business concept of "electronic commerce (e-commerce)" could not have been envisioned prior to the development of micro-computing and the Internet; prior to the creation and recognition of cyberspace as a legitimate domain of warfare, wars could hardly be conceptualized as anything other than its "trinitarian" (or, "Clausewitzian") form.

Warfare in this earlier sense was viewed as the final extension of international politics: they were initiated by states, fought by professional militaries, and experienced by people (civilians). Individuals (or non-state actors) were clearly distinguished from states and professional militaries in the roles that they each played. From this perspective, individuals, who entered into a social contract with their state, were considered to have foregone their right to the private use of force in exchange for the state's guarantee to provide security, regulatory functions, and legal remedy to disputes. States, on the other hand, which have never existed in a hierarchically ordered political system, were given a monopoly over the use of force within the international system in exchange for the burden of having to fend for itself in the anarchic realm.[18]

The emphasis of states and professional militaries over individuals and non-state actors in trinitarian warfare also influenced the structural realists' definition of power. Although power is initially described by Waltz as the general distribution of capabilities

[18] Martin Van Creveld, *The Transformation of War* (New York, N.Y.: The Free Press, 1991), 35-39.

that differentiate states according to how well, or how poorly, they can accomplish common tasks, the capabilities that are emphasized over others in structural realism are military capabilities. Because structural realists believe that the ability to forcibly coerce an adversary is the "*ultima ratio"* of international politics, structural realists use actionable military capabilities to measure states against one another in the international system. As Mearsheimer clearly summarizes, "great powers are determined largely on the basis of their relative military capability. To qualify as a great power, a state must have sufficient military assets to put up a serious fight in an all-out conventional war against the most powerful state in the world….[and] in the nuclear age great powers must have a nuclear deterrent that can survive a nuclear strike against it, as well as formidable conventional forces."[19]

By defining the world system according to the Westphalian nation-state system, and viewing warfare as a clearly defined trinity between the state, the military, and the people, the contours of structural realism are shaped and constrained by the physical reality in which it exists. For example, structural realists were able to reduce the billions of interacting entities within the world system to great powers, and assert that the stability of the international system depended on the behavior of these great powers because to some extent the technological constraints of the times limited who could participate in international conflict, and how they were waged.

Today, as with any other transitional period in history, the world system is marked by continuities and discontinuities, and technological breakthroughs have both reinforced

[19] Mearsheimer (2001), *Tragedy of Great Power Politics*, 5.

and changed the nature of international conflict. On one hand, despite the fall of the Soviet Union and the widespread distribution of information and communications technology, many find that the present world is remarkably similar to the period defined by the Cold War. The world is still populated by self-regarding nation-states that coexist in an anarchic system; strategic nuclear weapons continue to deter these powerful, nuclear-armed states from engaging in all-out war; and states that possess and can sustain the most powerful militaries continue to cast the longest shadows within international politics by maintaining "pre-eminent offensive cybercapabilities."[20] Structural realists such as Waltz argue that "globalization is the fad of the 1990s" and that states are no more economically or politically interdependent than they were in the early twentieth century.[21] He argues that even the fear of terrorism that was sparked by the September 11, 2001 attacks is neither novel nor system transforming, and that terrorism "contribute[s] to the continuity of international politics."[22] Selections of recent structural realist literature, therefore, seems to collectively point to the conclusion that because the underlying conditions of the world are largely unchanged, the propositions made by structural realism still maintains its explanatory power of system dynamics.

On the other hand, however, while aspects of the physical realm remain relatively unchanged since the Cold War, structural realists discount the systemic changes brought about by the emergence of a new, virtual domain of interaction in the post-Cold War

[20] James Lewis commenting on U.S. offensive CNO capabilities while discussing the difficulty of maintaining a retaliatory deterrence strategy in the information age. See: John Markoff, David E. Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *The New York Times* (January 26, 2010).

[21] Kenneth Waltz, "Globalization and Governance," *PS: Political Science and Politics* 32:4 (Dec., 1999): 693-700, 693.

period. As previously argued, the information revolution and the creation of cyberspace are much more than enablers of globalization. From a security perspective, the virtual domain has begun to change the nature of warfare, and the means by which it is fought. As Col. William Bayles (US Army) noted in an article in *Parameters*, as the result of the "proliferation of computers and ever-increasing computer power available to nearly every private citizen in developed countries," computer-networks and cyberspace will "redefine how we wage war and, in many cases, blur the current line between economic competition and warfare."[23]

The Evolution of Warfare

The information revolution and the creation of a virtual domain have altered the nature of warfare in two important ways: (1) how wars are fought, and (2) who fights them. First, the types of security competition in the information era in many ways no longer resembles its trinitarian past. Wars today are not only an engagement of two professional militaries interlocked in physical combat over political ends, but they are also non-violent competitions over economic and informational superiority to achieve economic, political, and even social ends. While some argue that "war" is not the apt term to apply to the wide range of offensive activities that are being conducted against commercial, educational,

[22] Kenneth Waltz, "Chapter 31: The Continuity of International Politics," in *Worlds in Collision: Terror and the Future of Global Order* eds., Ken Booth and Tim Dunne (New York, N.Y.: Palgrave Macmillan, 2002): 348-354, 354.

[23] William J. Bayles, "The Ethics of Computer Networked Attack," *Parameters: U.S. Army War College* 31:1 (Spring, 2001): 44-61, 44.

governmental and military targets within cyberspace,[24] the offensive CNO conducted against the "soft digital underbelly" of heavily networked countries indicates that these activities, like violent warfare, have the (often intended) effect of undermining the comprehensive power of states and shifting the distribution of power to one's favor.[25]

Adversaries to a heavily networked, military power like the United States can increase their relative power by using CNO to directly or indirectly undermine the comprehensive national power of the United States. They can, for example, take a direct approach by compromising weapon systems, as well as logistical and information networks; or an indirect approach, by interfering in commercial activities by U.S.-based firms, or by stealing valuable intellectual property to weaken the economic and technological competitiveness of American firms and research institutions. In taking these measures, because cyber-based operations are often difficult to attribute, are non-violent in nature, and have not been considered *casus belli*, these adversaries, either unitarily or in unison, can attempt to undermine the socio-economic and military power sources of a country like the United States without having to directly confront the guns of the military powerhouse.

In recent years, the newfound types of threats to comprehensive power have begun to materialize at an accelerating rate. According to U.S. military estimates in 2010, over 100 states are thought to already have some proficiency in offensive CNO, and the main U.S. military network, the Global Information Grid (GIG) is subject to over three million

---

[24] Amit Yoran, "Cyberwar or Not Cyberwar? And Why that is the Question," *Forbes: The Firewall* (May 25, 2010), http://blogs.forbes.com/firewall/2010/03/25/cyberwar-or-not-cyberwar-and-why-that-is-the-question/.

[25] James Adams, "Virtual Defense," *Foreign Affairs* 80:3 (May/June, 2001): 98-113, 105.

unknown probes per day by potential adversaries.[26] Multinational companies are experiencing multi-billion dollar losses due to compromises in computer security and intellectual property theft,[27] and online "memes" such as "Anonymous" have already begun to wage an offensive against government regulatory and oversight bodies by using offensive CNO.[28]

The broadened scope of security competition and warfare leads to the second point that the primary actors in these conflicts have also veered from the trinitarian past. Unlike the Cold War and the two World Wars before it, wars today are not only fought by professional militaries for political ends, but are also waged by private citizens and non-state actors for a variety of reasons. The information revolution, and the creation of cyberspace have contributed to this change both indirectly and directly. In terms of indirect influences, as George Tenet warned in February 2001, "the same technologies that allow individual consumers in the United States to search out and buy books in Australia and India also enable terrorists to raise money, spread their dogma, find recruits, and plan operations far afield."[29] The tools that have emerged alongside the creation of cyberspace have helped enable loosely networked non-state agents to successfully engage state governments and professional militaries in low-intensity conflict throughout the world. While critics are correct in asserting that non-state groups have used terrorist and insurgent

[26] See William Lynn (2010), "Defending a New Domain," and Clay Wilson, "Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," *Congressional Research Service (CRS) Report for Congress* (November 15, 2007), 14.

[27] Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel, "Economic Impact of Cyber-Attacks," *Congressional Research Service (CRS) Report for Congress* (April 1, 2004), 1.

[28] Chris Cox, "Anonymous 4GW (Fourth Generation Warfare)"

[29] George Tenet, "The Worldwide Threat 2001: National Security in a Changing World," Testimony before the Senate Select Committee on Intelligence (February 7, 2001).

tactics prior to the information revolution, and that current low-intensity conflict is a "resurgence" rather than a "revolution" of style, the major difference between the old and the new is perhaps scale. Cost-effective, discreet, and mobile technologies such as cell phones, public wireless hotspots, and social networking platforms have allowed transnational terrorist and criminal organizations such as Al Qaeda to communicate to a broader global audience, better organize, obtain intelligence, and avoid detection by law enforcement and professional militaries.[30] Even computer amateurs whose allegiances lie with such religious fundamentalist groups can join cyber-offensives by networking themselves to organized criminal syndicates that offer CNA tools such as botnets, zero-day exploits, and pre-authored viruses for sale.[31]

Cyberspace has also directly contributed to the blurring of traditional lines between state combatants and civilian non-combatants by providing non-state entities with the means to directly affect the distribution of relative power within the international system. While this does not imply that any individual *can* or *will* wage full-scale war against a military power like the United States, the change is best understood in terms of potential. As James Adams cogently summarized, "I have the power, the capability, sitting in my home with my computer and my modem--if I only understood how to do it—to wage

[30] Uses of the Internet in recent low-intensity conflict between Al Qaeda (AQ) affiliated groups and state-entities were noted in reports following the 2007 NATO Advanced Research Workshop on Responses to Cyber Terrorism. See in particular Philip B. Brunst, "Use of the Internet by Terrorists: A Threat Analysis," in *Responses to Cyber Terrorism* Centre of Excellence Defence Against Terrorism (Amsterdam, Netherlands: IOS Press, 2007): 34-60, and Ashlee Woods, "Terrorists and the Internet," in *Understanding Terrorism: Analysis of Sociological and Psychological Aspects* Suleyman Ozeren et al. eds., (Amsterdam, Netherlands: IOS Press, 2007): 270-280.

[31] Clay Wilson, "Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," *Congressional Research Service (CRS) Report for Congress* (November 15, 2007), 15-18.

war."[32] In contrast to the Cold War era where only state actions, especially those undertaken by great powers, had any meaningful sway upon the distribution of relative power, today, individuals and non-state actors with the proper tools and training are capable of having an active role in the shifts of relative power that take place between states. Whether this is done by stealing privileged information and destroying the servers of major multinational corporations, or by directly disabling military systems such as Blue Force Tracker,[33] non-state actors that were traditionally given non-combatant status now have the potential to cause consequential effects upon the systems-level from the comfort and security of their homes.

The information revolution and the creation of a virtual domain have therefore altered the image of war that was used to describe the ultimate end game of international politics in previous ages. This assertion is different from arguing that modern ICT has "revolutionized" warfare, or that war today no longer resembles the physical engagements of yesterday. War is still very much about state militaries, about achieving political ends, and about the use, or the threat of using physical force to achieve them. War is still the final arbiter of disputes in the international realm; and the means of waging it, are still the ultimate ratio by which the international system is ordered.

[32] James Adams, "Information Warfare: Challenge and Opportunity," *USIA Foreign Policy Agenda*, November 1998 quoted in, Bayles (2001), 1.

[33] Jorge Muñiz Jr. notes in his thesis that the U.S. military's dependence on systems that exist within cyberspace (Blue Force Tracker, GPS, Predator feeds etc.) creates vulnerabilities that can be exploited by a variety of adversaries including Chinese hackers. See: Jorge Muñiz Jr., *Declawing the Dragon: Why the U.S. must Counter Chinese Cyber-Warriors* (Master of Military Arts and Sciences Thesis) (Fort Leavenworth: U.S. Army Command and General Staff College, 2009), 5.

However, what cyberspace has done is that it has created a new layer of conflict—or a new field in which both state and non-state actors can supplement their actions in the physical domain to achieve the economic, political, and social ends they seek. In this virtual domain, states no longer hold a monopoly over the use of force, the duration and rationale for conflicts often blur and merge, and power is no longer a matter of measuring the distribution of material capabilities among nation-states. In the post-Cold War period, ongoing international conflicts such as the so-called U.S led "Global War on Terror," the Taiwan Strait Crisis, and the Russo-Georgian Conflict have demonstrated that international conflict today is an interwoven narrative of traditional state-on-state conflict with this still nascent level of virtual conflict.

In the Taiwan Strait Crisis, for example, on one level the crisis is defined by the three major incidents (1954-5, 1958, 1995-6) wherein the PRC launched armed offensives against Taiwan (Republic of China, ROC), and the United States intervened militarily to deescalate the situation. On another level, however, the long standing tension between the PRC, the ROC, and the United States has manifested in the ongoing "hacker wars" that began in 1999 after former Taiwanese President Lee Teng-hui's controversial "special state-to-state relations" comment, and also after the 2001 Hainan Incident, where a U.S. EP-3 naval reconnaissance aircraft collided with a People's Liberation Army Navy (PLAN) J-8 interceptor.[34] According to several reports, PRC hackers have conducted online propaganda campaigns by defacing American and Taiwanese government and military websites; penetrating and stealing privileged information from American companies; and

[34] Bryan Krekel et als. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Networked Exploitation* (McLean: Northrop Grumman, October, 2009) and Mara Hvistendal, "The China Syndrome," *Popular Science* 274:5 (May, 2009): 60-65.

stealing classified information regarding weapon system design, logistics, and military command and control (C2) systems.[35]

In this cross strait "cyber-conflict," although some experts suggest that some of the intrusions were likely state-sponsored based on the sophistication of some of the methods used, we can still see the differences between the two layers of conflict, as well as how they intersect. In the virtual level of conflict, non-state actors are much more involved in the conflict. Highly trained individuals are potentially capable of undermining state power by directly accessing and compromising government and military systems, and at times, the motives and intentions of some of the ultra-nationalist actors diverge from that of the state.

Polarity and International Stability

If the underlying conditions that support the structural realist theories change, then the question becomes, do structural realist theories also have to change? More specifically, if warfare and shifts in relative power are no longer monopolized by states with hulking militaries, then how accurate are structural realist arguments that base their expectations of stability on the number of these "great powers" in the international system?

From the defensive realist perspective, Waltz has argued that bipolar systems are favorable to multipolar systems because, "two great powers can deal with each other better than more can."[36] In a mature bipolar world[37], he finds that pairs of great powers need only

[35] Media coverage on alleged Chinese CNE into U.S. government and military systems are mainly regarding cases such as "Titan Rain" (2005), and "GhostNet" (2008-9). For a comprehensive timeline of known incidents, see: Krekel et als. (2009), 68-74.

[36] Waltz (1978), *Theory of International Politics*, 193.

worry about the actions of the other, that each of the powers have greater flexibility in their policies, and because all states are security-seeking states, both great powers will pursue conservative strategies that will mitigate the competitive nature of the international realm.

From the offensive realist perspective, Mearsheimer also adds that bipolarity is the most stable type of system because war is more likely in multipolar systems. He explains his reasoning with three points:

> First, there are more opportunities for war, because there are more potential conflict dyads in a multipolar system. Second, imbalances of power are more commonplace in a multipolar world, and thus great powers are more likely to have the capability to win a war, making deterrence more difficult and war more likely. Third, the potential for miscalculation is greater in multipolarity: states might think they have the capability to coerce or conquer another state when, in fact, they do not.[38]

In both perspectives, Waltz and Mearsheimer are able to conclude that bipolar systems are more stable because they hold the underlying assumption that systemic stability, which Waltz defines as "no consequential variation taking place in the number of principal parties that constitute the system,"[39] is determined by the great powers, and can either be maintained or disturbed according to their behavior.

In a world where warfare is a tool that is securely held in the state's tool shed, and the means to fight them is generally limited to physical combat operations and kinetic

---

[37] Waltz defines a "mature" bipolar world as one in which the distribution of power between the two major states is relatively balanced, and both parties "behave as sensible duopolists"—meaning, they both strive to moderate the intensity of conflict while still being cautious of the other. See: Waltz (1978), *Theory of International Politics*, 203.

[38] Mearsheimer (2001), *Tragedy of Great Power Politics*, 338.

[39] There is no strict definition for stability that is commonly held by structural realists. Waltz defines stability according to the changes in relative power at the highest levels of the system, whereas Glaser, Jervis,

strikes, it is perhaps reasonable to predominantly focus on the behavior of great military powers to deduce conclusions about the stability of the international system. However, as I have previously described, war in the information era has changed in both how it is fought, and by whom. In this evolved form of warfare where there are more active participants, and violent conquest is not the only means to alter the distribution of power, the problem with maintaining the assertion that stability can be explained by a system's polarity can be understood by asking three questions.

First, *is violent warfare still the only means to rapidly change the distribution of power?* Waltz asserts that, "war aside, the economic and other bases of power change little more rapidly in one major nation than they do in another." He further explains that while "entering the club" of great powers was easier when great powers were "large in number and smaller in size," in a bipolar Cold War system where there were two predominant superpowers, the sheer gap in economic power between the top two and the rest, as well as the military technology of the times raised the barriers to entry so high that few others had a chance of gaining entry by way of their own efforts.[40]

However, in the post-Cold War period, while the United States has retained its role as the sole superpower within the system, the impermeability of its power base does not seem as secure as it was prior to the information revolution. Increased dependence on information and communications technologies have enabled the United States to maintain its technological edge over other states on one hand, but on the other, the systems and networks that promote innovation and stimulate economic growth are also the sources of

---

Mearsheimer and others seem to define stability according to the likelihood of conflict, or war. The definition used here is taken from, Waltz (1978), *Theory of International Politics*, 161-162.

[40] Waltz (1978), *Theory of International Politics*, 177.

new vulnerabilities that could potentially undermine the sources of American power. As William Lynn warns:

> Every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies. As military strength ultimately depends on economic vitality, sustained intellectual property losses could erode both the United States' military effectiveness and its competitiveness in the global economy.[41]

In the increasingly complex environment created by the use of networked systems within cyberspace, violent warfare is not the only means of rapidly shifting levels of relative power. Novel forms of economic warfare as well as industrial espionage can also directly threaten the power bases of developed states. Accidents, insider sabotage, cyber espionage, and intentional acts of offensive CNO from anywhere in the world could lead to the short-run destabilizing of highly networked countries, as well as the long-run possibility of lesser powers using stolen intellectual property and privileged information to raise their relative economic and military power.

Second, *does polarity still constrain the ability of actors to conduct offensive behavior?* According to Mearsheimer, bipolar systems are more stable because there are fewer opportunities for great powers to go to war in a bipolar system. When two states hover above all others, the argument goes, there is only one possible great power conflict dyad. When compared to a tripolar system where there are six such dyads, the difference becomes clear. Even if one considers great powers going to war against minor powers,

[41] Lynn (2010), "Defending a New Domain," 100.

Mearsheimer argues that because bipolar systems are more "rigid" (allegiances between great and minor powers are tighter), the opportunities for great-minor conflicts to erupt is still less than in multipolar systems.[42]

Although this reasoning remains valid for the trinitarian sense of warfare, the opportunities to engage in war are less dependent on polarity when non-violent wars can be waged in the virtual domain. Trinitarian wars in the physical domain are usually overt, and decisive. During the Cold War, for instance, the United States was deterred from launching a nuclear first-strike against the Soviet Union because doing so would lead to a retaliatory strike, which would result in a decisive, macabre end. Likewise, the United States was also deterred from using military means to take Hungary or Poland because doing so would set off a chain of responses that would risk dragging the two superpowers into direct physical confrontation.

Today, however, as states and other actors are increasingly able to accomplish similar political ends through discreet, non-violent wars within cyberspace, the risks are much lower, and the actors have a greater range of autonomy to engage in such non-violent conflicts. As this new form of conflict, which can be described as "death by a thousand paper cuts," emerges and gains recognition, using great power conflict dyads to continue explaining system stability creates a false sense of security, and great powers may not realize the threat of cyber-enabled adversaries, great and small.

Third, *does miscalculation still only apply to multipolar systems?* Structural realists have argued that because of the rigidity of bipolar systems, wherein the capabilities of each great power is not dependent on the capabilities of its allied minor powers, the great powers

[42] Mearsheimer (2001), *Tragedy of Great Power Politics*, 339-341.

in a bipolar system have a less tenuous task of calculating the capabilities, intents, and resolve of potential rivals. In contrast to multipolar systems, these great powers do not need to look for windows of opportunity to coerce or conquer other great powers within the system based on shifting alliances because there is only one potential great power rival to worry about. Moreover, as bipolar worlds mature, repeated interactions between the two great powers supposedly allow for clearer lines of communication to signal each other's intents and resolve, and there is a smaller margin of error associated with conflicts arising from misinterpretation or false hopes of success.

The difficulty of attributing attacks, measuring capabilities, and identifying actors in cyberspace raise the threat of miscalculation and unintended consequences arising within the international system irrespective of polarity. During the Cold War, states could depend upon military net assessments, early warning systems (launch detection satellites, over-the-horizon radars, and airborne early warning and control systems), and "Hot Lines" to mitigate the likelihood of unintended conflicts arising from miscalculations or accidents. Today, as recent cases such as Solar Sunrise (1998), the Estonian Cyberwar (2007), and Operation Buckshot Yankee (2008)[43] indicate, the complexity of information systems and networks has made it difficult for states to identify their potential state-based and non-state adversaries, calculate the level of threat they pose, and differentiate between accidents and intentional attacks. Consequently, CNO has become an enticing tool for actors that seek anonymity and plausible deniability for attacks, and a nightmare for defending entities that are left with little evidence to base their response on. This environment, therefore, raises

[43] Lynn (2010), "Defending a New Domain," 97.

the danger of conflict arising from miscalculation and misperception regardless of the number of great powers within the system.

In sum, while in some respects the advent of cyberspace, and the securitization of this new virtual medium buttresses the continuity of the structural realist view of international politics, the unique, force multiplying aspects of this technology also produces the potential for "virtual conflict" to upset the state- and military-centric view of international politics and war. Today, as some predict the world to be headed toward a new age of bipolarity between the United States and the People's Republic of China, depending on the notion that bipolar worlds mitigate the competitive nature of the international system to inform policy threatens to create a false sense of security that dangerously overlooks the potential for non-state actors, lesser powers, and even the great powers themselves to use offensive, computer-network operations to alter the distribution of power, and foment conflict within the global realm.

Chapter 6: Conclusion

This essay argued that the "information revolution" produced significant changes within the world system. It found that these changes, such as the ability to create value within a virtual domain, the erosion of boundaries between state and non-state actors, and the evolution of international conflict and warfare, can potentially favor the offensive usage of certain information and communications technologies, and act as a destabilizing force within the international system.

First, I argued that the world today is marked by signs of continuity and change. The continuity of the structural realist worldview in today's world can perhaps be best expressed by the observation that the world is still an anarchic realm. The state, or any other alternative political unit, is still not hierarchically ordered according to a higher global authority, and while self-regarding states continue to pursue their interests within their own means, differentials in relative power still effectively explain the global truism that "the strong will do what they will, and the weak will suffer what they must." Moreover, in regions of the world such as Northeast Asia, where remnants of Cold War politics continue to influence regional dynamics, the world continues to benefit from the merits of strategic nuclear deterrence in keeping conflicts between North and South Korea and China and Taiwan from degrading into violent confrontations.

The discontinuities from the structural realist worldview, on the other hand, were raised in this study by explaining how the information revolution had altered the nature of various interactions between global (meaning both state and non-state) actors. For one, breakthroughs in information and communications technologies produced a change of

scale: mutually reinforcing technologies such as micro-computing, wireless broadband, mobile phones, and the Internet allowed for informational value to be created and stored in greater quantities, processed and transferred at faster speeds, and disseminated to a wider audience. From a security perspective, one of the most important consequences from these changes was that the world became much more interconnected, and less compartmentalized. Individuals and non-state groups, for instance, have been able to take on a larger, more direct role in political and military affairs by organizing on a global scale (e.g., international campaign to ban land mines), or using offensive computer network capabilities to take political and security matters into their own hands (e.g., "hacktivism").

Conversely, the advent of cyberspace has also allowed the state and the military to play a greater role in the private lives of citizens and within the business community. As the world draws closer to a state of pervasive computing (or "ubiquitous computing") where ICT has permeated into almost every facet of post-industrial society,[44] states and national defense agencies are faced with the challenge of maintaining a balance between respecting civil liberties and privacy, maintaining the efficacy of government and business, and protecting the homeland from cyber-based threats and attacks. As one computer security analyst, Dan Geer, summarized:

> Those with either an engineering or management background are aware that one cannot optimize everything at once — that requirements are balanced by constraints. I am not aware of another domain where this is as true as it is in cybersecurity and the question of a policy response to cyber insecurity at the national level. In engineering, this is said as "Fast, Cheap, Reliable: Choose Two". In the public policy arena, we must first

[44] A good explanation of the concept of pervasive computing is M. Mitchell Waldrop, "Pervasive Computing: An Overview of the Concept and Exploration of the Public Policy Implications," *Woodrow Wilson International Center for Scholars Foresight and Governance Project* (March, 2003).

> remember the definition of a free country: a place where that which is not forbidden is permitted. As we consider the pursuit of cybersecurity, we will return to that idea time and time again; I believe that we are now faced with "Freedom, Security, Convenience: Choose Two."[45]

Another salient consequence of the information revolution has been the evolution of international conflict and warfare. During the Cold War, although strategic nuclear weapons turned the theater of operations from regional to global, the technological frontiers of the time limited the domains of warfare to land, air, sea, space, and RF. In the post-Cold War period, the creation of cyberspace as the sixth recognized domain of warfare has expanded the scope of war to include a virtual domain, which has led to several changes in the reasons and the wherewithal behind international security competition.

In this essay, I suggested that power in the post-Cold War period has become less about possessing brute military strength and more about sustaining economic wealth. In agreeing with views held by Joseph Nye and others that "factors such as technology, education, and economic growth are becoming more important, whereas geography, population, and raw materials are becoming less important,"[46] I go on to argue that wars between developed countries today are more about achieving gains in relative socio-economic power, and that warfare in the traditional, state-military-centric trinitarian sense has been supplemented by an emerging form of warfare that is conducted by various state and non-state actors in a non-violent way to achieve socio-economic, and political ends.

---

[45] Daniel E. Geer, "Cybersecurity and National Policy," *Harvard National Security Journal* 2:1 (April 7, 2010), http://www.harvardnsj.com/2010/04/cybersecurity-and-national-policy/.

[46] Nye (1990), "The Changing Nature of World Power," 179.

Second, upon establishing the view that the information revolution is a source of "supplemental" change of the international system and not "transformational,"[47] I argued that the securitization of cyberspace favors offensive usage over defensive usage, and that the virtual medium can potentially act as a destabilizing force within the international system. This conclusion was arrived at after assessing cyberspace according to structural realist arguments grounded in the security dilemma, and also the distribution of power.

From the security dilemma perspective, I concluded that the securitization of cyberspace would result in an increase in the severity of the security dilemma, and that states would be encouraged to engage in arms races within the virtual domain. Unlike nuclear weapons that greatly mitigated the deleterious effects of the security dilemma by favoring the defense through nuclear deterrence, cyberspace has the opposite effect on the security dilemma by favoring the offensive and providing it with asymmetric advantages such as cost, anonymity, and deniability. Actors that choose to acquire offensive computer network capabilities require relatively little fixed costs, can don the cloak of anonymity by operating out of various remote servers located in neutral countries, and plausibly deny any wrongdoing by leaving very little trace evidence. Defensive forces, on the other hand, require watertight security measures that constantly monitor key systems and networks, differentiate between probes, suspicious activities, and actual attacks, and adapt to the constantly changing nature of the threats.

[47] I note that the difference between the two types of change is that transformative changes require the variable to either turn the world political order into a hierarchical system, or order it according to a different unit. Supplemental changes are those that either amplify or diminish an inherent characteristic of the international system. See Kenneth Waltz, "Reflections on *Theory of International Politics:* A Response to my Critics," in *Realism and International Politics* Kenneth Waltz (New York, NY: Routledge, 2008).

In addition to favoring the offensive, cyberspace also increases the level of uncertainty that weighs against states making strategic decisions about their cybersecurity policy. Because many of the agents involved in conducting CNO cannot be distinguished between their offensive and defensive uses, and there is a "bifurcation of responsibility and control" over the signaling of intentions to other states within cyberspace, states must make their decision to either pursue competitive or cooperative policies enshrouded in uncertainty. For example, states that observe another state recruiting highly skilled programmers or former-hackers into government or military service will have a difficult time discerning whether they are being recruited for the purposes of conducting "white hat" or "black hat" activities. Or alternatively, if an ultra-nationalistic hacker steals terabytes of classified information from another country's national defense networks and claims to be working for the state, then how does the victim state assess whether the intrusions are a signal of the hacktivist's home country's malicious intent, or simply of the individual's? Taken together, the material and informational variables that indicate the severity of the security dilemma explain why states will be tempted to pursue competitive arming policies in the information age.

Assessing cyberspace using structural realist arguments that deduce expectations of stability based on the distribution of power also led to the conclusion that cyberspace will potentially be a destabilizing force within the international system. According to arguments made by Waltz and Mearsheimer, a world with two dominant powers is more stable than a world with several great powers because less is easier to manage than more. In bipolarity, power is more likely to be evenly distributed between the two superpowers, and more concentrated at the top. As the argument goes, the security of the two dominant

states is less contingent upon the actions or realignment of minor powers, the behavior of the pair is more likely to be risk averse and conservative, and the opportunities for great power war to arise either intentionally or unintentionally are less.

Today, although I caveat that the assertions by Waltz and Mearsheimer remain true in the traditional, trinitarian sense of warfare, I argue that cyberspace has made it possible for various actors to threaten the stability of the international system irrespective of the given polarity of the system. By providing the capabilities to state and non-state actors to target the economic and military power bases of highly networked states, cyberspace has made it possible for non-violent warfare to produce decisive shifts in relative power. In the post-Cold War era, while on one hand states can remain deterred by the threat of nuclear annihilation, on the other, states can also attempt to increase their share of relative power by stealing the intellectual property of rival state companies, directly disrupting the commercial activities of the rival states, and probing their government and military networks for vulnerabilities that could be used as leverage in a time of actual crisis.

Looking forward, as China steadily closes the economic and military gap between it and the United States, and as many suggest, the world is nearing the beginning of a bipolar U.S.-China system, the key policy concern for academics and policy makers alike has been whether the transition is going to be peaceful. While this study is unable to make sweeping predictions made by structural realists such as Waltz, Mearsheimer, and Glaser, the idea that the information revolution has produced significant changes within the international system leads to some cautionary points.

First, contrary to the optimistic views of Waltz and Glaser, who believe that the defense advantage created by nuclear deterrence allows for the United States to remain unthreatened by the rise of China, the argument that cyberspace favors the offensive and allows for shifts in relative power to be achieved without violent military confrontation cautions the possibility of conflicts to escalate within cyberspace, and for pressures to rise within the United States to take preemptive action to slow the economic and military growth of China. The tense interactions within cyberspace between China and the United States are already surfacing with allegations on both sides of malicious activity, and as the gap in relative power between the two states become narrower in the near future, the conflict being waged by both Chinese and American state and non-state "cyber-warriors" could increase in severity and lead to dire consequences between the two sides.

Second, in addition to the dangers of state-on-state conflict between the Chinese and the Americans within cyberspace, another source of danger is the possibility of unintentional and accidental cyber-attacks that could set in motion catastrophic events. As Niall Ferguson explained in his recent article in *Foreign Affairs*, all empires are complex adaptive systems, and not all empires "cycle sedately from Arcadia to Apogee to Armageddon."[48] Although the subject of Ferguson's piece was the fragility of the U.S. economy, the underlying lesson that transitions in the world are not all gradual and linear remains quite appropriate to the dangers of the information revolution. As the interconnectedness between all sectors of the modern, informationized society increases with the spread of pervasive computing capabilities, the naïve actions of a young, highly

[48] Niall Ferguson, "Complexity and Collapse," *Foreign Affairs* 89:2 (March/April, 2010): 18-32, 31.

talented Chinese or American hacktivist could lead to a destructive positive feed-back loop that could result in disastrous economic, political, and even military consequences.

As the United States and China continue to move forward through uncharted waters, and as the information revolution surges on, the current global superpower and the aspiring regional superpower will need to consider many of these obvious and less obvious dangers that could lie ahead. Difficult and multifaceted issues such as drafting a set of terms regarding the offensive usage of cyberspace similar to the Geneva Protocol or the Hague Conventions will need to be considered. And more technical challenges such as compensating for the bifurcation of state responsibility and control will need to be addressed. The result of many of these complex issues will eventually determine whether cyberspace becomes the next global commons for free and universal use, or the next existential threat that keeps the world on the precipice of chaos and collapse.

Bibliography

Abrams, Randy. “The Biggest Botnet in the World.” *ESET Threat Blog* (March 4, 2010) http://blog.eset.com/2010/03/04/the-biggest-botnet-in-the-world.

Adams, John. “Virtual Defense.” *Foreign Affairs* (May/June, 2001).

———"Information Warfare: Challenge and Opportunity." *USIA Foreign Policy Agenda* (November 1998).

Albanesius, Chloe and Erik Rhey. “Inside the Biggest Online Theft Case.” *PC Magazine* 29:5 (May, 2010).

Alexander, Keith B. “Advanced Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command: Section 7.” *United States Senate Armed Services Committee Hearing* (April 15, 2010).

Baker, Stewart, Shaun Waterman, and George Ivanov. *Into the Crossfire: Critical Infrastructure in the Age of Cyber War*. London: McAfee, 2010.

Barnett, Thomas and Brad Hayes. “System Perturbation: Conflict in the Age of Globalization.” In *War and Virtual War: The Challenges to Communities*, edited by Jones Irwin. New York, NY: Rodopi, 2004.

Bayles, William J. “The Ethics of Computer Networked Attack.” *Parameters: U.S. Army War College* 31:1 (Spring, 2001): 44-61.

Becker, Elizabeth. “Pengaton Sets Up New Center for Waging Cyberwarfare.” *The New York Times* (October 8, 1999).

Betz, David. “The Malevolence of Crowds.” *Kings of War* http://kingsofwar.org.uk/2010/10/the-malevolence-of-crowds/.

Brunst, Philip B. “Use of the Internet by Terrorists: A Threat Analysis.” In *Responses to Cyber Terrorism*, edited by Centre of Excellence Defence Against Terrorism, 34-60. Amsterdam, Netherlands: IOS Press, 2007.

Castells, Manuel. *The Rise of the Network Society: The Information Age: Economy, Society and Culture (Volume 1)*. Malden, Massachusetts: Blackwell Publishers, 2000.

Carr, Jeff et al. “Project Grey Goose: Phase 1 Report.” *Project Grey Goose* (October 17, 2008).

———“Project Grey Goose Phase 2 Report: The Evolving State of Cyber Warfare.” *GreyLogic* (March 20, 2009).

Cashell, Brian, William D. Jackson, Mark Jickling, and Baird Webel. “Economic Impact of Cyber-Attacks.” *Congressional Research Service (CRS) Report for Congress* (April 1, 2004).

Cox, Chris. “Anonymous 4GW (Fourth Generation Warfare).” *Campaign Reboot.* (October 5, 2010) http://recampaign.blogspot.com/2010/10/anonymous-4gw.html.

Davis, Joshua. “Hackers Take Down the Most Wired Country in Europe.” *Wired Magazine* 15.09 (Aug., 21, 2007).

Edelstein, David M. “Managing Uncertainty: Beliefs about Intentions and the Rise of Great Powers.” *Security Studies* 12:1 (Autumn, 2002): 1-40.

Elster, Jon. *Rational Choice* (Oxford, London: Basil Blackwell, 1986).

Enders, John. “California Computer Whiz is First Alleged Hacker Charges with Espionage.” *The Associate Press* (December 10, 1992).

Ferguson, Niall. "Complexity and Collapse." *Foreign Affairs* 89:2 (March/April, 2010): 18-32.

Friedman, Thomas. *Longitudes and Latitudes: Exploring the World After September 11*. New York, NY: Anchor Books, 2003.

———"Prologue: The Super Story" *Longitudes and Attitudes: Exploring the World after 9/11*. New York, NY: Farrar, Straus, and Giroux, 2002.

Geer, Daniel E. "Cybersecurity and National Policy." *Harvard National Security Journal* 2:1 (April 7, 2010), http://www.harvardnsj.com/2010/04/cybersecurity-and-national-policy/.

Gilpin, Robert. *War and Change in World Politics*. New York, N.Y.: Cambridge University Press, 1981.

Glaser, Charles. *Rational Theory of International Politics*. Princeton, NJ: Princeton University Press, 2010.

Glaser, Charles and Chaim Kaufmann. "What is the Offense-Defense Balance and can We Measure It?" *International Security* 22:4 (Spring, 1998): 44-82.

Global Security. "Solar Sunrise" *Global Security* (2008), http://www.globalsecurity.org/military/ops/solar-sunrise.htm.

———"Eligible Receiver" *Global Security* (2008), http://www.globalsecurity.org/military/ops/eligible-receiver.htm.

Hathaway, Melissa E. "Cyber Security: An Economic and National Security Crisis." *The Intelligencer: Journal of U.S. Intelligence Studies*, 16:2 (Fall 2008).

Honeynet Project. "Know Your Enemy: GenII Honeynets." (May 12, 2005), http://old.honeynet.org/papers/gen2/.

Hvistendal, Mara. "The China Syndrome." *Popular Science* 274:5 (May, 2009): 60-65.

Internet World Stats: Usage and Population Statistics. "World Internet Users and Statistics." *Internet World Stats* (June 30, 2010), http://www.internetworldstats.com/stats.htm.

Jervis, Robert. "Cooperation Under the Security Dilemma." *World Politics* 30:2 (January, 1978): 167-214.

Kabay, M.E. "Hiring Hackers (Parts 1 & 2): Verify, then Trust, then Verify." *Network World* (August 17, 2009).

Kreisler, Harry and Kenneth Waltz. "Theory and International Politics: A Conversation with Kenneth Waltz." *Conversation with History Series* (University of California, Berkley: Institute of International Studies, February 10, 2003), http://globetrotter.berkeley.edu/people3/Waltz/waltz-con0.html.

Krekel, Bryan et al. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Networked Exploitation*. McLean: Northrop Grumman, October, 2009.

Leiner, Barry M. et al. "A Brief History of the Internet V.3.32." *The Internet Society* (December 10, 2003), http://www.isoc.org/internet/history/brief.shtml.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Project AIR FORCE Monograph, 2009.

Longstaff, Thomas A. et al., "Security of the Internet." In *The Froehlich/Kent Encyclopedia of Telecommunications vol. 15*, edited by Fritz E. Froehlich and Allen Kent. New York, NY: Marcel Dekker, 1997.

Lewis, James A. et al. *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, D.C.: Center for Strategic and International Studies, December, 2008.

Lynn, William J. III. "Remarks at Stratcom Cyber Symposium." *Stratcom Cyber Symposium* (Omaha, NE, May 26, 2010). Transcript available online at, http://www.defense.gov/speeches/speech.aspx?speechid=1477.

———"Defending a New Domain." *Foreign Affairs* 89:5 (September/October, 2010): 97-102.

Markoff, John. "Cyberwarfare Breaks the Rules of Military Engagement." *The New York Times* (October 17, 1999).

Markoff, John, David E. Sanger, and Thom Shanker. "In Digital Combat, U.S. Finds No Easy Deterrent." *The New York Times* (January 26, 2010).

Mazzafro, Joseph, ed. *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models*. Arlington, VA: Intelligence and National Security Alliance, November, 2009.

Mearsheimer, John. *Tragedy of Great Power Politics*. New York, N.Y.: W.W. Norton & Company, 2001.

Mills, Elinor. "Conficker Infected Critical Hospital Systems, Experts Say." *CNET News: Security* (April 23, 2009), http://news.cnet.com/8301-1009_3-10226448-83.html.

Muñiz, Jorge Jr. *Declawing the Dragon: Why the U.S. must Counter Chinese Cyber-Warriors*. Fort Leavenworth: U.S. Army Command and General Staff College, 2009.

National Security Directive No. 42 (July 5, 1990).

Nye, Joseph S., Jr. "The Changing Nature of World Power." *Political Science Quarterly* 105:2 (Summer, 1990): 177-192.

Pilieci, Vito. "For Security, Hire Hackers: Insistence on Certificates Overlooks Real Experience, Consultant Says." *National Post* (November 11, 2009).

Ruggie, John G. "Continuity and Transformation in the World Polity: Toward a Neorealist Synthesis." *World Politics* 35:2 (Jan., 1983).

Schneier, Bruce. "It Will Soon be too Late to Stop the Cyberwars." *Financial Times* (December 2, 2010).

Strassler, Robert B., ed. *The Landmark Thucydides*. New York, N.Y: Simon and Schuster Inc., 1996.

Sverdlove, Harry. "Stuxnet Worms Shows Critical Infrastructure Attacks No Longer Just Hollywood Hype." *SC Magazine* (October 18, 2010), http://www.scmagazineus.com/stuxnet-worm-shows-critical-infrastructure-attacks-no-longer-just-hollywood-hype/article/181212/.

Symantec Corporation. "Outbreak Alert "Storm Trojan." *Threat Advisory Center* *http://www.symantec.com/outbreak/storm_trojan.html*.

Tenet, George. "The Worldwide Threat 2001: National Security in a Changing World." *Testimony before the Senate Select Committee on Intelligence* (February 7, 2001).

"The Hacker Who Turned Himself In." *The Guardian* (Factiva), March 26, 1998.

The Tor Project. *About: Tor*. (September 15, 2010), https://www.torproject.org/index.html.en.

Thomas, Timothy. *Decoding the Virtual Dragon*. Fort Leavenworth, KS: Foreign Military Studies Office, 2007.

Tkacik, John J. Jr. "Trojan Dragon: China's Cyber Threat." *The Heritage Foundation Backgrounder* (February 8, 2008), http://www.heritage.org/research/AsiaandthePacific/bg2106.cfm.

United States Joint Chiefs of Staff (JCS). *Joint Publication 3-13: Information Operations* (February 13, 2006).

United States Strategic Command. *United States Cyber Command: Fact Sheet*. (October, 2010) http://www.stratcom.mil/factsheets/cc/.

Van Creveld, Martin. *The Transformation of War*. New York, N.Y.: The Free Press, 1991.

Vatis, Michael A. "Trends in Cyber Vulnerabilities, Threats, and Countermeasures." In *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies*, edited by Jacquis S. Gansier. Washington, D.C.: National Defense University Press, 2004.

———"Cyber Attacks: Protecting America's Security against Digital Threats." *Executive Session on Domestic Preparedness (ESDP) Discussion Paper*. Cambridge, Massachusetts: John F. Kennedy School of Government, Harvard University, June 2002.

Veit, Stan. *PC-History*. http://www.pc-history.org/

Waldrop, M. Mitchell. "Pervasive Computing: An Overview of the Concept and Exploration of the Public Policy Implications." *Woodrow Wilson International Center for Scholars Foresight and Governance Project* (March, 2003).

Walt, Stephen M. "Is the Cyber Threat Overblown?" *Foreign Policy Online* (March 30, 2010) http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown.

Walters, Conrad. "Cyber Cold War a Threat to All." *The Sydney Morning Herald* (December 24, 2007).

Waltz, Kenneth. *Theory of International Politics*. Long Grove, IL: Waveland Press, 1979.

———"Globalization and Governance." *PS: Political Science and Politics* 32:4 (Dec., 1999).

———"Structural Realism after the Cold War." *International Security* 25:1 (Summer, 2000): 5-41.

———*Chapter 31: The Continuity of International Politics.* In *Worlds in Collision: Terror and the Future of Global Order*, edited by Ken Booth and Tim Dunne, 348-354, New York, N.Y.: Palgrave Macmillan, 2002.

———*Reflections on Theory of International Politics: A Response to my Critics*. In *Realism and International Politics*, edited by Kenneth Waltz. New York, NY: Routledge, 2008.

Weik, Martin H. "The ENIAC Story." *ORDNANCE* (January/February, 1961), http://ftp.arl.army.mil/~mike/comphist/eniac-story.html.

"White Collar Hackers—A Matter of National Insecurity." *The Guardian* (March 26, 1998).

"Who Caused the Crash?" *BBC* (April 5, 2001).

Wilson, Clay. "Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress." *Congressional Research Service (CRS) Report for Congress* (November 15, 2007).

Woods, Ashlee. *Terrorists and the Internet*. In *Understanding Terrorism: Analysis of Sociological and Psychological Aspects*, edited by Suleyman Ozeren et al., 270-280, Amsterdam, Netherlands: IOS Press, 2007.

Yoran, Amit. “Cyberwar or Not Cyberwar? And Why that is the Question.” *Forbes: The Firewall* (May 25, 2010), http://blogs.forbes.com/firewall/2010/03/25/cyberwar-or-not-cyberwar-and-why-that-is-the-question/.

Zetter, Kim. “Computer Malware the New ‘Weapon of Mass Destruction’.” *Wired: Threat Level* (December 10, 2008).

———“’The Analyzer’ Hack Probe Widens; $10 Million Allegedly Stolen from U.S. Banks.” *Wired: Threat Level* (March 24, 2009).