UNIVERSITY OF CALIFORNIA

Los Angeles

The Spatiality of Power in Internet Control and Cyberwar

A dissertation submitted in partial satisfaction of the
requirements for the degree Doctor of Philosophy
in Geography

by

Cameran Hooshang Ashraf

2015

ABSTRACT OF THE DISSERTATION

The Spatiality of Power in Internet Control and Cyberwar

by

Cameran Hooshang Ashraf

Doctor of Philosophy in Geography

University of California, Los Angeles, 2015

Professor John A. Agnew, Co-Chair

Professor Michael Edward Shin, Co-Chair

Recent debates on Internet censorship and the role of the state in online communications highlight concerns about sovereignty, borders, and territory in a globalizing world. Conventional geopolitical thought views the world as divided into discrete spatial units, with each state free to act within its territory. The space in which the state can act is its territory, demarcated by its borders, and its freedom to act within those boundaries is its sovereignty. Territory, borders, and sovereignty are the geographical assumptions which underpin the international state system.

States viewed the Internet as an extension of existing territory, and sought to extend that territory in the new informational space by developing laws and technical systems to territorialize cyberspace. In effect, the international state system became duplicated in cyberspace, such that the Internet experienced from within one state could radically differ from the Internet experienced from another. However, the image of stability provided by replicating existing geopolitical logics becomes illusory during times of cyberwar. States no longer regard the informational boundaries and territories they created in cyberspace as meaningful, and instead seek to gather as much cyberpower as possible without regard for the very geographic logic which cyberwar attempts to maintain.

This dissertation exposes the cyber-geographical gap between state territorialization of cyberspace and state practice during times of cyberwar. It does so by demonstrating how states territorialize the Internet and, through case studies, how cyberwar is conducted without regards for conventional geographies. This research is significant because 1) it represents the first critical geopolitical engagement with Internet filtering and cyberwar in academic geography; 2) it provides a theoretical background for the problem of attribution in cyberwar; 3) it reveals a theoretical geographical instability at the nexus of traditional sovereignty and alternative spatialities of power. It is this last element of geographical instability which this dissertation ultimately argues may represent a new geography for states in cyberspace.

The dissertation of Cameran Hooshang Ashraf is approved.

Eric Sheppard

Nazli Choucri

Michael Edward Shin, Committee Co-Chair

John A. Agnew, Committee Co-Chair

University of California, Los Angeles

2015

Dedicated to my mother. Thank you for helping me with my homework one last time.

I miss you.

TABLE OF CONTENTS

FIGURES AND TABLES

ACKNOWLEDGEMENTS

This has been a long and difficult journey, and one which could not have been completed without the support of many kind individuals. I would like to thank as many of them as I can.

Thank you to John Agnew, who provided much wisdom and guidance throughout my time here at UCLA, believed in me both before and after being accepted to the program, and for a heartfelt conversation after my mother's passing. Michael Shin, thank you for working with me through some difficult times – I know it wasn't easy for you, and I am very grateful for your patience and guidance. I thank Michael Curry for stimulating reading lists, opening my mind to orality and literacy, and for his helpful technique for getting through writer's block. Thank you to Stephen Bell for encouraging words which made a difference early in my time at UCLA. Eric Sheppard, for asking the right questions during my dissertation proposal defense. I thank Nazli Choucri for her support of my dissertation and guidance with my proposal.

Within the Department of Geography I would like to thank Kasi for her support, many conversations, and support through the good times and the bad times, I truly appreciate it. I also thank Vanessa, Rebecca, and Tanja for making my visits to the office something I enjoyed and looked forward to, and for always having time to say hello and talk with a graduate student.

There are many graduate students who made a profound difference in my life. Luis, for many thoughtful conversations, support, and encouragement, and for being such an excellent human being and inspiration. Diane, whose kindness began before I was a student and continued throughout the journey, with thoughtfulness, grace, and empathy. Katie for a summer of crappy hours and laughter which made a difference. Nick, for so many laughs and fantastic projects. Scott, for his empathy, care, and positivity. Ago, for wise insights and a lunch which made an

impact. Heather, whose hilarious texts and attitude made much of grad life more bearable. Setareh, for her kindness and encouragement near the end. Tom, for his positivity and graduate student wisdom. Ford, for many talks and walks which inspired me with confidence.

Outside of grad school, I send profound thanks to Jason for his many years of friendship and for absolutely always being there for a phone call no matter what the cause or time. I will never forget it. Rob for picking things up and putting them down. Ivonne, for our conversations and hikes where I again learned everything that is yes. I thank Mehdi for being a friend I can count on at any time. Ali, for your presence, support, and straight-talking. Ilona Grzywinska for showing me another way of living is possible.

Facing my lifelong fear of swimming and water helped me immeasurably in life and academics, and so I thank my swimmies. Henly, for getting my face in the water and being an excellent friend and swim instructor. Amy, for constant encouragement, positivity, warmth, wisdom, a kind ear, and support. Jenny, for patience and showing me courage. Gerald, for depth of insight, patience, and compassion. And Brian for just moving here but for readily toasting me when I completed writing - something deeply needed!

Other thanks include the great thinkers Rousseau, Wittgenstein, Joseph Campbell, Rumi, Hafez, Pema Chodron for their guidance. I sincerely thank Dr. Ali Moinzadeh for tremendous, life-changing insight, support, wisdom and for teaching me how to have faith in myself – I could not have done it without you.

I honor the memory of my grandmother and grandfather. Lastly, and certainly not least, I send my deep thanks and love from my heart to my father who stood by me and taught me many true lessons. Finally: I did it, Mo. Thank you for everything, and for this gift of life.

CURRICULUM VITAE

EDUCATION

C.Phil., Geography	University of California, Los Angeles. 2013
Certificate in Digital Methods	University of Amsterdam. 2011
M.A., Geography	California State University, Fullerton. 2009
B.S., Geography (Cum Laude)	California State Polytechnic University, Pomona. 2005
B.S., Business (Cum Laude)	California State Polytechnic University, Pomona. 2005

ACADEMIC EMPLOYMENT

Teaching Fellow	University of California, Los Angeles. 2013 - 2015
Teaching Associate	University of California, Los Angeles. 2011 - 2013
Lecturer	California State University, Pomona. 2009 - 2010
Research Assistant	California State University, Fullerton. 2007 - 2008

NON-ACADEMIC EMPLOYMENT

Co-Founder & Executive Director 2010-2011
Expression Technologies - *NGO providing technology solutions to human rights activists in closed societies*

- Migrated AccessNow’s secure hosting and communications infrastructure
- Extended security services to include clients in South America and Southeast Asia
- Secured $2.1 million U.S. Department of State Internet Freedom grant as sub-grantee

Co-Founder, President, & International Projects Director 2009-2010
AccessNow - *International NGO focused on technology and human rights*

- Provided secure hosting to vital human rights and democracy websites
- Distributed secured communications tools to human rights defenders in closed societies
- Facilitated more than 3 million video downloads from inside Iran
- Developed international and corporate governance policy recommendations to keep the Internet free and open while facilitating the secure flow of information in closed societies
- Finalist, Sakharov Prize for Freedom of Thought – selected as finalist by the European Parliament for the 2010 Sakharov Prize for Freedom of Thought, Europe’s highest human rights honor

PRESENTATIONS

Invited Presentations

“International Cybersecurity and the Legal-Territorial Paradox” York Symposium, Lawrence Livermore National Laboratory, November 2013.

“Technology and the Places of Everyday Life” University of California, San Diego, March 2013.

“The Internet and Human Rights” in the undergraduate class Human Geography. Instructor Aline Gregorio, California State University, Fullerton, March 2011.

"New Communications Technologies and Iran's Green Movement" in the undergraduate class Place, Identity, and the Networked World. Professor Michael Curry, Department of Geography, University of California, Los Angeles, November 2010.

"Strong Ties, Weak Ties, and Iran's Green Movement: A Response to Gladwell" in the graduate seminar The Cultural, Ontological, and Digital – Global Perspectives. Professor Ramesh Srinivasan, Department of Information Studies, University of California, Los Angeles, October 2010.

"Civics in Difficult Places." MIT Communications Forum at the Massachusetts Institute of Technology, May 2010.

"#iranelection: The Digital Media Response to the 2009 Iranian Election." Berkman Center for Internet & Society at Harvard University, November 2009.

AWARDS AND HONORS

University of California Institute on Global Conflict and Cooperation, Herbert F. York Global Security Dissertation Fellowship, 2013-2014.

University of Oxford, Selected Participant to Summer Doctoral Programme at Oxford Internet Institute, 2013

University of Toronto, Full Scholarship, Connaught Summer Institute on Monitoring Internet Openness and Rights, 2013

University of Toronto, Selected Participant to Connaught Summer Institute on Monitoring Internet Openness and Rights, 2013

University of Amsterdam, Selected Participant to Digital Methods Program, 2011

University of Pennsylvania, Digital Methods Initiative Full Scholarship, 2011

UCLA International Institute Fellowship, 2010-2012.

UCLA Regents Stipend, 2010-2011.

Sakharov Prize for Freedom of Thought, European Parliament, finalist as co-founder of AccessNow, 2010.

Third Place, Graduate Paper Competition, California Geographical Society Annual Conference, 2007.

Third Place, Innovative Application of GIS, California State Polytechnic University, Pomona GIS Expo, 2004.

MEDIA COVERAGE

New Internationalist Magazine - "Beyond Burnout" May 2014

SiriusXM Radio – The Agenda: "2013 Iran Election Panel" June 2013

Slate "The Heavy Psychological Toll of a Digital Activist's Work" April 2013

The Global Mail "Iran: Not Tweeting, Hacking" April 2012

PC World Magazine "In Iran, New Attack Escalates Ongoing Cyberconflict" March 2011

National Public Radio "1 Year Later Iran's Opposition Still Relies On Internet" June 2010

TechPresident "Getting Past Digital Censors Becoming 'Part of Youth Culture'" March 2010

New York Times "Supporting Dissent With Technology" February 2010.

Bloomberg Businessweek "Iran 'Cyber Army' Hits Radio in Latest Crackdown" February 2010

PC World Magazine "Clinton Praised for Internet Freedom Speech" January 2010

New York Times "Clinton Urges Global Response to Internet Attacks" January 2010

Chapter 1

Introduction

In mid-2010, someone at Iran's Natanz nuclear enrichment lab quietly inserted a USB drive into a secured computer which controlled Iran's nuclear centrifuges and ushered in the modern era of cyberwar. These computers were supposed to be highly secure, protected by an “air gap”, a term for computers which are completely disconnected from the Internet. Because of this, Iran's security engineers believed they would be safe from espionage or hacking attempts from the outside world. What security practitioners fail to account for is that computers are easy to secure and people are not: the air gap is a fictional border which is only as robust as the humans which develop and maintain it. Somehow, someone messed up and rendered the air gap useless.

In June 2010 computer security researchers from VirusBlokAda discovered a new virus, one which was never supposed to be discovered. Dubbed StuxNet, a combination of words which appeared in the virus' code (Lüders 2011), the virus displayed peculiar features which were unusually specific and highly sophisticated. The virus was designed to “...spy on the industrial systems and even cause the fast-spinning centrifuges to tear themselves apart” (Kushner 2013, p. 50). It was programmed to feed false data to engineers to cover its tracks, ensure that it could only spread to three computers from each host, and delete or disable itself if a specific set of conditions were not met (Falliere et al. 2011). StuxNet focused only on a specific type of Siemens brand supervisory control and data acquisition (SCADA) system. The targeted system controlled Iran's nuclear enrichment program and StuxNet targeted it with a goal to cause the centrifuges to spin out of control and malfunction (Gross 2011, Falliere et al. 2011, Zetter 2011). This could delay Iran's nuclear program by several years while being virtually bloodless and untraceable. It was, in the words of security expert Ralph Langner, “a precision, military-grade cyber missile deployed ... to seek out and destroy one real-world target of high importance” (Clayton 2010).

StuxNet was never intended to go beyond Natanz and a few other key locations. But in the same way that it had crossed the air gap, infected files were also transferred back out to computers connected to the Internet. This allowed StuxNet to be released “into the wild” and alert security researchers to its existence as it spread surreptitiously across the world, infecting over 60,000 computers with approximately 60% of those located in Iran (Falliere et al. 2011, Farwell and Rohozinski 2011). Although the developers had targeted hardware they believed to be only located in Iran, gaps in security allowed for other computers to be infected by StuxNet. Here was an example of the potential for collateral damage, discussed in the White House's own *International Strategy for Cyberspace* as a side-effect of the networked nature of cyberwar when weapons unintentionally spread beyond their intended target.

Security researchers from Symantec, Kaspersky Labs, and F-Secure, discovered taunts, biblical, and historical references in StuxNet's source code which seemed to indicate that Israel and the United States were involved in developing and deploying the virus. At the time security researchers were unsure as to whether or not these clues were intentionally placed to deceive digital forensic investigators and implicate states which may not have been involved. Later admissions from key officials in the Obama administration (Sanger 2012), however, seemed to confirm the development of StuxNet by the United States and its subsequent unauthorized modification by Israel. The estimated cost was put at over USD $10 million (Langner 2010) and believed to have been developed at multiple sites across the world, including a mock setup of Iran's nuclear labs in Israel, designed to accurately simulate the ecosystem in which StuxNet would operate.

The *International Strategy for Cyberspace* highlights a critical point in modern cyberwar: that there is a hidden geopolitics to cyberwar, and a neglect of cyberwar's geography may have unintended and unanticipated consequences for international stability and security. StuxNet, as the first major cyberweapon discovered, serves as an example of this in its international development, anonymous distribution, and unintentional transnational spread. Though digital forensics seemed to uncover clues to its development, there was no explicit admission of responsibility from any state or non-state actor and researchers could not determine whether the clues were intentionally deceptive. Had StuxNet targeted common infrastructure, such as electrical utilities or computer servers used in high speed financial transactions, its stealth and spread alongside its geographical amorphous origins could have resulted in serious consequences for global stability.

This dissertation seeks to demonstrate that a gap exists between the geographies of cyberspace and the geographies of cyberwar. The existence of both of these geographies may be seen as controversial given the widespread belief that the Internet is an open public commons, the geopolitics and geographies of cyberspace already exist and states are aggressively bordering and territorializing cyberspace in line with their geopolitical visions. Far from being ageographical, the Internet is profoundly grounded in geography through international transit agreements, domain name administration, and autonomous systems deployment alongside state efforts at Internet censorship and control. State geopolitical visions emerge in the relationship between the state and information, most succinctly expressed in policies and practices of Internet filtering. The geographies of cyberwar between states, on the other hand, are expressed through alternative spatialities of power and stand at geographical odds with the geopolitics of cyberspace.

Thus, this dissertation will demonstrate the existence of a gap between the cyberspace as practiced by states and the prosecution of cyberwar. The existence of this *cyber-geographical* gap is significant because 1) it represents the first critical geopolitical engagement with Internet filtering and cyberwar in academic geography; 2) it provides a theoretical background for the problem of attribution in cyberwar; 3) it reveals a theoretical geographical instability at the nexus of traditional sovereignty and alternative spatialities of power.

It does so through answering two specific research questions: **1) Does geopolitics manifest in cyberspace? If so, how?; 2) What are the geographies of cyberwar?** These two questions demonstrate the existence of the *cyber-geographical gap* between cyberspace and cyberwar. The cyber-geographical gap is the space where efforts to geographically define and articulate cyberwar and cyberspace encounter each other, and where notions of territory, borders, and sovereignty find and lose meaning and relevance.

Introduction Structure

This introductory chapter will provide a brief overview of cyberwar and of territorialized cyberspace. It will then discuss the nature of the cyber-geographical gap before outlining and articulating the research questions which the dissertation seeks to answer. Finally, the organizational structure of the dissertation is outlined and discussed.

Understanding Cyberwar

In this dissertation, cyberwar is assumed to be between states, despite the presence of non-state and other actors and other forms of conflict and violence in cyberspace (Stone 2013). Therefore, cyberwar is actions undertaken by states to alter information, disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. Historically, the origins of modern cyberwar lay in concerns about the physical security of information systems in the 1960s, (Warner 2012). These concerns were grounded in a “filing cabinet” mentality of information storage, which saw information as something inherently physically grounded, and extended the idea of filing cabinets to computers. As technological development progressed and state reliance on information technologies increased, the sophistication of cyberattacks also increased. Those early concerns about the theft of state secrets evolved into the ability of attacks to disable or slow or disable Internet-dependent communications and the development of cyber superweapons, such as the StuxNet malware.

These actions which constitute cyberwar can include infiltrating computer systems to install malicious software designed to sabotage physical infrastructure. It can also include infecting millions of computers around the world for the purpose of crippling a country’s Internet infrastructure through distributed denial of service attacks. Logic bombs can be planted in critical industrial systems and remain hidden for years, only to cause critical system shutdown through remote activation. Cyberwar's actions are wide and varied, and constitute a new domain in which states are acting in an attempt to gain or project power as well as to leverage its asymmetrical nature.

Cyberwar sees territorial states appropriate an aterritorial technology, the Internet, for their political purposes. To successfully prosecute cyberwar, a state must utilize global resources distributed without regard for political territorial boundaries. For example, the servers used to control StuxNet were based in Denmark and Malaysia (Chen and Abu-Nimeh 2011, Gross 2011) and the massive distributed denial of service (DDoS) attacks against Estonia by Russia in 2007 came from hijacked computers across the world. Iran's attack on the DigiNotar web browser security certificate authority had global implications: all of the world's Internet browsers, such as Internet Explorer, Firefox, and Google Chrome, had to be updated to safeguard them from Iran's attack (Arthur 2011). Defensively, the state of Georgia chose to relocate critical official state digital assets to Google and other companies in the United States, without that state's knowledge (Deibert et al 2012).

Cyberwar largely ignores traditional territorial boundaries. States must seek to address their territorial concerns in cyberspace through technological means which disregard territory. This is a feature of the ways in which the technological protocols which power the Internet were developed and contributes to the uniqueness of cyberspace as a domain for war. Thus, states approach cyberwar from a position which eschews conventional notions of territory both on attack and defense. However, in cyberspace states also seek to articulate clearly bounded territory through Internet censorship and control, discussed in the following section.

Territorialized Cyberspace

Early cyber-utopians such as John Perry Barlow, co-founder of the Electronic Frontier Foundation, envisioned cyberspace as a radical space where borders and states no longer mattered: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather" (Barlow 1996). In cyberspace one could be something radically different and no longer be constrained by any of the perceived drawbacks of the physical world, such as physical appearance or geography.

This utopian vision was echoed by the early founders of the Internet, many of whom believed they were developing a radically new alternative to the existing system of international communications enabled by technical protocols which supported their utopian vision. Internet pioneers such as Jon Postel (Goldsmith and Wu 2008) sought to protect the Internet against any government intrusion by developing protocols and technical approaches which would ensure that their vision of communicative freedom was enshrined in code. These efforts were bolstered by the early attitude of the U.S. government to take a hands-off approach to Internet development after it had secured the portion of the Internet used for sensitive military communications, known as MILNET (Roberts et al 2011).

However, the growing popularity of the Internet and its increasingly relevance outside of academia and potential security risks quickly grabbed the attention of U.S. government administrators. The government's legal authority was again asserted as it took control of key aspects of the Internet in a bid to centralize control, ostensibly to promote and support its global growth. As the Internet's development and popularity began to stabilize, the U.S. government gradually relinquished its formal oversight of key aspects of the Internet though it continues to retain disproportionate powers.

As the Internet has matured states have moved to assert conventional notions of territoriality in cyberspace. States approach the Internet from a realist perspective (Manjikian 2010) whereby the Internet is simply an extension of the state's existing territory in the same way as airspace or territorial waters. As Manjikian (2010) argues, states view the Internet as something to be controlled and monitored rather than a space where the free flow of ideas or information can take place. States have utilized two approaches in modifying cyberspace to fit geographical norms: activity and technical regulation, which Goldsmith and Wu (2008) argues underpins the existence of sovereignty in cyberspace.

Activity regulations are the laws, norms, and international legal agreements which underpin much of the conventional territorial state. Applying “offline” laws in cyberspace at first proved problematic as the cyber-utopian rhetoric seemed to confirm. However, since the year 2000 states have moved to regulate ecommerce, monitor child pornography, and prosecute cybercriminals. With some modifications territorial states were able to adapt their laws to the Internet bringing online activity firmly into the domain of the state. Partnerships with Internet service providers (ISPs) allowed law enforcement to trace activity to individual computers and sophisticated national surveillance systems allow states to gather and share intelligence. Emergent transnational agreements on cybercrime (Clough 2012, Jakobi 2013) demonstrate the potential for states to cooperate in cyberspace while respecting the territory and sovereignty of other states. Within the scope of exercising traditional territorial sovereignty, then, activity regulation brings territorially-bound law into cyberspace.

Geographical concepts such as borders, territory, and sovereignty have technical analogues which supported and extended their conceptual development and maturation throughout human history. The Treaty of Westphalia's principle of mutual recognition, for instance, was dependent upon surveying technologies which could accurately demarcate and communicate borders. Technology plays a critical role for states in demarcating their limits and extents as well as communicating and defending those extents. States therefore must not only regulate activities within their geographies through activity regulation but demarcate their geography through technical regulation. The Internet is a tremendously territorial medium grounded in space with easily identifiable packets, standardized national domain registrars, transnational data transit agreements and configuration, and national or sub-national networks (autonomous systems) whose deployment is the foundation of the Internet and the purview of states (Roberts et al. 2011). Further, states can use technology offensively to enforce their real or perceived boundaries through cyberattacks which can further be geographically spoofed in order to present plausible deniability.

Cyberspace is increasingly territorialized by states through activity and technical regulations. States see cyberspace as an extension of the existing geographical status quo and have extended their legal domains to encompass it this, while simultaneously beginning to pursue international conventions in cyberspace. Technologically, states retain a tremendous amount of power over that portion of cyberspace which exists within their geographical boundaries. They can further extend this power through launching cost-effective cyberattacks which can be geographically obfuscated. The existence of a geography of cyberspace alongside state territorializing behavior becomes problematic when it results in a “cyber-geographical gap”, which is the subject of the next section.

The Cyber-geographical Gap

Cyberwar, the geographical foundations of the Internet, and state behavior in cyberspace are examples of how geopolitics are manifested in cyberspace. Regardless of early cyber-utopian rhetoric, sovereignty, borders, and territory are not obsolete ideas but rather deeply embedded within the modern Internet. Despite representing a conceptual and empirical frontier, academic geographic research has largely ignored the geopolitics of cyberspace and has wholly ignored cyberwar. The geographies of cyberspace and cyberwar have been taken up by political science, international relations, and security studies whose engagement with critical geographical literature is lacking.

The gap between the Internet's inherent geography, cyberwar, state territorializing behavior in cyberspace on one hand and the security responsibilities of geography on the other hand constitutes a “geographical gap” in modern cyberspace discourse and practice. This gap contributes to instability by essentially leaving cyberspace as a “wild west” or “frontier” where different rules apply from the territorial world, many of which are not conducive towards security. The difficulty in holding states accountable for cyberwar or cyberterrorism, for instance, represents a fundamentally geographic question largely ignored as states instead opt for primarily offensive cyberwar solutions. Further, the inherent geography of cyberspace facilitates the development of censorship and surveillance regimes which can freely cross borders and restrict the flow of information, a driver of recent economic growth and prosperity in both the developed and developing worlds (Czernich et al. 2011).

Research Questions

This dissertation's exploration of the cyber-geographical gap is predicated upon two research questions:

1) Does geopolitics manifest in cyberspace? If so, how?

2) What are the geographies of cyberwar?

The importance of these questions to the dissertation's inquiry into the cyber-geographical gap is explained below.

1) Does geopolitics manifest in cyberspace? If so, how?

The popular geopolitical model of cyberspace is very much in line with early cyber-utopian and libertarian models of a geographically unencumbered public space for discourse and information retrieval or sharing. This model is reinforced through political rhetoric in Western states, specifically the United States, and its emphasis on “Internet Freedom” and maintaining an “open Internet” (Morozov 2012). Further, the early logic behind the Internet's ability to allow information to remain geographically resilient during the Cold War (Aksoy and DeNardis 2007) was a technological response to and creation of Cold War ideological geopolitics. That is, the existential threat to the United States threat presented by the Soviet nuclear arsenal necessitated the development of a nuclear-resistant communications protocol.

The “open Internet” ideal articulated by the United States and Western Europe represents a continuation of the ideological geopolitics which gave birth to the Internet. Hegemony and the globalist sovereignty regimes (Agnew 2009) are an inheritance of Cold War geopolitics, of which the Internet is a communicative component. At the same time, Russia, China, and other post-Soviet and authoritarian states continue to ground their vision of geopolitics in anti-Western and anti-imperialist rhetoric and practice by hardening their digital borders through aggressive Internet filtering and control. The geopolitics of cyberspace, then, is grounded in the ideological geopolitics of the Cold War, of the “free world” and a closed world, but in the sense of a filtered and unfiltered cyberspace.

2) What are the geopolitics of cyberwar?

The geopolitics of the Cold War influenced the development of the Internet which itself has greatly influenced post-Cold War geopolitics and geoeconomics. Conflict and survivability, therefore, underpin the historical foundations of the Internet. These conflict and geopolitical models became embedded in the protocols and software code which form the technological foundations of cyberspace. As a domain whose foundations lay in conflict, it is therefore no surprise that the Internet is uniquely suited to being a site of conflict itself.

The first research question demonstrates the existence of a structural geopolitics to cyberspace itself, leveraged by states overtly and covertly in pursuit of political goals. As Clausewitz (Rid 2013) argues, states also resolve differences through war and conflict. The geopolitics of the Internet is therefore present in cyberwar.

However, the Internet itself is designed to ensure the survivability of information and resilience in the face of blockages or other obstructions in information flow. This ability has lent itself to the “end of geography” tropes which have abounded due to the Internet's flexibility, yet also is relevant to how cyberwar is actually prosecuted. Cyberwar can be waged across global cyberspace without regard for national boundaries and attacks can be further masked to appear as if they originate in other states. How cyberwar is waged, therefore, has at its foundation a conception of geopolitics which ignores the realities of geopolitics in the offline world. It is precisely the method through which cyberwar is prosecuted and its offline implications and geographies which contribute to greater structural instability.

Dissertation Structure

This dissertation is written on the model of six chapters, including a traditional introduction and conclusion as well as a glossary of key technical terms. This chapter, the introduction, has provided background information regarding the current state of cyberspace and cyberwar as well as briefly outlining the ways in which these are geographical. It articulated the three research questions as well as brief explanations as to their importance and academic significance. Finally, it outlines the structure of the dissertation by chapter and provides notes on terminology.

Chapter two provides a theoretical background for geopolitics and the geopolitical concepts which inform this dissertation. At first it discusses the different varieties of geopolitics which exist as well as providing a brief conceptual history of the term. Then, the three geographical assumptions which underpin geopolitics (sovereignty, territory, and borders) are introduced. Each of these assumptions is given a section of the chapter where a brief history of the idea is presented and modern, post-Cold War debates factor into understanding how these concepts continue to inform the world. Finally, the chapter will conclude by articulating how geopolitics is conceived of for the purposes of the dissertation.

The third chapter addresses the first research question. It examines Internet control and filtering as a means to articulate how the geopolitics of the Internet is constructed around notions of sovereignty and borders. These geopolitical conceptions are reified through practices associated with whether or not states enact Internet controls, filtering, and censorship. Then, the chapter will examine the geopolitics of Internet control with an examination of data on Internet control and its relationship to existing political institutions and structures. In doing so, the practice of Internet control is married with geopolitical and political ideologies, demonstrating the connection between terrestrial geopolitics and the geopolitics of cyberspace.

Chapter four seeks to define cyberwar, and in doing so provide definitional preparation and clarity for addressing the second research question on the geopolitics of cyberwar. This is accomplished through examining the history of cyberwar from the 1960s and the evolution of cyberwar amongst the major cyberpowers: the U.S., Russia, and China. Then, an argument is put forth to differentiate cyberwar from cyberespionage, cyberterrorism, and cybercrime while including considerations from skeptics on whether or not cyberwar even exists, or whether instability or disruption represent new norms of conflict resolution in cyberspace. Definitions are provided to address the structural definitional ambiguity surrounding both terms in academic discourse and to guide understandings of what cyberwar is for the remainder of the dissertation.

Chapter five builds on chapter four by outlining the methods which constitute cyberwar, and revisiting the spatiality of power. No articulated treaty or definition of cyberwar exists in international politics. The best measure of understanding cyberwar is through its methods and actual prosecution. Thus, in order to understand how the spatiality of power manifests during cyberwar it is necessary to understand exactly how cyberwar is prosecuted, premised on the methods of attack and defense used by states. Together with chapter four, these chapters form the basis for understanding what constitutes cyberwar through definitional and practical clarity, preparing for the case studies in the next chapter.

Chapter six brings the definitional and practical clarity established in chapters four and five to the forefront by presenting three key case studies as well as analyzing these case studies from the perspective of the spatiality of power. This chapter, therefore, demonstrates how the spatiality of power exists during cyberwar between states, and how it operates opposed to conventional state territorial approaches embodied in the geopolitics of Internet control.

Chapter seven is the concluding chapter and seeks to bring together the preceding chapters into a coherent framework exposing the cyber-geographical gap, demonstrating its theoretical significance, and articulating the threat to stability which emerge. A review of the key geopolitical concepts of sovereignty, territory, and borders as well as a review of the geopolitics of the Internet and cyberwar is provided. This is incorporated into a discussion of the cyber-geographical gap: what it is and its existence as an absence of geography in cyberspace practice. The implications of the cyber-geographical gap are presented, in line with the preceding chapter's discussion of how cyberwar is waged. The potential instability discussed is therefore grounded in case studies and the technological logic of cyberspace. Finally, future research opportunities are recommended.

Conclusion

Academic geography has largely ignored both cyberspace and cyberwar. Despite this, both cyberspace and cyberwar have clear geographies and are strongly influenced by geopolitical visions and practice. This dissertation exposes the geographies of both cyberspace and cyberwar, highlighting a gap in practice termed the *cyber-geographical gap*. This gap sits at the intersection of sovereignty regimes and spatialities of power, providing both a source of geographical instability as well as a theoretically rich domain in which geopolitical concepts can be examined and tested. In exposing the cyber-geographical gap, this dissertation contributes to literature in international relations and security studies through its examination of the sources of the attribution problem and its geographical instability. It contributes significantly to academic political geography through developing the first examination of the geopolitics of cyberspace and cyberwar, while also demonstrating the limits of existing geopolitical thought at the intersection of both: the cyber-geographical gap.

Chapter 2

Geopolitics

Geopolitics is a way of seeing and constructing the world through geographical representations and practices. It is a practical method which humans have used to structure their world, and to frame the unfamiliar within the familiar. However, geopolitics does not exist in isolation from its human context nor did its development occur outside historical trends. The idea of geopolitics emerges at a specific time, in a specific place, and influenced by specific political, social, and technical reasons. In other words, a broader sociopolitical context contributed to the emergence of geopolitics. As a way of seeing and framing the world it has persisted and been adapted in response to human change and remains an important way through which international politics is articulated and made.

The notion of geopolitics, a way of framing, seeing, and constructing politics through geographical representations, was grounded in the terrestrial earth but has been extended to other spaces where humans act. There is a geopolitics to the ocean, to subterranean assets, to airspace, to outer space satellites, and to the moon (Agnew 2003; Brown 1990; Dolman 2002; Elden 2013; Oxman 2006; Romancov 2003; Sage 2008). In domains where human activities occur, geopolitical visions are extended, expanded, and articulated to bring that domain in line with the world at large and to make the strange as familiar (Agnew, 2009b). Insofar as information space has become a dominant and existent sphere in which a range of human actions occur, it stands to reason that a geopolitics of informational space, cyberspace, is itself geopolitical.

However, before the geopolitics of cyberspace can be considered or developed, geopolitics needs to be understood in terms of its history, evolution, manifestation, and present situation. This chapter will briefly discuss the history of geopolitics since 1815, its present configuration, and its different manifestations. Further, this chapter will explore key geographical concepts which underpin geopolitics: borders, territory, and sovereignty.

History of geopolitics

The term geopolitics was first used by the Swedish political scientist Rudolf Kjellén in 1899, during a time of intense global colonial rivalry amongst European nation-states. Originally the term was intended to demonstrate how the relative geographical positions of states influenced the ways in which they could engage in global politics (Agnew, 2003). For example, an island state would have a different world political profile than a landlocked mountainous one.

The emergence of the term “geopolitics” does not mean that a new way of seeing and behaving in the world suddenly emerged at the turn of the 19th century. Instead, the term encapsulated a way of seeing the world which had existed for nearly a century. The international political scene at the time, however, facilitated the creation of a more formal term to encapsulate a view of the world itself as a political entity in which states, as political entities of a different scale, acted. The geopolitical vision was an outgrowth of Renaissance-era reductive views of the world (Agnew, 2003, 2009a) through which the map was made to substitute for the place. The uniqueness of locales and their particulars could be easily reduced to broad, generalized groupings, aided by the appearance of objectivity through the “view from nowhere” or Apollonian eye which casts the human as the god-like observer of reality at a distance (Cosgrove, 2003; Nagel, 1989).

At the same time, these Renaissance-era views contributed to envisioning the world as a whole and as a whole which could be understood and have meaning. The world could be understood as an entity apart from its constituents while those constituents could also be understood as independent entities. This is the idea which underpins the development of geographical scales of analysis which Agnew (2003) argues are, in order of importance:

1. Global: the world as a whole

2. International: scale as it relates to intra-state relations

3. Domestic/National: scale of individual states

4. Regional: parts of a state

A hierarchy of scales highlights the hierarchy through which geopolitics must operate: from the global to the regional. However, Agnew (2003) argues that geopolitics effectively discounts the latter two scales, and in doing so brands geopolitics as the purview of the global and the international.

Through these early ways of *seeing, t*he world's political diversity has been distilled into various geographical containers, including the world itself. Geopolitics is a way of constructing a worldview which in turn influences actual political practice in the world itself. There is no inevitability to the emergence of geopolitics, however. It reflects the European historical and material experience, grounded in the loss of a religious and dynastic hierarchical worldview through the Renaissance and the Enlightenment. In support, Agnew has proposed a three age model through which geopolitics was practiced and formalized: 1815-1875, 1875-1945, and 1945-1991 (Agnew, 2003). These three ages are oriented around the European and North American history, but due to power disparities and the colonial and cold war projects, also reflect the dominant way of constructing the world by non-European states which emerged from the end of the colonial project.

On the other hand, Klinke (2013) argues that attempts to rigidly demarcate history into discrete units of time in geopolitics, as Agnew (2003) has done is problematic. The very act of carving the world into separates spaces is a counterpart to attempts to do the same with time. However, to understand the modern state of geopolitics, it is nonetheless important to understand its evolution so as to better witness and discern the historical fragments which remain and inform present geopolitics. The periods offered by Agnew should not be interpreted as rigid demarcations of time, but rather useful conceptual guides for understanding broader trends since the end of the Napoleonic Wars.

Civilizational Geopolitics, 1815-1875

Civilizational geopolitics is the immediate successor worldview to the religions and aristocratic/dynastic perspective which had dominated Europe for centuries. It proposes a narrative that fuses the social mission of religion with the uniqueness and superiority of European civilization, alongside the idea of a broken world which Europe can save.

To construct civilizational geopolitics predicated upon a sense of European superiority and solidarity, Europe itself had to be conceived of and constructed as a distinct and different cultural area with common shared interests and a shared history. This idea of “Europe” emerges as Christendom, Jesus' status as a person from the Middle East and the presence of Arab and Iranian Christians notwithstanding. Early maps show Europe as a distinct and largely homogenous region, with minor scalar differences in culture which are nonetheless subordinated to the broader European vision. The seemingly arbitrary demarcation of Europe's eastern extent as the Ural Mountains is part of this broader process to segment out a distinct Europe.

This segmentation was furthered by a narrative which did not explicitly disregard the histories of other cultures. Indeed, we can see this in British colonial representations of Persia in the Royal Geographical Journal as having once been a powerful nation, but which had fallen prey to Islam (E. C. Sykes, 1910) and other depredations and was in need of new inspiration from the United Kingdom to join the world and resume its historical role a civilized peoples in the Near East. This mantle was re-scaled and taken up by Iranians themselves as part of their nationalistic project starting with the ascent of Reza Shah in 1925 and persisting in diaspora communities to this day (Gelvin, 2011).

Thus, civilizational geopolitics was grounded in the medieval and dynastic past, presenting the nation-state as an evolutionary successor to the historic peoples who inhabited Europe. To this extent, the “otherness” of the rest of the world represented opportunities for “conquest rather than recognition” (Agnew, 2003, p. 92), a geopolitical imagining which gave intellectual grounding to imperialist global politics (Agnew & Corbridge, 1995).

Naturalized geopolitics, 1875-1945

Naturalized geopolitics takes its name from a trend in the 19th and early 20th century to embrace perceived outcomes of revolutions in biology by seeing human beings in terms of Darwinian natural selection, and as fundamentally biological organisms obeying certain rules of nature. This idea was extended to seeing states and nations as almost biological organisms needing “living room”, an ideology which supported Nazi geopolitics (G. Ó. Ó Tuathail & Dalby, 1998). The naturalized perspective also lent itself to geography's engagement with environmental determinism, that human societies were simply influenced by their natural environments whereby certain regions would produce humans who were superior or more productive (Peet, 1985).

Agnew (2003) argues that naturalized geopolitics becomes formalized as the Congress of Vienna's Concert of Europe falls apart in the latter half of the 19th century. Groups of states emerged in competition which spanned the globe, culminating in the First World War, which he argues is perceived as an almost inevitable conflict which states saw as the only resolution to the general geopolitical impasse they perceived to exist. The inevitability was seen to be predicated upon the state as a natural organism which corresponded to the biological and social sciences of the time. States, like other organisms, needed space and resources to survive. Other states, as organisms, had a similar desire and the success of one group must ultimately be at the expense of another – a state-based survival of the fittest. Their people were part and parcel of this greater organism and their actions and behaviors would influence the greater good of the nation-state. The emergence of nationalism in Europe, in large part due to the rallying cries ore resistance surrounding the French Revolutionary and Napoleonic invasions (Anderson, 2006), extended biological rationalism to a multiscalar level – the individual and the state were in a naturalized geopolitical feedback loop.

This idea extended into perceptions of superiority based on biology and geography, accelerating a trend which emerged during civilizational geopolitics of turning time into space. This was based in a teleological idea that certain broad areas of the world were at a different stage of a common historical civilizational evolution, and that assistance by Europe was necessary for humanity's greater good and evolution.

Finally, this biological logic found perverse application in the naturalized rationalization (Horkheimer & Adorno, 2007) of Nazi geopolitics with the concept of Germanic 'lebensraum' or living space. The liquidation of certain populations and states, such as Poland, was seen as a natural event rather than a moral one and found intellectual sympathy and support in the naturalized geopolitics of nation-based survival of the fittest. This perspective, was seen by Horkheimer and Adorno (2007) as the final expression of the Age of Enlightenment, with scientific and rational principles applied to a level of precision without regard to morality.

The end of World War II saw geopolitics as a tainted subfield due to its perceived association with Nazism. As an academic discipline few studies were published and the term largely vanished from use. However, as discussed earlier the appearance or disappearance of terms does not imply that the ideas or concepts which the terms embodied are no longer extant. On the contrary, the subsequent era of geopolitics incorporated both civilizational and naturalized elements despite its relative geopolitical stasis.

Ideological geopolitics, 1945-1991

World War II's end ushered in a new era of geopolitics which saw the ideas of civilization and naturalism became subsumed under an ideological conflict between capitalism and communism. This was a move towards a geopolitics of economic organization rather than ones rooted in almost exclusively in time, as stages in human development. It was aided by a popular geopolitical vision initiated by Churchill's famous “Iron Curtain” speech and the explicit doctrine established by US President Harry Truman to defend Greece from communism during its civil war. The idea of environmental determinism or a biological analogy to state conflict shifted towards one where blocks of the earth's surface were considered to be wholly submerged beneath the ideological allegiance of the state (Agnew, 2003). This broader concept is encapsulated in the concept of the first, second, and third worlds which supported the United States, Soviet Union, or were unaligned, respectively.

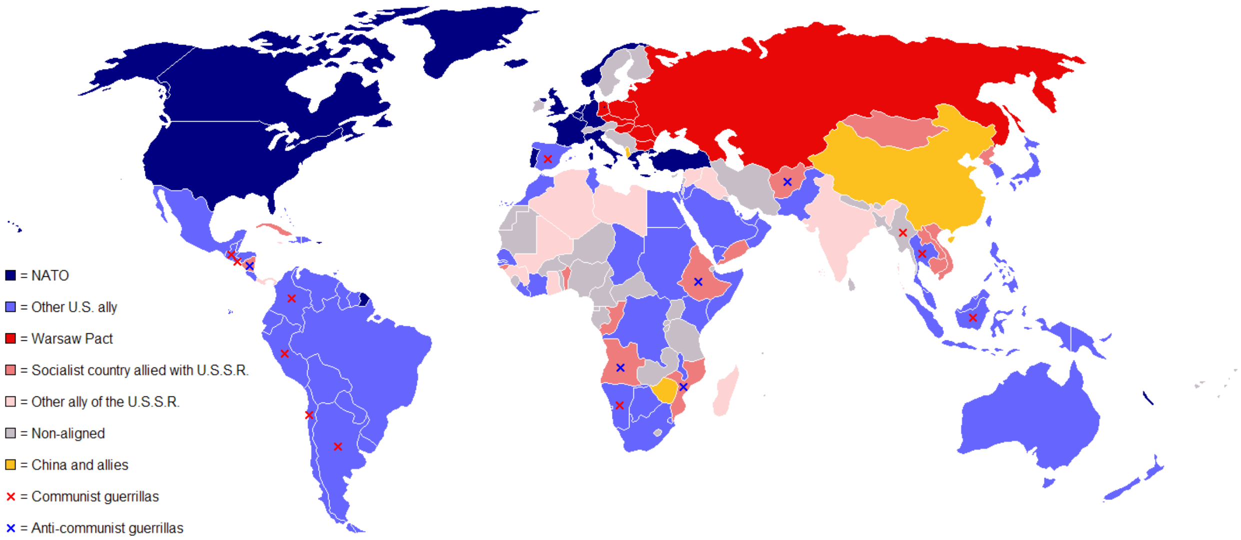

■ = NATO
■ = Other U.S. ally
■ = Warsaw Pact
■ = Socialist country allied with U.S.S.R.
□ = Other ally of the U.S.S.R.
■ = Non-aligned
■ = China and allies
× = Communist guerrillas
× = Anti-communist guerrillas

Fig. 1 - Cold War Alliances in 1980 (“Cold War (1979–85),” 2015)

Local conflicts were dispossessed of their local or historical character and enrolled in the broader ideological global struggle. Longstanding domestic tensions, such as in Vietnam, became existential crises due to the geopolitical concept of the domino effect and containment. Containment theory sought to keep global communism within its 1945 and “fall of China” boundaries while the domino theory proposed that the loss of one state to communism made subsequent losses easier – ultimately ending with the loss of the United States.

The recasting of conflicts to a global scale was made more vivid through the potential for local or international nuclear escalation. This lent a tremendously technological and “de-territorialized” element to the ideological geopolitics through long-range bombers and later intercontinental ballistic missiles (ICBMs). Ideological geopolitics was also posited as engaging with metaphysical, deterritorialized concepts such as the “Evil Empire” and was supported by the potential of hellfire from the sky under the ever watchful eye of Soviet and U.S. satellites. Indeed, ideological geopolitics and its potential for real global annihilation happily wrapped itself in “end of times” rhetoric as the ultimate struggle between good and evil.

As the Cold War continued and the components of conflict shifted, so too did the rhetoric and practice with the United States facilitating greater economic and legal integration with states aligned with its economic and political aims. This was a means of integrating allies and building dependencies designed to align states in the United States' orbit (Agnew, 2005). This integration and cooperation was the infrastructural groundwork for the rise of globalization (Agnew, 2009a) after the Cold War ended. It facilitated the easy spread of the Internet due to the legal, technical, and political legacies left by the global cooperation and integration sought by the United States.

The history of geopolitics – conclusion

The history of geopolitics traces back to the development of perspective and the "Apollonian eye" which established an objective and detached "view from nowhere" of the world (Agnew, 2003; Cosgrove, 2003; Nagel, 1989). At this perspective the world as a whole was easily envisioned and reduced to a political entity. The creation of "Europe" as a distinctive and unique cultural whole was greatly facilitated by this new technologically-enabled worldview. Subsequently, whole politics were envisioned which married ideas of scale with the supposedly civilizationally or racially superior standing of the recently-constructed European ideal.

Geopolitics has informed the direction of national and international politics for over 300 years, and continues to inform contemporary political rhetoric and decisions. The Internet, whose technical and infrastructural foundations were conceived of with ideological geopolitics as a backdrop, is an heir to that geopolitical tradition both in practice and in theory. However, like technology broadly understood, it is both influenced and influencer of the human condition in which it is situated (Ellul & Merton, 1967). To more fully understand the geopolitics of the Internet, therefore, we must therefore briefly examine modern geopolitics. However, before that analysis there will be a brief overview and acknowledgement of alternative geopolitics which can inform subsequent research.

Other Geopolitics

The literature on geopolitics is broad and varied, and more recently has included a strong critical as well as feminist element. While largely outside the scope of this dissertation, critical and feminist geopolitics offer intellectual purchase on cyberspace and geopolitics more broadly.

Critical geopolitics seeks to interrogate the discourses and practices surrounding geopolitics so as to better understand the worlds which are imagined, represented, and discursively constructed. From the perspective of Internet control and cyberwar, critical geopolitics would examine the discourses which have attempted to establish cyberspace as a domain of threat and conflict. This has not been addressed in the geopolitical literature proper, but recent research by Tsui (2008) has demonstrated how contemporary discourse on Internet control has revolved around Cold War rhetoric and geopolitical models. Further, critical geopolitics seeks to engage with issues related to geopolitical identity, and would therefore offer purchase on the ways in which Western states refer to hackers in ways which highlight national identity concomitant with existing discursive representations, i.e. "Chinese hackers". Critical geopolitics therefore seeks to interrogate the normative and examine how the geopolitical normatives are produced and practiced (L. Jones & Sage, 2010).

Feminist geopolitics would seek to extend critical geopolitics through examining "the ways in which the nation and the international are reproduced in the mundane practices we take for granted" (Dowler & Sharp, 2001, p. 171. With regards to cyberspace, Derek Gregory (2011) has argued that the local and the mundane has become a new space for the spread of war through ever-present cyberwar and the militarization of cyberspace. In other words, the local and the private become spaces in which cyberwar becomes manifest, demonstrated in the methods for malware infecting private computers.

Both critical and feminist geopolitics provide vital avenues for understanding and critically examining geopolitics more broadly. At present, there is a lack of literature in academic geography surrounding cyberspace, let alone in critical or feminist geopolitics. For future geopolitical research on cyberspace, both critical and feminist geopolitics offer important and nuanced approaches to better understanding how geography and technology interface within geopolitics.

Further, this section has primarily emphasized the perceptual and cognitive aspects of geopolitics. However, geopolitics is not exclusively representational, and is also a process of doing and becoming. The ways in which the world is represented are vital and often serve as the first conceptual tools in actually embodying geopolitical visions. The importance of geopolitical representations in influencing geopolitical actions is illustrated in Agnew's case of Macedonia (Agnew, 2007), whereby the borders and the national genealogical and geopolitical representations are first established and borders drawn afterwards. Thus, these perceptual and cognitive geopolitics are often the foundations of geopolitical action, hence the emphasis in this section on this aspect of geopolitics. This dissertation will focus on both, despite the emphasis of this chapter.

Modern Geopolitics

The fall of the Soviet Union and the loss of an "other" for geopolitical purposes, as well as rapid developments in globalization and communications led many to believe that the "end of history" and end of geography had been achieved (Fukuyama, 2006). As geopolitics had been largely articulated as a way of seeing and constructing politics using geographical representations, the end of geography and history would usher in a new era devoid of geopolitics. On a more practical level, globalization and the rise of the Internet contributed to a greater sense that the world was a single political entity and concept was undergoing radical change, evidenced through early cyber-utopian visions (Evgeny Morozov, 2012) amongst academics and activists as well as media proclamations of a flat world or a world without borders (de Blij, 2010; Friedman, 2007)

The apparent end of geopolitics did not mean the end of geography or politics. Initial euphoria on new investment vehicles and opportunities for communications and travel were soon tempered by the dotcom stock market crash and the terrorist attacks of September 11, 2001. Although the bursting of the dotcom stock market bubble demonstrated the limits to technology's powers to remake global wealth, it was the terrorist attacks of September 11, 2001 which saw a new geopolitics quickly cobbled together and rushed forward for public consumption and to frame the new world in which Western powers, led by the United States, were to operate.

The “geopolitical other” from the perspective of Europe had often been predicated upon a threat from the east or the Islamic world (Diez, 2004; G. Ó Tuathail, 2005). Early in the construction of the idea of Europe maps routinely displayed Europe as clearly ending where the Middle East or North Africa began (Agnew, 2003) while the border with Russia proved to be more problematic. The invasions of Europe by the early Islamic empire through Spain and later by the Ottoman Turks through the Balkans became the historical backdrop against which Europe could be seen to be ever at peril, separated only by a few miles either at the Bosporus or the Strait of Gibraltar. A familiar intellectual template, therefore, existed in which these cultures, religions, and peoples could be readily assumed to be dangerous and untrustworthy and through the sheer size of the faith in terms of population and geographical extent could be easily constituted as a global threat against “Western” values.

The effort by the United States to limit the Al-Qaeda network into a set geography becomes problematic when the hijackers are seen as truly global citizens, with international educations and residence in Europe and North America. Their lives resembled those of middle and upper-middle class Western citizens who were both well-traveled and well-educated. Regardless, influential political analysts and government officials, such as Karl Rove and President George W. Bush, repeatedly portrayed the problem as one where “they hate our freedoms”, a clash of civilizations, or likened the Global War on Terror (GWOT) to a crusade (Ford, 2001). The world was again drawn into a familiar template of us against them, good versus evil, with the fate of Western civilization at stake. This line of reasoning has not yet abated, through considerations about extremists in the Syrian civil war to European unease with Islamic practices.

Geopolitics, however, is not the exclusive purview of European or North American political elites. Indeed, as Agnew strikingly points out, the worldview espoused by Osama Bin Laden al-Qaeda is one of simplistic geographies and geopolitics of believers and unbelievers and a revivified caliphate (Agnew, 2006). This historical geopolitics was extended through outrage that Saudi Arabia, as the political successor to the Kingdom of Hejaz and the Sharifate of Mecca, was the land of the holy cities of Mecca and Medina. This holiness was defiled by the presence of U.S. troops, despite the very real tensions and historical conflict between Saudi Arabia and the peoples of the Hejaz (bin Laden, 2005; McAuley, 2005).

Geopolitics returned after a brief interlude where neither history nor geography apparently existed from 1991-2001. It was ready-made, constructed from earlier logics and othering of regions and religions. To that extent the present world is a mirror or echo of past geopolitics and facilitating a future geopolitical vision. Agnew, therefore (Agnew, 2003) argues for the potential existence of three new geopolitics for the modern world and the near future.

Globalization and Market Access

Agnew's first model of contemporary geopolitics focuses on existing trends in globalization and expanding market access worldwide. As part of the United States' effort to develop substantive ties with its allies during the Cold War, deep economic and legal ties were developed (Agnew, 2005). These ties laid the foundation for transnational economic integration, enhanced market access, and relatively fluid geographic allocation of capital. The end of the Cold War saw the expansion of this geoeconomic logic as well as a concomitant rise in resistance to neoliberal economic policies.

Protests in Seattle, Rio de Janeiro, and elsewhere against global inequality and the relative ease with which the Internet facilitates transnational organizing have also ushered in a new era of contestation of global policies by presenting an alternative vision for the geopolitics of the future (Agnew, 2003; Juris, 2005). However, both perspectives remain locked in an effort to redefine and strengthen the idea of the state as a geographic framework for regulation and reform. The end result is the development of city-centric zones and hinterlands of rich and poor which leave capital largely free to move around the world with little friction.

The Endless Clash of Civilizations

The next model proposed by Agnew (Agnew, 2003) centers on Samuel Huntington's (Huntington, 1993) controversial thesis that future conflicts will not be ideological, racial, or dynastic as in historical geopolitics. Rather, they will be between nine “civilizations”: Western, Orthodox, Islamic, Confucian, Buddhist, Japanese, African, Hindu, and Latin American tied to associated geographic regions such as Middle East/North Africa and Russia (Huntington, 1993).

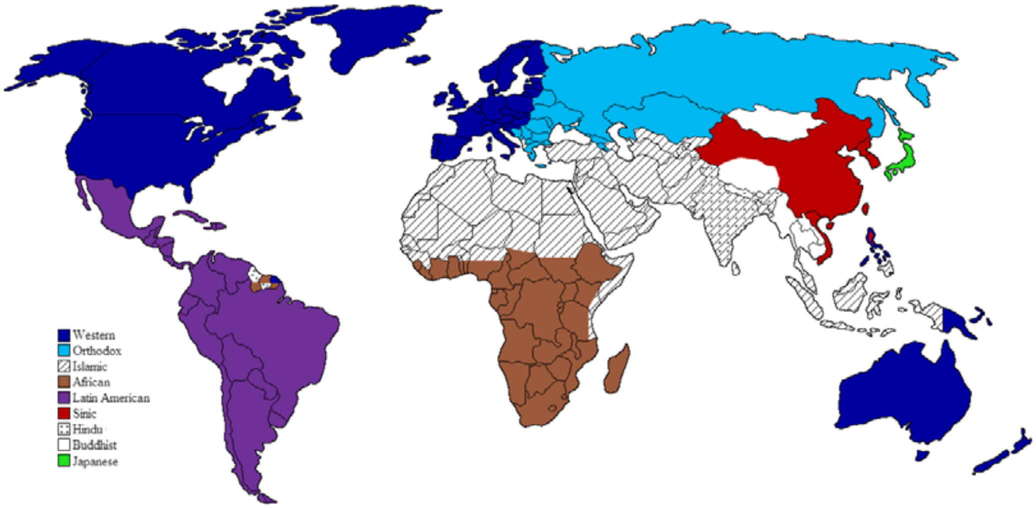


Fig. 2 - The Clash of Civilizations (“Clash of Civilizations,” 2015)

Although superficially reassuring in that it borrows much from the map-centric geopolitical imagination of the Cold War, the Clash of Civilizations obfuscates as much as it reveals. Defining civilizations is tremendously problematic: few Middle Easterners could readily agree that there is a coherent Islamic civilization with disparate cities such as Tehran, Istanbul, Cairo, and Tunis included. For example, the Iran-Iraq war from 1980-1988, with over a million casualties, was a major regional conflict between two branches of the same faith (Hiro, 1989). Further, the “Western” identity includes North America, Australia, and Europe - all of whom have had major political differences surrounding the War in Iraq and Afghanistan as well as on telecommunications laws such as ACTA (Bennett, Breunig, & Givens, 2008). The Orthodox world, further, has seen its own share of recent conflict between Russia and the Ukraine.

All these examples stand to demonstrate the complexity in using a civilizationally-reductive model for current geopolitics. This model in many ways is a re-scaling of previous geopolitical logics, retaining certain geographies while discarding civilizational or ideological imperatives. Further, the idea of classifying individual civilizations and seeing these as monoliths destined to grind against each other perpetually presupposes a broad unifying civilizational logic to each region which impels it to seek to advance at the expense of other civilizations.

Business as usual: the unipolar world

The final model is a traditional one which sees the United States pursuing many of the geopolitical perspectives of the George W. Bush administration. This is a state-centric model where the world continues much as it has since the end of the Cold War. Its main difference, however, is that a singular state – the United States – is global hegemon and the state of last resort. This perspective argues that the United States will fully embrace its unipolar position as global hegemon and seek to maintain its position by preventing the emergence of any serious rival. This is a perspective embraced as the "New American Century" with a United States which actively maintains its large military and flexes its economic might in pursuit of its global political goals (Agnew, 2003).

The counterpoint to the perceived dominance of the United States is the reality of its weakened position. The global integration during the Cold War developed transnational networks which have enabled economic power to migrate out of the United States as a geographic center. The forces which it unleashed in attempting to build a common zone of economic activity have led to it being one jurisdiction amongst many which capital and transnational corporations can choose from. Further, while it remains the world's preeminent military power its deployment of that power is not without domestic and international resistance making unilateral action, especially after the deceptions associated with the invasion of Iraq, increasingly unlikely. Finally, Agnew (2003) argues that without a clear single unifying threat, building international solidarity or cooperation for an extended "Pax Americana" is unlikely as different states or regions will have different interests which they will seek to pursue.

Contemporary Geopolitics – Conclusion

Agnew (2003) proposes three potential models for a future geopolitics. These models were centered on globalization, civilizations, and unipolarity. Each of these models is an inheritor of the preceding three ages of geopolitics by combining various philosophical or infrastructural foundations laid in the past. For instance, the model of market access and globalization is predicated upon the foundations of globalization established as part of the broader political aims of the United States during the ideological geopolitics of the Cold War. That globalization is an extension of those same ideologies of extending and expanding capitalism and market access. Clash of civilization geopolitics finds much of its grounding in earlier civilizational geopolitics in its attempts to define whole civilizations along with the geographical particularities and map-centrism of ideological geopolitics and the "lebensraum" ideas informing naturalized geopolitics. Finally, the unipolar model is essentially a continuation of the status quo of geopolitics since 1815, being state-centric and focused on the maintenance of a state-centric world order, albeit with a single dominant power – the United States.

There are, however, alternative ways of understanding the spaces associated with political power. Since the Peace of Westphalia and accelerating since the fall of Napoleon this has been largely interpreted, in the European world, as centered around states as the legitimate centers of power. However, history shows that there are alternatives to the spatiality of power –

for instance as residing in geographically diverse dynasties as in Europe's middle ages. Thus, future geopolitics may not necessarily be oriented around states and the legacies of historical geopolitics.

The Spatiality of Power

The spatiality of power model is an alternative way to understand power and space in the 21st century. The spatiality of power model has its origins in works by Durand and Lévy (1993) and Lévy (2007) as a means to integrate four ways of thinking about globalization and the world, embodied in four different spatialities. This model was extended by Agnew (2003) as a way to see “beyond geopolitics” (Agnew, 1999, 2003). As originally presented, this model emphasized the ways in which actors could see their power envisioned in alternative spatialities not necessarily tied to the territorial state. In this dissertation, however, the spatiality of power is understood as a conceptual framework for understanding power and resources exercised by states in cyberspace. Thus, rather than focus on actors in cyberspace, the framework is used here to articulate the ways in which different spatial modalities of power always involving states can be configured by the Internet.

Cyberpower, a state's real or potential ability to leverage its cyber resources during times of cyberwar (Kuehl, 2009a), can reflect a geography which is counter to existing political geographical logics invariably centered around the territorial nation-state. This does not mean that cyberpower is deterritorialized or negates geopolitics and geography, but that the potentiality which cyberpower embodies could be spatially organized in configurations which are not centered around the territorial nation-state. Thus, these models merit mention in the dissertation as a way of conceiving of a non-conventional spatial basis for power. The four models for alternative spatialities of power are: an ensemble of worlds, the field of forces, a hierarchical network, and a world society. Each of these will be discussed with brief commentary on the applicability of each model on cyberpower. The "Geopolitics of Cyberwar" chapter will address these spatialities in more substantive terms.

Ensemble of Worlds

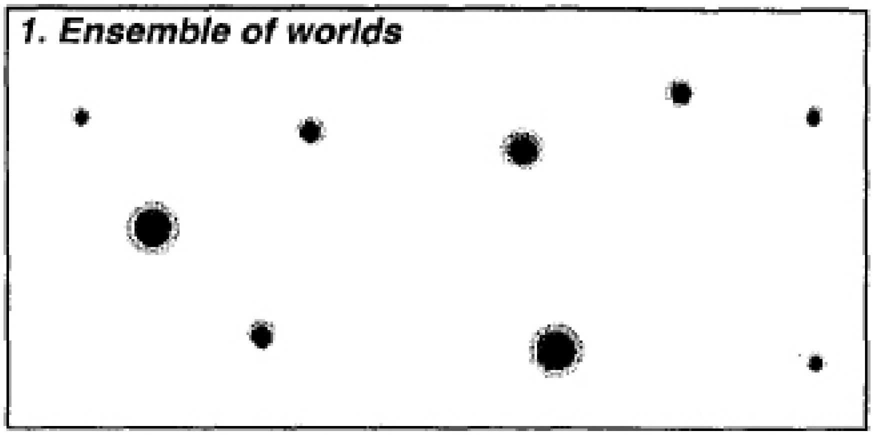


Fig. 3 - Ensemble of Worlds (Agnew, 1999, p. 505)

The models correspond loosely with historical epochs of human political, social, and technological development, such that the ensemble of worlds model echoes early pre-Columbian world cultural regions. In this model cultures and societies are largely isolated from each other aside from sporadic trade interactions. Power is thus directed towards the maintenance and sustenance of the existing culture within its "natural" boundaries.

For cyberpower, this historical model is superficially problematic due to the interconnection and easily networked environments of the global Internet. However, key intelligence and military systems are separated by an "air gap" where these systems are not connected to the Internet in any way. These are often vital systems which would form the focus of a sustained and serious cyberwar effort to compromise. Indeed, this is verified through the StuxNet case where Iran's air-gapped control systems at the Natanz nuclear processing plant were explicitly targeted. The air gap was crossed by planting USB sticks which were then inserted into the vulnerable systems. Regardless, air-gapped systems represent spaces of significant power which are disparate and separate from broader connectivities and the power vulnerabilities those connections facilitate.

The Field of Forces

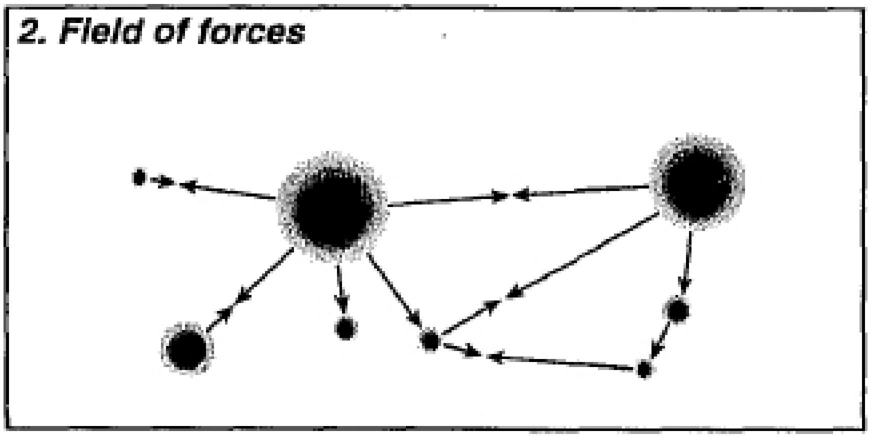


Fig. 4 - Field of Forces (Agnew, 1999, p. 505)

This model maps onto the existing state logic with strictly defined territories and spaces in a geographical zero-sum game in which all territorial gains come at the expense of others. The state is considered the boundary of the society with clearly articulated rights and responsibilities existing within its clearly demarcated geographical boundaries. These boundaries are facilitated by technological developments, such as surveying and cartography, which allow for clearly measuring, mapping, and communicating the boundaries which define this spatiality of power. Historically, this model is similar to the 19th century nation-state and balance of power situation in Europe.

The perspective of cyberpower for the field of forces model is the clearly demarcated autonomous systems logics through which existing states allocate internal computing resources. Further, this is extended through ICANN-enabled administration of domain names and IP addresses. In terms of practice, what this means is that the absolute cyber-resources available for the extension and explication of cyberpower are located domestically in a demarcated and internationally recognized space where no other state or entity has final authority. This is a conventional understanding of “national Internets” (Deibert, 2011) often considered as preceding the much politicized balkanization of the Internet (Goldsmith & Wu, 2008) which has been a policy concern of the United States and many European states.

Hierarchical Network

The hierarchical network moves from rigidly defined spaces towards cities and their associated hinterlands. These cities exist in a global mesh network of regions, peripheries, semi-peripheries where the dominant connections are those of trade and international finance alongside labor-related migration. This is a pattern consistent with contemporary globalization which facilitates uneven global development and relatively footloose capital. Agnew argues that power is largely based on location relative to the locations or places most closely associated with being global centers of finance or trade.

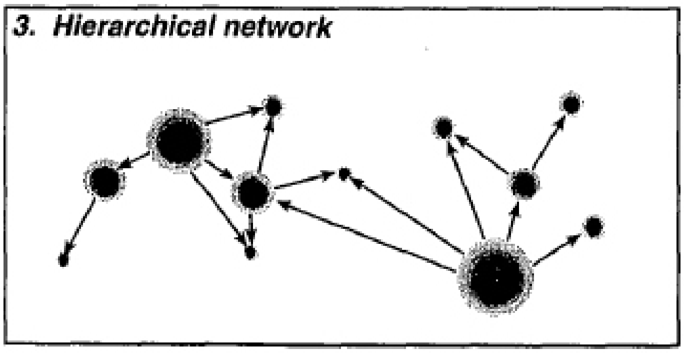


Fig. 5 Hierarchical Network (Agnew, 1999, p. 505)

This model is consistent with asymmetric cyberpower associated with states, non-state actors, and social movements. These actors utilize global cyberspace in pursuit of their political and conflict-oriented goals through utilizing and leveraging the geographies of cyber-resources. These actors utilize global cyberspace in pursuit of their political and conflict-oriented goals through utilizing and leveraging the geographies of cyber-resources. Social movements, such as Iran’s Green Movement or the Occupy Movement, while highly localized and geographically focused, nonetheless utilized global communications resources to pursue their more localized goals. For states, North Korea remains a state with a relatively undeveloped cyber infrastructure and lacks significant cyber resources to be considered a conventional threat. However, it leverages this by employing mercenaries and purchasing resources from China, Russia, and many Eastern European and Western states to launch attacks and conceal their activities (Clarke & Knake, 2012).

World Society

The final model is that of the world society grounded in a global sense of "humanness" which transcends borders and cultural identities. This is the groundwork for addressing global problems such as climate change or global inequality. The centers of power revolve around social groups rather than discretely bounded entities or their locations to places of economic power. Global communications is a foundation of a global public opinion, best expressed with global opposition to the U.S.-Iraq war under President George W. Bush.

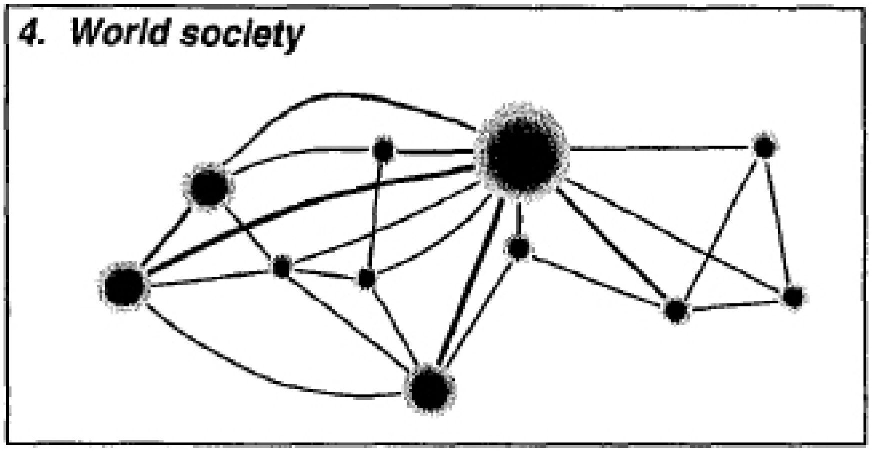


Fig. 6 - World Society (Agnew, 1999, p. 505)

This model is familiar as many elements embody the present state of the world. For cyberpower this has been demonstrated most acutely through the example of Anonymous, which leverages global communications and social groupings to present a relatively potent cyberpolitical force responsible for numerous high-profile cyberattacks. The World Society model, for example, allows Anonymous, as a collective for individual political (Norton, 2012), to leverage global communications and social groupings to achieve its aims. With Anonymous, an individual or small group of individuals will propose an "operation" to the group afterwards interested members will agree to pursue it (Norton, 2012). In contrast to the hierarchical network model, the world society model is less about resources and nodes and more about social groupings and connectivity (Agnew, 2003).

These are issue-networks (R. Rogers, 2002) which arise around social groupings where the global commons of the Internet associated with social media and open-source software enables amateurs and interested individuals to quickly gain scale and power. This power rises, migrates, and dissipates rapidly such that any strict or constructive action against it becomes difficult. It can also be used with the "patriotic citizen" model of cyberwarfare where citizens launch attacks. Examples of this model are the 1999 attacks against NATO (D. E. Denning, 2001; Lesk, 2007), the 2007 cyberwar against Estonia (A. Schmidt, 2013), and the 2009 citizen interventions in Iran (Hearn, Mahncke, & Williams, 2009).

Spatialities of power – discussion

These models of spatialities of power envision alternative ways in which power and space can exist apart from the territorial state dynamic which dominates geopolitical thought. Though power can be concentrated within a territorial state and the state can function as an effective facilitator of power, it is not the only entity which wields power nor does it have an exclusive monopoly. Further, as geographies, borders, and territory become more ethereal and conceptual in practice the need arises for understandings of power which relate to this greater ephemerality of heretofore solid geographic concepts. Viewing power in terms of spatialities rather than rigid geographical boundaries allows for the existence of multiple scales of power which can exist simultaneously. The contemporary globalizing world shares many features of multiple spatialities of power despite the insistence in conventional and popular geopolitics of the primacy of the state.

Geographical Concepts

Both modern and historical geopolitics are underpinned by several geographical concepts, namely those of borders, territory, and sovereignty. Even the alternative spatialities of power make reference these concepts if only as a means to differentiate itself from conventional geopolitical thinking. Nonetheless the concepts are highly influential in terms of policy, popular perceptions, and practice by states and non-state actors. Further, these geographical concepts form the logical underpinnings of how much of the Internet is technologically administered and resources assigned.

In order to better understand the dynamics of geopolitics and the ways in which conventional geographical ideas have influenced cyberwar, this section will briefly discuss these three core geographical concepts.

Borders

Borders are "...the physical and highly visible lines of separation between political, social and economic spaces..." (Newman, 2006, p. 144) and represent a means through which human groups attempt to control, symbolically and in actuality, sources of threat or sustenance (Oxman, 2006). Indeed, even the act of naming and of establishing species and genii is itself an act of demarcation (Rousseau, 1987a) and a conceptual extension of a "territorial temptation" (Oxman, 2006). The process of "othering" which has been at the core of much of 20th century geopolitics

(Agnew, 2003) is an example of this temptation and tendency through which control may be symbolically established through a demarcation of difference.

A brief history of borders

The idea of demarcation of space and its strict enforcement is not a concept which was developed in modern times. Archaeological evidence demonstrates that certain spaces were considered sacred to many peoples such as sacred caves or lakes (Sponsel, 2015). Entry into these spaces often demanded dressing in a certain way or undertaking ritual ablution in order to purify oneself. Further, many societies had concepts of male and female spaces in which certain behaviors and types of knowledge were appropriate (Bhathal, 2006). This is to say that the idea of bordering is not a modern concept, and that the idea of demarcating space is at least as old as recorded history.

The ways in which space is demarcated vary with changing technologies and social norms. Studies on modern hunter-gatherer tribes show that they develop reciprocal agreements on hunting or foraging grounds which are demarcated through common natural features, such as with the !Kung people of southwestern Africa (Diener & Hagen, 2012). Sometimes, however, these ancient borders are directly demarcated through the laying of stones or carving of trees, a practice common with the Veddas of Sri Lanka (Diener & Hagen, 2012). Enforcement of these borders varied with tribes and peoples in much the same way that border enforcement varies between states. Elaborate rituals could often accompany requests for border intrusion, and our own passport system can be seen as a descendant or modern interpretation of these ancient demarcating rituals and practices. The ensemble of worlds model for the spatiality of power demonstrates how a world such as this would exist, as some groups had rigid boundaries and others more permeable ones.

As agriculture progressed and human societies became increasingly sedentary, the territorial temptation did not subside. Rather, new settlement patterns developed with increasingly permanent locations for habitation and alternative methods for organizing the spatiality of power. Groups laid claim to farming regions or regions, and these areas became valuable to group survival and desired by other groups out of necessity, greed, or any number of other reasons. The expansion of tax-collecting and tribute facilitated a more static view of territories, one in which their borders could be seen as containers of resources or income rather than as the strict limits of environmental/spiritual/natural sustainability which underpinned many pre-agriculture borders.

Early border conflicts are recorded on some of the tablets of ancient Sumeria (Diener & Hagen, 2012), highlighting and providing documentation of the idea that border violations could contribute to armed conflict, and more importantly that an early version of the “field of forces” model of spatialized power was extant more than 7,000 years before the present. Sumeria, ancient Egypt, and the Mayan civilizations all actively marked their borders with stone slabs (Diener & Hagen, 2012) which were explicitly erected as distinct from carvings or natural boundaries. Though simple causation may tempt one to assume that more permanent settlements led to the establishment of (seemingly) more permanent borders, it can also be considered that technologies and ways of envisioning polities, space, and power facilitated a desire to more accurately demarcate boundaries.

These static settlements guarded vital resources, and were often the target of other powers attempts to seize territories. Ancient empires, such as the Persian or Akkadian empires eventually coalesced through repeated conquests and through judicious delegation of power to local viceroys. In this way the strength of borders could vary throughout an empire not only due to relative threats but also through agreements with client or vassal states which managed their local affairs (Diener & Hagen, 2012). Empires, such as the Persians, could contain various polities including nomadic tribes and semi-nomadic pastoral groups in addition to city-states, cities, and kingdoms. In the case of the Roman Empire, certain critical boundaries were clearly demarcated, such as Hadrian's Wall, while others were left “fuzzy” as in central Germany (Diener & Hagen, 2012). An empire could theoretically be comprised of varying polities all with differing interpretations of borders and the territorial temptation. These borders could be unequally demarcated, reliant upon the guidance of local rulers or chiefs, and vary depending on the varying local or regional geographic particularities of the empire.

In the ancient world alternative polities and interpretations of borders existed simultaneously and often within each other. Unlike the modern conception of strict nation-state borders and centralized state power (articulated in the field of forces), power could be distributed or shared spatially across scales and between or within polities, as with empires. The development of more sophisticated technologies and increasing economic and military links with distant polities allowed for the relationship between borders and political power to become less based on local contingencies and instead migrate to an appeal to an objective Apollonian view from nowhere (Cosgrove, 2003; Nagel, 1989) grounded in the “nation” or the body of the monarch.

The modern state system depends upon a “view from nowhere” where the state can be seen as existing independent of local contingencies. It is an almost metaphysical existence and a political-geographical mythology which develops as technologies facilitate the demarcation and communication of boundaries. While much has been written on the ability to demarcate boundaries (Sahlins, 1991), the development of cartography and mass-produced maps also served to reinforce the collective fiction of stable, objective boundaries which exist independent of any local conditions which might mitigate their objectivity.

The era of feudalism saw overlapping boundaries governed by aristocratic lineages, marriages, and dynastic competition existing in a patchwork across Europe. The same feudalistic logic existed in the Middle East as well, implying a general Western and Near Eastern trend towards borders and boundaries being less vested in nations or polities and more vested in individuals, families, clans, tribes, and dynasties. The loyalty or geography of a territory had less to do with territorial contiguity or even ethnicity or nationality and more with the feudal chain of allegiances. Thus, a region could have a lord which had married into a family and who resided hundreds of miles away and did not speak the language yet who reigned and was recognized as the local ruler. The myriad of proposed monarchies during the First World War headed by distant families were modern manifestations of this ancient trend.

The 1648 Treaty of Westphalia attempted to address many of the conflicting allegiances and overlapping hierarchies and fealties and general geographical ambiguities of the time. The predecessor to the modern territorial state was emerging prior to the Thirty Years War, and the Peace sought to address the idea of borders, territory, and sovereignty in an emergent way in hopes of avoiding another major conflict. The treaty recognized the exclusive authority over specific territories (Agnew, 2009a; Elden, 2007) something which had major implications for the spatiality of power. States could govern with demarcated boundaries, sovereign territory, and had mutual recognition. Further, dynasties or vassals could no longer unilaterally wage war as the legitimate actor which could leverage violence was now the state.

The Treaty of Westphalia's emphasis on demarcated boundaries had technical foundations in The Treaty of the Pyrenees in 1659 which created the first modern border mediated by technological innovation (Elden, 2007, 2010; Sahlins, 1991). The accuracy of these new technologies was met with the problem of establishing where borders should be drawn. Thus, while new technologies enabled greater accuracy, the question of locating borders emerged and was resolved through the emergent idea of “natural borders”, of which the Pyrenees and Rhine are two examples (Elden, 2007, 2010). While portrayed as inevitable and objective, natural boundaries more often than not reflected the political aims of states rather than an idea grounded in scientific research.

Natural borders, coupled with early nationalism after the defeat of the French, contribute to the emergence of the nation-state and its often politically motivated and arbitrary boundaries in 19th century Europe. The borders of the nation-state were presented as inevitable, ancient, and enabling the undisputed right of the majority to exercise complete sovereignty over what occurred within those borders (Agnew, 2007a). These borders are first established, and then the sovereign myth is filled in (Agnew, 2007a) through making the borders seem real and ancient. Agnew (2007a) pursues this in his study on the borders of Macedonia:

> “In this construction, it is borders and the threats to them from beyond (and before) which they conjure up that makes the nations and not vice versa. Once the borders are oh so

> tentatively in position and not before, the nation-state in its turn begins to make its place." (Agnew, 2007a, p. 416)

The nation-state creates a collective mythology which serves to function as a raison d'etre for the state itself. These borders serve as a foundation for the "territorial trap" (Agnew, 1994) where the state's borders are a container for society and the limit between the domestic and the foreign, as well as demarcating fully sovereign space. This is the present conception of borders in the international system, and the one upon which much of international finance, transportation, communications, and politics is based.

History of Borders - Conclusion

This brief history of borders has traced bordering and borders from ancient, pre-modern times up until the dawn of the international state system. Borders and bordering represent an impulse within human societies to demarcate and delineate space, be it conceptual or physical. From early sacred and gendered spaces to the abstracted and often arbitrary borders of modern states, human societies and groups have responded to the "territorial temptation" (Oxman, 2006) through methods varying in complexity and abstractness. The modern conception of borders has shifted, though the dominant image of rigid borders remains in popular geopolitics. These borders present tremendous ethical challenges as the difference of a few feet on the ground can mean the difference between life and death, of political participation or repression, and of poverty or opportunity. These are extreme binaries, but conflicts around the globe continue to remind us of the importance of borders in setting limits to and enabling futures.

The present international state system and its conception of borders serve as one of the pieces of geographical logic which informs policy and international relations, in addition to framing cyberwar. However, the changing nature of capital, communications, trade, and travel has contributed to a changing interpretation of borders, despite their cartographic and legal rigidity. Some have argued that we are entering a period where borders are less relevant or even where the state itself is deteritorrialized (Diener & Hagen, 2009, 2012; Ōmae, 1995). On the other hand, post-9/11 restrictions on human travel within certain bounded spaces and the persistent geographic humiliation of Palestinians (Agnew, 2009a) demonstrate that borders are still relevant.

Geopolitics & Territory

The international state system is predicated upon a global ensemble of mutually exclusive territories which are generally considered as being "...a bounded space under the control of a group of people, with fixed boundaries, exclusive internal sovereignty, and equal external status" (Elden, 2013b, p. 18). Territory itself is held to be something self-evident and enclosed by borders and over which sovereignty is exercised by a territorial state. No other entity is accorded international recognition or acceptance.

However, recent research has argued that the borders which bound territory and the sovereignty which those borders demarcate must take as their ontological prior the *idea* of territory proper. Much in the same way that the nation precedes its borders (Agnew, 2007a), so too does the idea of territory precede the territory itself and the geographical techniques which reify territory. The concept of territory is metaphorically extended into air (Butler, 2001; Graham, 2004; Kaplan, 2006; Williams, 2011), the sea (Mahan, 1987; Oxman, 2006), and under the earth (Bishop, 2011; Elden, 2013a) as the concepts of of air space, territorial waters, and subterranean spaces respectively. Each of these are domains where the idea of territory has taken hold, despite its logical and conceptual grounding in terrain and the land itself. As states move significant portions of flows and actions into cyberspace, and with the explicitly political nature of the Internet and its artifactual politics (Winner, 1980), the concept of territory becomes vital in understanding the geopolitics of cyberspace.

Territory is a contested concept, often confused with the idea of territoriality which itself is confused with biology and political action. Two general definitions for territory exist within the geographical literature: territory as controlled container and territory as outcome (Elden, 2010). The first definition is the common standard definition which argues that a territory is some bounded space under the control of a group of people, be they tribe, dynasty, or state (Diener & Hagen, 2012; Elden, 2010; Giddens, 1987). The second definition has its roots in biological research on primates (Ardrey, 1971; Sack, 1986) and other animals which argues that territory is simply a result of territoriality, a biological impulse present in certain animals.

Neither definition adequately describes territory or the methods by which the concept is made real. This lack of conceptual clarity has been recognized by several geographers, each of whom developed important concepts through which the contested idea of territory could be understood. At first, early thinkers engaged with territoriality rather than territory directly. Territory was, therefore, taken as something implicit and understood rather than as the subject of inquiry itself. *How* territory came into being became a topic of interest. Thus, Robert Ardrey's *Territorial Imperative* argued for an emphasis on the creation of territory (through territoriality) as an engagement with animal behavior and biology, grounding the idea of territory as something natural and inevitable based on biological determinism (Ardrey, 1971). Territory itself did not precede territoriality, rather it was a natural outcome of an equally natural process of territoriality. This approach is reminiscent of naturalized geopolitics (Agnew, 2003) whereby the state and its actions were natural and inevitably determined by nature rather than directed human intentions.

Urban geographer Edward Soja argued against a biologically deterministic territoriality and towards one which was politically and socially determined in *The Political Organization of Space* (Soja, 1971) and space organized into spheres of influence exclusive of each other. Territoriality occurred at multiple scales, according to Soja, rather than existing solely at a scale conducive to “grander” politics. Yet again territory remained underutilized as a concept with emphasis placed on the processes of developing territory as having primacy.

Jean Gottmann developed the first significant investigation into territory itself and argued that territory is a geographical expanse which coincides with the extent of a state's jurisdictional authority (Gottmann, 1975). Further, Gottmann believed it is a concept “generated by people organizing space for their own aims.” (Gottmann, 1975, p. 29) and as such it is neither natural or inevitable in shape and constitution. It exists as both political and geographical concept: political because it ignores geography, geographical because it is bound by it. Thus territory exists as a function of this duality between the political and the geographical.

Territory is a concept whose meaning has shifted throughout history, and Gottmann acknowledges that at the time (1970s) territory was losing its importance as a strategic element of power and increasingly becoming a means to organize economics and political opportunity (Gottmann, 1975). It is a “psychsomatic device needed to preserve the freedom and variety of separate communities in an interdependent accessible space.” (Gottmann, 1975, p. 45) and has its existence in social utility. Thus, Gottmann's later book *The Significance of Territory* (Gottmann,

1973) extended this thinking towards one which sees territorial concepts as being influenced by human ideas and tendencies and social, subject to politics, in nature.

Swiss geographer Claude Raffestin argues for a Janus-like approach to territory which has two faces: concrete and abstract and that true human territoriality includes both (Raffestin, 1984). At first, Raffestin sees territory in a multiplicity of ways: from cities to broader political constructs. Concrete territory can be the physical and built environment (such as a city) or the borders and boundaries of a modern nation state. These concrete structures guide and to some extent determine the direction of human behavior, politics, and social development in a technologically deterministic way. Abstract territory, on the other hand, represents precisely those social practices and political constructs which guide lived existence within concrete territories (Raffestin, 1984). To Raffestin territory is at one point technological and on the other culturally symbolic, but both parts are mutually constitutive. It makes no sense to speak of a territorially-contingent way of life without both the territory and the life constructing each other.

Engaging more with territoriality rather than territory, Robert Sack in *Human Territoriality* migrates territory and territoriality towards a social construct, predicated upon power relationships (Sack, 1986). As Murphy (2012) argues, Sack's perspective is rooted in a specifically European experience and understanding yet is presented in universalist terms, as evidenced by the title's assumption that his interpretation of territoriality, predicated upon power and control, is the one way in which territoriality is evidenced with humans. As research into nomadic and tribal relationships to place and power demonstrate (Diener & Hagen, 2012), there is no global standard for territoriality. Regardless, Sack's contribution migrates territoriality and territory into concepts which are on the one hand rooted in the European political and historical experience and which on the other hand are extended to the globe as a whole. The definitional ambiguity of territory itself remains, despite serious and sustained engagement by geographers with the notion of both territory and territoriality.

Stuart Elden's recent work (Elden, 2007, 2009, 2010, 2013a, 2013b) historically contextualizes territory as a concept or political technology developed in the European historical experience, now closely associated with the state. It is a political technology because it is a mode of thinking, or *technique* (Ellul & Merton, 1967) and a method through which a world is made or remade (Winner, 1980). Territory, to Elden is a summation of a variety of techniques encompassing "...legal systems and arguments; political debates, theories, concepts, and practices; colonization and military excursions; works of literature and dictionaries; historical studies, myths," (Elden, 2013b, p. 17) while at the same time relying on explicitly technological (in the sense of artifacts) through "...geometrical instruments, statistical handbooks, maps, land-surveying instruments, and population controls" (Elden, 2013b, p. 17).

Thus, for Elden territory is not simply a means of deciding something is to be bounded and then asserting that to be territory. Utilizing the work of Jean-Jacques Rousseau he seeks to demonstrate how Rousseau's 18th century missive on the establishment of civilization through the demarcation of property was already late, and something Rousseau anticipated by arguing that the logic for the idea that land could be bounded, claimed, and owned was the culmination of a long series of social, cultural, and political change enabling that idea to exist. Rousseau's exact quote is instructive:

> "The first person who, having enclosed a plot of lands, took it into his head to say *this is mine* and found people simple enough to believe him, was the true founder of civil

> society [civilization]. What crimes, wars, murders, what miseries and horrors would the human race have been spared, had someone pulled up the stakes or filled in the ditch and cried out to his fellow men: ‘Do not listen to this impostor. You are lost if you forget that the fruits of the earth belong to all and the earth to no one!’ But it is quite likely that by then things had already reached the point where they could no longer continue as they were. For this idea of property, depending on many prior ideas which could only have arisen successively, was not formed all at once in the human mind. It was necessary to make great progress, to acquire much industry and enlightenment, and to transmit and augment them from one age to another, before arriving at this final stage in the state of nature. Let us therefore take things farther back and try to piece together under a single viewpoint that slow succession of events and advances in knowledge in their most natural order.” (Rousseau, 1987b, p. 60)

This passage encapsulates the idea of territory as political technology. At first, it is simply “believed” by others rather than reasoned or demonstrated. Belief has an important component of being self-evident and needing no rationalization as it is normative in structure and finds grounding in broader social and cultural trends. To wit, Rousseau addresses this by arguing that this idea of territory (property) was the culmination of many earlier ideas, and later argues that to have arrived thusly at bounded property depended vitally on the development of technologies to store, record, and transmit information (Rousseau, 1987b). Territory is not straightforward, but historically generated and owing to technologies which demarcate, communicate, transmit, and store information about the world and present it in ways which normalize it. Maps of the “cartographic state” (Branch, 2014) are methods through which that state is normalized through reproduction in public and private space (Curry, 1999a).

Elden is careful to avoid casting territory within Agnew's influential “territorial trap” (Agnew, 1994). Agnew saw modern international relations as falling into a territorial trap of three components:

> “The first assumption, and the one that is most fundamental theoretically, is the reification of   state territorial spaces as fixed units of secure sovereign space. The second is the division of the domestic from the foreign. The third geographical assumption is of the territorial state as existing prior to and as a container of society.” (Agnew, 1994, pp. 76–77)

Agnew's intention was to highlight the way an emphasis on strict territorial states as the ultimate (legitimate) unit of global power avoids how power exists in alternative spatial configurations (Agnew, 2010). The territorial trap creates a static or “frozen geography” in which power and action are only vested in the territorial state which itself is a historically contingent spatial organization of power and politics, at the expense of engaging with the multiple geographies and scales and complexities of politics and political action worldwide (Agnew, 2010). To move forward out of the territorial trap, Agnew (2010) argues that territory should be seen as a power which is not the exclusive purview of states, and that it is contingent upon relationships which change and shift and can also redefine the notion of territory itself. Finally, despite recent attention on territory itself, territoriality remains an important concept as states or other actors can use its methods and logic to pursue other power goals, such as redefining regional or global supra-national power arrangements (Agnew, 2010).

Elden's (2013b) approach to territory does seek to move beyond the territorial trap towards territory as a political technology used by social or political actors. It is a mixture of “political, geographical, legal, technical, practical, and relational questions.” (Elden, 2013b, p. 16) and these questions themselves have historical genealogies and contingencies. Thus, territory is, as Elden argues, a process and one which is relational in the Liebnizian spatial sense (Alexander, 1998) as well as technological as it has historically measured and controlled land

and terrain. Territory is a political technology and broader process through which “national spaces” can be constructed and articulated (Painter, 1995).

Both Agnew and Elden seek to move past territory in its conventionally and popularly understood form and towards seeing territory more conceptually. It moves territory away from a static background concept and to the foreground, becoming a “bundle of political techniques” (Elden, 2013b, p. 17) that creates the very idea of territory which grounds the territorial state itself. Thus, the notion of territory is fluid and open to interpretation and change, and can most recently be seen in the way it is used to bound or open the Internet as a means to exercise interpretations of sovereignty.

The ways in which states filter their Internet, through technical and activity regulation, be seen in a broader theoretical context as establishing Elden's sense of territory. In other words, the filtering mechanisms discussed earlier in this section are the means by which a state creates territory in cyberspace.

This form of territory is relational and less dependent upon traditional notions of the territorial state. Its background power dynamics, established in the working groups which determine the Internet's technical development and governance, embrace a sense of supra-national non-territorial power which Agnew (2010) sees as a future for engaging with a more fully-formed geopolitics. Despite this, however, the state remains a crucial actor in cyberspace and the existing alternative non-territorial governance methods remain under threat, demonstrated by Russia's efforts at the ITU as well as the continued balkanization of the Internet along state territorial borders.

Territory - Conclusion

This section has discussed a multiplicity of views on territory, finally arguing that territory is a concept, as embodied in recent research by Agnew (Agnew, 2010) and Elden (Elden, 2013b). Territory is not simply a static object, but something contingent upon trends in technologies, law, political thought, and cultural practices. Thus, territory is a concept which continues to have relevance in the modern world for international politics. State territory is made and remade, and this includes the expansion of state territory to include the Internet.

Sovereignty and Sovereignty Regimes

The traditional understanding of the modern state system has seen sovereignty as a form of power exercised exclusively by states. This is a territorial and terrestrial expression of political power which trends in modern technology, trade, and law have altered. This has chiefly come through an uncritical acceptance of the geographical assumptions which underpin much of geopolitical discourse. Three assumptions underpin geographies of power:

> "…first, that states have an exclusive power within their territories as represented by the concept of sovereignty; second, that "domestic and "foreign" affairs are essentially separate realms in which different rules obtain; and finally, that the boundaries of the state define the boundaries of society such that the latter is totally contained by the former." (Agnew, 2009a, p. 22)

These assumptions reinforce each other so that a state-centric view emerges whereby sovereignty is the exclusive purview of the state itself, and further that the state is an entity which has always existed and exercised sovereignty in similar ways through (Agnew, 2009a).

Further, sovereignty has historically been linked to the state and its territory (Agnew, 2005; Elden, 2009) and as a function of state power and authority. This is a historical evolution from the physical and earthly body of the monarch to the physical territory inhabited and demarcated by the nation. However, sovereignty can be seen as disaggregated and relational, through which states can share or change some aspects of their territorial authority for specific issues, such as those relating to the natural environment (Choucri, 2012). Historically, sovereignty has never been firmly rooted to the territorial state, and has been implemented and practiced in a variety of ways globally and historically. It is spatiotemporally contingent and its modern conception is an over-simplification of a complex concept and social practice.

The idea of utilizing the political technology of territory for explicit political, economic, or social goals, known as territoriality (Agnew, 2005), further disaggregates sovereignty from territory. As Agnew articulates, this implies that “political authority is not restricted to states and that such authority is thereby not necessarily exclusively territorial” (Agnew, 2005, p. 441). There are multiple ways in which sovereignty can be practiced and articulated, in some ways more closely connected to territory and in others less so. This spatial differentiation in sovereignty is expressed in sovereignty regimes, which are different ways in which elements of authority and power are unevenly distributed around the world. Agnew proposes a typology of four sovereignty regimes, centered upon two axes: state territoriality (the use of territory for explicit political, social, or economic goals) and central state authority (Agnew, 2005, 2009a). These axes are interpretations of Mann's despotic and infrastructural power:

> “The first sense [despotic power] denotes power by the state elite itself over civil society. The second [infrastructural power] denotes the power of the state to penetrate and centrally co-ordinate the activities of civil society through its own infrastructure.” (Mann, 1984, p. 188)

Thus, state territoriality is its infrastructural power and despotic power is articulated through central state authority. Each state approaches these forms of power differently, and is enrolled within different sovereignty regimes based on their approaches.

Four “ideal type” sovereignty regimes have been identified (Agnew, 2009a) which hold as variables the central authority of the state and the state's relationship to its territory. These four types are: classic, integrative, globalist, and imperialist. The four types are extremes in the present practice of effective sovereignty rather than yet another form of rigid geographical assumptions about the state and sovereignty. They demonstrate possible configurations of modern sovereignty rather than seeing sovereignty as it is. That is, they demonstrate the possible ranges of effective sovereignty in the modern state system. The next section will briefly describe each sovereignty regime and then provide examples of how cyberspace is constructed under each regime.

		STATE TERRITORIALITY	
		Consolidated	*Open*
CENTRAL	*Stronger*	Classic	Globalist
STATE	*Weaker*	Integrative	Imperialist
AUTHORITY			

Table 1: Sovereignty Regimes (Based on Agnew, 2009a, p. 130)

Classic

The era of absolute monarchies under which Westphalia was established has given rise to a similarly despotic conception of modern sovereignty. The regime of classic sovereignty lies closest to the traditional Westphalian model of sovereignty which dominates contemporary political thought. This regime is generally associated with centralized, authoritarian states which exercise (or seek to exercise) as much control over their borders and external transactions as possible. These states would have a strong sense of central state authority and a consolidated relationship to state territory (Agnew, 2009a). In other words, both power and territory are held closely by the state, with sovereignty applied as effectively as possible across the geographical territory under state control

Integrative

Integrative sovereignty is a more complicated understanding of sovereignty which sees state authority as weaker yet state territory as nonetheless closely held and consolidated. Agnew (2009a) states that it is more analogous to the European Union, where there are different government and governance strata overlapping at different geographical scales. This form of sovereignty sees Westphalian states cooperating to create formally and legally create an alternative, geographically bound form of collective sovereignty by sacrificing some local/regional levels of sovereignty.

Globalist

Globalist sovereignty is a component of the broader process of globalization. The origins of globalization stem from political, economic, and military networks built largely between the United States and its allies during the Cold War (Agnew, 2005). This process saw other states accede to a level of enrollment in a broader globalist form of distributed sovereignty, typically underpinned by global financial markets and regimes (Agnew, 2009a). The historical foundations of globalist sovereignty regimes comes from the British Empire, whose trade and financial networks were largely incorporated into the postwar proto-globalization Cold War era networks through which the United States sought to extend its influence and counteract Soviet power. Interestingly, this form of globalist sovereignty dominated by a hegemon (The United

States) has come under threat from the very institutions which served to under pin its foundation: financial markets and common international legal regimes (Agnew, 2005).

Imperialist

The final sovereignty regime is the imperialist regime. This regime would constitute a “failed state” such that state authority is tenuous at best due to internal corruption and separatist conflict. This form of sovereignty need encompass an entire state, but rather can consist of regions within one state or across multiple states. This sovereignty regime is considered as imperialist due to domestic reliance upon external elites, be they institutional such as the IMF (Agnew, 2009a).

The specific configurations of states allows them to have a tendency towards one or more sovereignty regimes. For instance, China is a highly centralized state with a strong emphasis on territorial integrity. Thus its infrastructural and despotic power tends it towards Agnew's classic sovereignty regimes whereby a state has stronger central authority and a more consolidated state territoriality. The United States, by contrast, is considered to be within the globalist sovereignty regime, owing to its more open approach to state territoriality, facilitated through its sponsorship and enrollment in various economic regimes challenging state sovereignty. Despite this, the U.S. still has a strong centralized government authority and power which both challenges and enhances its position as global hegemon, associated with the globalist sovereignty regime (Agnew, 2005).

State territoriality and centralized authority, as functions of infrastructural and despotic power respectively, are ways in which a specific state exists within the global continuum of states and state sovereignty regimes. In many ways this echoes the Platonic ideal of security and opportunity vis-a-vis territory (Gottmann, 1973), with an emphasis on the need for flexibility in state territoriality in different geopolitical and sociopolitical contexts. Following this, Agnew's typology allows for a flexibility whereby the state is seen within a historical and geopolitical context, as well as one which is technologically contingent (Winner, 1980) through artifactual politics. The sovereignty regime is not something imposed from above, or a metaphysical concept, but rather reflects a sociopolitical form of life **,** an emergent process from state practices and policies.

In addition, through the concept of effective sovereignty (Agnew, 2005) argues that sovereignty must be seen as a principle of human interactions rather than the domain of states exclusively. Further, that states are participants in a variety of regimes of sovereignty which see centralized state authority and state territorial relationships as the variables. Thus, "...sovereignty is made out of the circulation of power among a range of actors at dispersed sites rather than simply emanating outward from an original and commanding central point such as an abstracted 'state'" (Agnew, 2009a, p. 9). The ability of the state to exercise exclusive sovereignty is therefore part of sovereignty's historical contingency and development rather than something which is inherent to the state itself. Sovereignty can therefore operate through several different modalities: territory, place, and interactions across space (Agnew, 2009a)

Sovereignty and sovereignty regimes - Conclusion

These four examples represent potential configurations of sovereignty in the modern world and are "ideal types." As Agnew carefully notes, no state can necessarily be a perfect example of each approach, but rather their actions and orientations can be seen in light of the sovereignty regime structure and their general trends towards their sovereignty (Agnew, 2009a). The examples offered have focused on purely conventional territorial understandings of sovereignty, without discussion of if and how these sovereignty regimes manifest themselves with regard to cyberspace and a state's broader relationship to information flows. Other flows, such as capital and immigration, are actively influenced by the sovereignty regimes which they encounter. In the case of globalist sovereignty, capital flows are encouraged the flow freely through a lowering of tariffs and other financial borders. Sovereignty often manifests itself with regards to capital flows as incentives for capital through reduced taxes, tax incentives, cheaper labor, and other variables.

If sovereignty regimes are emergent and process-oriented, they are a reflection of existing policies and practices of the state. To further support this point, Agnew proposes that state currency is a useful method to examine sovereignty regimes. For instance, a classic sovereignty regime emphasizes territorial currency processes (Agnew, 2005), in which a state has a controlled national currency and limited access to other currencies and whose exchange rate and associated policies are centrally controlled by the state. On the other hand, the globalist regime sees a national currency as transnational and influential, traded globally and underpinning other currencies – the U.S. dollar, for example (Agnew, 2005).

Currency processes provide a useful proxy by which sovereignty regimes can be seen empirically. Currency is “a symbolic feature of central state authority” (Agnew, 2005, p. 447) and the historical role of currency in the creation of national identities and its use in the day-to-day functioning of the state allow for it to be a useful measure of infrastructural power. It provides a means through which sovereignty can be seen in its effective operation rather than as a concept, with variances reflecting the diversity of sociopolitical contexts worldwide. Currency processes can be evaluated and mapped as such due to the availability of data which can be easily used for empirical analysis.

For some thinkers, such as Helleiner (1996), currency is where the modern challenges to sovereign state territoriality are most manifest, a perspective which Agnew (2005) implicitly agrees with. While currency may be a useful proxy for understanding sovereignty, territoriality, and sovereignty regimes, information is also emerged as critical to states in the modern information economy. The rise of the "creative class" (Florida, 2002), the importance of global intellectual property and copyright to state economies, "brain drains" as a means through which states lose vital skilled employees**,** and the predominance of the modern digital and information divide as a means through which a state can remain globally competitive highlight the importance of information to states. Historical information networks, such as the letter or telegraph, also enabled information to flow or be restricted, aiding in scientific and economic development (Perkins & Neumayer, 2011), the spread of new social ideas or political unrest (Diamond, 2010; Evgeny Morozov, 2012; Shirky, 2009), while also representing something to be controlled, managed, or restricted to populations or limited to information elites (Diamond & Plattner, 2012; Evgeny Morozov, 2012).

The flow of information, understood as occurring at a measurable level through the Internet, also represents a means through which a modern state can exercise its infrastructural power in relation to its territorial conceptions. The state relationship to information and information flows, through relationships to state despotic power on one axis and infrastructural power on the other can also be mapped to sovereignty regimes. State Internet filtering and controls can be seen within broad geopolitical contexts as part of the varying sovereignty regimes which exist worldwide. Thus, the ability of states to exercise geopolitics and its geographical components on the Internet is the subject of the next chapter.

Chapter 3

Geopolitics of Internet Control

Introduction

In June 2009 millions of Iranians filled the streets of Tehran demanding a recount to the contested presidential election between Mir-Hossein Mousavi and incumbent president Mahmoud Ahamdinejad. These protests were, in part, fueled by the development of a Facebook page, groups, and associated websites in support of opposition candidate Mousavi which called for peaceful and non-violent protests asking “Where is my vote?” (Gheytanchi & Kamalipour, 2010; Sohrabi-Haghighat & Mansouri, 2010). Due to the restrictions placed on international media in Iran, protestors had resorted to uploading videos and distributing news through social media and the Internet, becoming the world’s first “Twitter Revolution” (Grossman, 2009; Keller, 2010; Evgeny Morozov, 2009a) in Western media. Though the hyperbolic claims of Western media and politicians subsequently proved to be exaggerated (Ashraf, 2009; Beilin et al., 2009), the fact remained that the Internet represented a vital and new force in the ways in which states conceived of information.

Prior to the election, the Iranian regime had relaxed restrictions on banned websites by allowing access to Facebook and other social media websites, allegedly in a bid to demonstrate the openness and fairness of the upcoming elections (Esfandiari, 2010). However, after the election results the Iranian government quickly censored and restricted access to huge numbers of domestic and foreign websites which it deemed to be un-Islamic or threatening national stability, while cyberattacks crippled other sites located outside the country (Ashraf, 2011a). Further, the regime throttled and restricted Internet bandwidth (Aryan, Aryan, & Halderman, 2013) which had the effect of stopping users from watching or uploading videos documenting the state's brutal and violent suppression of the protest movement.

The decision of the United States State Department to intervene on behalf of protestors and ask Twitter to delay scheduled maintenance (Grossman, 2009) contributed to the politicization of cyberspace from the perspective of the Iranian government. With global media praising the power of the Internet to unseat dictatorships around the world, the Iranian government tightened its information borders and asserted its sovereign rights over domestic cyberspace through Internet filtering. In effect, at a time of political danger Iran opted for a territorial approach to information which articulated security over the opportunities of the Internet (Diener & Hagen, 2012) by hardening its informational territory.

Through utilizing Internet controls states are able to restrict the flow of information inside and outside of their borders, regardless of political circumstances. In cyberspace, the primary way states assert their geopolitical visions, which are founded on the principles of sovereignty and borders, is through Internet filtering. This is the “information curtain” (MacKinnon, 2011) first articulated by Secretary of State Hillary Clinton.

The purpose of this chapter is to explore the ways in which states articulate the geopolitical ideas of sovereignty, territory, and borders discussed in chapter two in cyberspace through the practice of Internet filtering. This is in support of the dissertation’s first research question which asks: does geopolitics manifest in cyberspace? If so, how? It does so by building upon Elden’s (2010) discussion of the role of technology in facilitating state bordering first by exploring the philosophy of artifactual politics through which a technology can be seen to be political and used for political purposes.

Once the philosophical underpinnings of technologies as political tools is established, the state must then create information as a category to be defended against and managed, in other words information must be territorialized, the subject of the next section. Following this section, the chapter then presents a brief history of the Internet to bring these two philosophical concepts together and demonstrate how the Internet, from its earliest conceptions, was political and designed for elements of territoriality and bordering. Finally, the chapter discusses the means and methods through which the Internet is actually bordered and territorialized. This is supported by empirical evidence supporting the ways in which these methods of territorialization correspond with those sovereignty regimes (Agnew, 2009a) which likewise exhibit high levels of traditional territorialization.

Philosophical foundations: the politics of artifacts

Any study of technology makes assumptions about the nature of technology itself. That is, some philosophical stance is assumed when discussing or theorizing about the nature of technology and its relationship to the human world. Attempting to understand what technology is and how it is situated within human affairs, or even if it can be considered apart from human affairs, is one of the main research agendas of the philosophy of technology.

Technology can be seen as objects separate and disconnected from humans, with its own logic and evolutionary pathways (Kelly, 2011). It can also be viewed as a way of thinking (Ellul & Merton, 1967), rooted in language (Wittgenstein, 2009), as part of the human body (Ihde, 1978; Umiltà et al., 2008), as discrete inanimate objects made by humans (Heidegger, 2003), a system for creating objects (Mumford, 1963), as groups of humans subject to certain rules (Rousseau, 1987a) the ways in which humans experience and see the world (Ihde, 1975, 2003) or as a sociotechnical system constructed and cohabited by humans and technology (Kline, 1985).

These perspectives are illuminating in their ability to challenge the notion that technology is clearly defined or understood. The origins of technology and its broader implications for human society are, however, ignored through perspectives which ponder the nature of what technology *is*. The ancient Greeks saw technology as originating from Prometheus and his gift of fire, that man's ability to control or limit nature through technology was in some ways divine or unexplainable (Demir, 2012). The myth positions the origins of technology in such a distant past as to render critical examination of the origin of technology meaningless, supporting the claim by technological determinists that technology's origins and development are autonomous (Kelly, 2011). Socrates challenges the technological deterministic view of technology as divine or mysterious by arguing against the ancient Egyptian god Theuth, who myth holds as having invented writing (Plato, 2009). He argues that the inventor of a technology has a vested interest in its promulgation and success, and that they are not the best judge of a technology’s worth or use. He further argues that writing will be detrimental to human learning, memory, and wisdom. In other words, Socrates argues in favor of a perspective in which technology's development is held to be socially contingent and its further development, uptake, or use is likewise dependent upon social considerations. Technology has a broader impact on society and on individuals, with consequences which may be undesirable should technology be uncritically adopted or adopted based solely on the self-interest of its inventor.

A portion of Socrates' critique is later adopted in the social constructivist perspective which sees technology as arising through human action alone and subject to human whims and direction (Bijker, Hughes, & Pinch, 2012). In this model technologies arise from developers and users who define and redefine what technologies should exist, what they mean, and how they should be used. Technology is reactive, a response to external needs and pressures which the society and key groups within society address through technological development and adoption. This reactive approach ignores a deeper political impetus which lies behind the invention, adoption, and obsolescence of technology.

Arguing for a politics of technology, Lewis Mumford believed that "...two technologies have recurrently existed side by side: one authoritarian, the other democratic, the first system-centered, immensely powerful, but inherently unstable, the other man-centered, relatively weak, but resourceful and durable" (Mumford, 1964, p. 2). This is an essentialist perspective in which technologies maintain certain political attributes inherent in their structure and design. They lead to inevitable, predictable political outcomes in a deterministic way, as in Marx's *Poverty of Philosophy*: "The hand-mill gives you society with the feudal lord; the steam-mill society with the industrial capitalist" (Marx, 1971, p. 109)

Early cyber-utopians and libertarians continued this line of thinking with beliefs that the Internet was inherently a democratic force (Barlow, 1996). Their position was bolstered by the early technical developers of the Internet who believed that their technology and modes of governance were democratic and libertarian, and often resisted attempts by the United States to assert its legally binding authority over portions of the early Internet (Goldsmith & Wu, 2008). The strength of this position declined significantly during the first decade of the 21st century, only to be revived with the Iranian Green Movement protests of 2009 and Arab Spring of 2011 in which social media technologies were implicated as inherently democratic and which lead to demands for additional political rights (Diamond & Plattner, 2012; Evgeny Morozov, 2012).

This approach is extended by Langdon Winner (1980) who proposed that technologies embody specific politics in two distinct forms: technical arrangements as forms of order, and inherently political technologies. The first is exemplified through the development of the low-hanging overpasses on Long Island (Winner, 1980). These overpasses were specifically designed to limit the presence of buses, which were commonly used by African-Americans, on Jones Beach and other surrounding areas. The architect, Robert Moses, blocked extending the Long Island Railroad from servicing Jones Beach as well.

This is Winner's (1980) example of an explicitly political intention. This need not be the case, as the longstanding development of public infrastructure which neglects and inconveniences handicapped citizens is another example of a technical system which had an explicit politics embedded within it prior to its actual implementation. Unlike the case with Moses where there was an explicit political intent and desired outcome, intent can be irrelevant if the technology is implemented or adopted without due consideration for the kinds of politics and “forms of life” (Winner, 1989; Wittgenstein, 2009) which it engenders. In the case of handicapped access, the exclusion of the handicapped was not an explicit goal, but lack of due consideration or discussion surrounding the rapid and largely unregulated expansion of public access contributed to a political outcome (Winner, 1980).

Winner (1980) argues that these are examples of technical arrangements as forms of order, in which technical systems can have politics *prior* to their intended use. The highway overpasses are not inherently political, but their design, construction, and specific implementation articulated an explicitly political standpoint by Moses. It was designed to produce a certain set of circumstances *before* it had actually been reified. There was a political logic in the explicit design of the system itself, and its intended use thus becomes almost ancillary to its original political intents. With regards to the exclusion of the handicapped, there was no explicit political intent, yet the technological implementation of public access was political in that it produced certain explicit political effects.

These technologies, Winner goes on, are ways in which humans render order in their world. Technology contains within it both the politics and ways of life of the past as well as the ways in which the future world will be constructed. The uptake of technologies influences how people work, partake in political life, relate to each other, and communicate for so long as the technology and its descendants play prominent roles in the life of society and the world. Recent research confirms that historical sites of early development with the telegraph continue this trend in leading in development and adoption of the Internet (Perkins & Neumayer, 2011). Great care must be taken in considering technologies for adoption, emphasizing the ways of life which will be destroyed, altered, or emerge from this technology's introduction. Technologies can therefore bear intended or unintended politics; despite their seemingly “neutral” appearance as tool and the actors which implement or have decision making powers over implementation can create explicit politics. Power actors realize or reify power through the implementation of technical systems of order and their associated technologies.

In the second approach, Winner (1980) argues that certain technologies are inherently political and linked to power, in contrast with his first position whereby power resided in actors and the technologies they adopt or influence. This perspective is evident in the early philosophy of Friedrich Engels who believed that certain technologies necessitated the development of specific social and political power hierarchies: "The automatic machinery of a big factory is much more despotic than the small capitalists who employ workers ever have been" (Engels, 1978, p. 731).

The focus is on the specific technology or technical system as having properties which are inherently political. The example used is that of the atomic bomb, whose danger and power render it something which must be treated in an explicitly political way, with clearly demarcated hierarchies and structure akin to authoritarianism (Winner, 1980, 1989). There could never be a "democratic" way to deal with nuclear weapons directly – its sheer power makes it an inherently political technology.   A technology, however, may be political but may not necessarily drive strongly towards Mumford's (1964) authoritarian or democratic mold, but instead have certain *tendencies* towards politics. Winner argues that solar power, for example, is something relatively uncomplicated and cheap which makes the technology itself more democratic than nuclear technology. Solar power could be adopted and used in an authoritarian setting, yet this is not a *requirement* per se as opposed to the way nuclear weapons are handled.

Alfred Chandler (1993) extended this argument through an analysis of the social patterns which emerged from the railroad and other industrial developments of the 19th century. He believed that these technologies and sociotechnical systems required specific social hierarchies and power associations again due to their specific technical requirements. A railroad cannot be a democracy, otherwise it would cease to function as a railroad, in other words. Winner (1980) believes that oil production and other extractive industries must likewise operate on similar principles which condition or necessitate certain social patterns and distributions of power associated with the broader social and political effects of the technology's adoption and uptake.

Winner's philosophy of artifactual politics posits two broad points: some technologies are flexible enough that their political implications arise from the actors who decide where and how to implement them, and some technologies can only be implemented or adopted in a way which necessitates an explicit political order. The previous examples demonstrate how a flexible system, such as highway overpasses, can be made to be explicitly political and how nuclear weapons necessitate a hierarchical power structure.

The principle of artifactual politics provides a framework for understanding the geopolitics of technologies. It demonstrates that technologies have political and social implications, which can influence the geographies in which they develop and are implemented in. The idea for low highway overpasses, for instance, was not conceived of in a lower-income predominantly African-American neighborhood. This technological decision had both a geography out of which it arose and a political geography which it subsequently created. Nuclear weapons created new understandings of national sovereignty and national vulnerability, with implications for borders and geopolitical visions, such as the Dew Line as a technological border to protect the United States yet located in the Canadian Arctic (Farish, 2010).

The Internet cannot be seen apart from its artifactual politics: both those of technical systems of order and those inherent to it. The decision to award Department of Defense grants to study packet-switching to allow information to be routed around nuclear catastrophe (Aksoy & DeNardis, 2007) and develop a system which would unify the country informationally is explicitly political and grounds the technology of the Internet in a way conducive towards government control. Understanding its artifactual politics, as Winner demonstrates, also involves understanding the historical development which immediately preceded the deployment of the technology.

Understanding artifactual politics also entails understanding the contexts in which those artifacts exist and function. Since the United States issued its *Green Paper* to assert control over all aspects of the Internet's architecture (Goldsmith & Wu, 2008; Mueller, 2004) states have politicized the Internet to ever-increasing degrees. Indeed, for states such as Saudi Arabia and Iran the Internet's introduction was delayed for the explicit purpose of inserting state censorship and control from the outset. Further, it becomes difficult to isolate the Internet's development from broader Cold War ideologies, and that these political ideologies of openness and connectivity continue to influence the development of the Internet – seen in the continued funding of "Internet freedom" projects by the United States government.

Within the context of international state behaviors and actions, therefore, the Internet becomes a politicized technical system of order whose fundamental architecture at virtually all levels is political. Indeed, this is seen empirically even at the level of technical protocols and Internet governance (DeNardis, 2009; Mueller, 2013) where we see explicit state action to colonize, demarcate, and control all aspects of the global information communications infrastructure.

Notably, the existence of mesh networks during the Arab Spring, for example, and alternative localized Internets precludes this broad categorization of the Internet as political through and through. These examples have largely emerged during specific political moments to serve specific political purposes, and to date alternative activist or oppositional Internets have not gained mainstream traction. Thus, for the purposes of this dissertation and keeping within its broad political context, the Internet should be considered thoroughly politicized.

Within this dissertation, Langdon Winner’s framework for artifactual politics will be used. Winner’s framework provides for categorizing technical objects into two broad categories, technical arrangements as forms of order or inherently politicized technologies. Within this framework a non-politicized object would be one whose presence would then be a technical arrangement as a form of order.

There would be numerous philosophical challenges to asserting the nature of objects in such a broad way. However, Winner does not seek to blindly assert that all things fall into two camps. Indeed, Winner argues that it is the contextual use of technologies which also influences the ways in which they can be categorized. He uses the example of a ship at sea, which may require a captain and thus necessitate a certain politics, but when docked no longer requires that specific political configuration. Therefore, objects within this dissertation should be seen as inhabiting both categories within the political context which frames this dissertation, but may have significantly altered politics in different contexts.

This section has articulated a philosophical interpretation of a relationship between technology and politics. This interpretation will guide the remainder of the dissertation. However, the Internet is a conduit for the flow of information, and for a geopolitics of cyberspace to exist information must exist as an entity which can be measured and demarcated in the same way in which the state encountered the idea of calculative space (Elden, 2007) and applied that idea to physical territory. The following section discusses information and territoriality in the creation of information.

Information and Territoriality (Creation of Information)

The discipline of academic geography is no stranger to the idea of politicized information. From its early conceptions as an aid to state colonization and militarization projects (Barnes & Farish, 2006) to recent incarnations in the Bowman Expeditions in Oaxaca, Mexico (Bryan, 2010), geography has attempted to classify and articulate specific types of knowledge, transforming them into useful and actionable intelligence items for the state.

However, the idea of information as discrete units of knowledge traces its history to the European documentation trends of the late 19th and early 20th centuries (Day, 2008). The birth of information science, under the "father of information science" Paul Otlet (1868-1944) contributed to the sense that the book was an "informational object" which existed not only by virtue of what was explicitly contained within it, but also in what the book itself symbolized as a cultural object. That is, the book "stands for facts, documents, physical books, and knowledge as information...and in turn, each of these signifiers refers back to the culture of the book" (Day, 2008, p. 10).

Otlet incorporates biological concepts in a "bibliographical organicism" (Day, 2008, p.

13) which enmeshes the book, as symbolic of information itself, within broader natural flows and trends of knowledge in human history and society. For Otlet, books have sociohistorical contexts, and can be connected to each other spatiotemporally through networks of knowledge and information which can be mapped genealogically through the books as physical objects. The idea of a discrete unit of information embedded within a network or web of spatiotemporally-contingent information becomes a founding principle of information science and the way in which states and public institutions categorized, related to, retrieved, and organized knowledge itself.

Information as a discrete unit finds its most famous and influential articulation in the aftermath of the Second World War and within global ideological struggle of the early Cold War. The limitation of books as informational objects resided in their explicit physicality: they required significant space to store and time to index. The development of nascent computing during the Second World War had its philosophical underpinnings in the logic articulated by Otlet – these computers were treated as electronic filing cabinets (Warner, 2012). The significant migration from physical books to electronic filing cabinets did not go unnoticed – its logic influenced two key thinkers at this time: Warren Weaver and Norbert Wiener (Day, 2008).

Wiener's development of cybernetic theory and Weaver's *Mathematical Theory of Communication* atomized communication into discrete elements which could be transferred between parties and through neutral mediums with the need for irrelevant “noise” to be filtered out . In this, noise represented a form of statistical uncertainty such that information became a variable within a quantified model of communications, arguably the first attempt to essentialize communication into discrete units of information (Day, 2008)**.** As Day states “The task of information theory and cybernetics to prescribe social space by the theory of information or communication aims towards representing beings, language, and communication in terms of operational relations" (2008, p. 46). In other words, communication could be reduced into discrete elements and operationalized. This, as discussed earlier, serves as the logical underpinning for packet-switching networks.

By the 1960s the idea of information as a discrete component of communications and as something which stood apart from communications and could be isolated was firmly established (Day, 2008). Information was a construct developed in response to specific needs by the state for knowledge and its development into discrete units reflected changes in the ways in which states began to relate to information storage and retrieval after the advent of computers. Information challenges or supports sovereignty and territoriality and represents a vital state interest. Thus, the combination of artifactual politics and the creation of information are seen to merge in the development of the Internet, explicitly created for the purpose of development and maintenance of an informationally-aware and dependent state during the Cold War. The following section will briefly discuss the history of the Internet so as to bring these two earlier sections into clear relief before examining how information on the Internet can become territorialized through filtering and control.

A brief history of the Internet

The creation of the telegraph, or the "Victorian Internet" (Standage, 1998), significantly altered the relationship between the state, space, and information. States began to regard information and the transmission of information in more geographic terms, demonstrated in the strict ways in which the British managed the deployment of telegraph lines across Persia to link their Indian holdings with Europe (P. M. Sykes, 1906).

The telegraph, and subsequent telephone system, contained within them certain technical features which became increasingly problematic as information flows increased substantially following the First and Second World Wars. At the same time, the expansion of information flows and its importance in issues of national security and military operations and communications was highlighted with the development of nuclear weapons and the long-range bombers which could deliver them. A nuclear strike could decapitate leadership but strikes elsewhere could also informationally isolate military units and disrupt national order or morale, leading to a situation which could make the defense of the United States untenable. However, the logic of the telegraph and telephone concentrated informational power and transmission at key nodes and locations, such that the elimination of Chicago, for instance, could devastate communications between Washington D.C. and Los Angeles.

Under the telephone network, a dedicated physical path is established between a person and the person they are calling – for the duration of the call no one else can use that line. Since the establishment of a dedicated line for each human being is not feasible, the telephone network uses “circuit switching”. Each phone call is routed to a switch and from this switch an incoming call is routed from the outgoing line to the end recipient. In the early and mid-20th century this was done manually via a switchboard operator, popularized in TV and cinema. With the advent of computer technologies in the mid to late 20th century, human switchboard operators were replaced and circuit switching performed by computers. The major structural limitation of this system was the reliance on centralized switches and static routes. In the event of a serious military confrontation, this would leave areas of the United States unable to communicate with the rest of the country (Aksoy & DeNardis, 2007).

The geographical implications of circuit switching are immediately evident. The reliance on a switching station in order to communicate represents a single point of failure. This fragility in the nature of the telephone network prompted a push from the U.S. government to discover alternatives to circuit switching. In response, the Rand Corporation developed “packet switching” as part of the push for nuclear-survivable communications (Aksoy & DeNardis, 2007).

One of the limitations of circuit switching was its reliance on physical infrastructure to facilitate the flow of information. This reliance ensured the quality of information connectivity, but could also be severely problematic for information flows because it made informational flows dependent on hard physical assets and rigid pathways. RAND's packet switching did not involve one particular centralized route and switching station. Instead, their researchers focused on the idea of segmenting information itself into discrete units and delivering units of information which could be reassembled at their destination (Aksoy & DeNardis, 2007).

Once information was segmented into discrete units, called packets, it could then be more efficiently routed across multiple data lines and reassembled at its end destination. Packet switching requires no dedicated end line which means that single lines can be used for multiple purposes. Each packet of information is sent from a user's computer to a router which reads each packet's end destination. The router then automatically determines the optimal path for information to travel. The information packet is then sent to another router which determines the next optimal route and so on until the packet reaches its destination. Once all the packets of information reach their destination, the packets are reassembled in the correct sequence - an epistemological shift towards the quantifying of information itself.

Packet switching's decentralized nature is its main advantage over circuit switching. A line is only used so long as it is transmitting a packet, instantly freeing up the line for other uses after the packet has been transmitted.   Since no dedicated route to the destination is required, packets are free to utilize any route available. This means that communications can continue on surviving nodes if other nodes are destroyed or incapable of operating.

The invention of packet switching allowed the United States to develop the Advanced Research Projects Agency Network (ARPANET) in the late 1960s (Roberts, Larochelle, Faris, & Palfrey, 2011).   This network initially linked large American universities together as rapid investment and development of the ARPANET continued. Its initial deployment and subsequent expansion was a success, leading to an increasingly complex network architecture which presented problems for managing researchers and military personnel which used the same network.

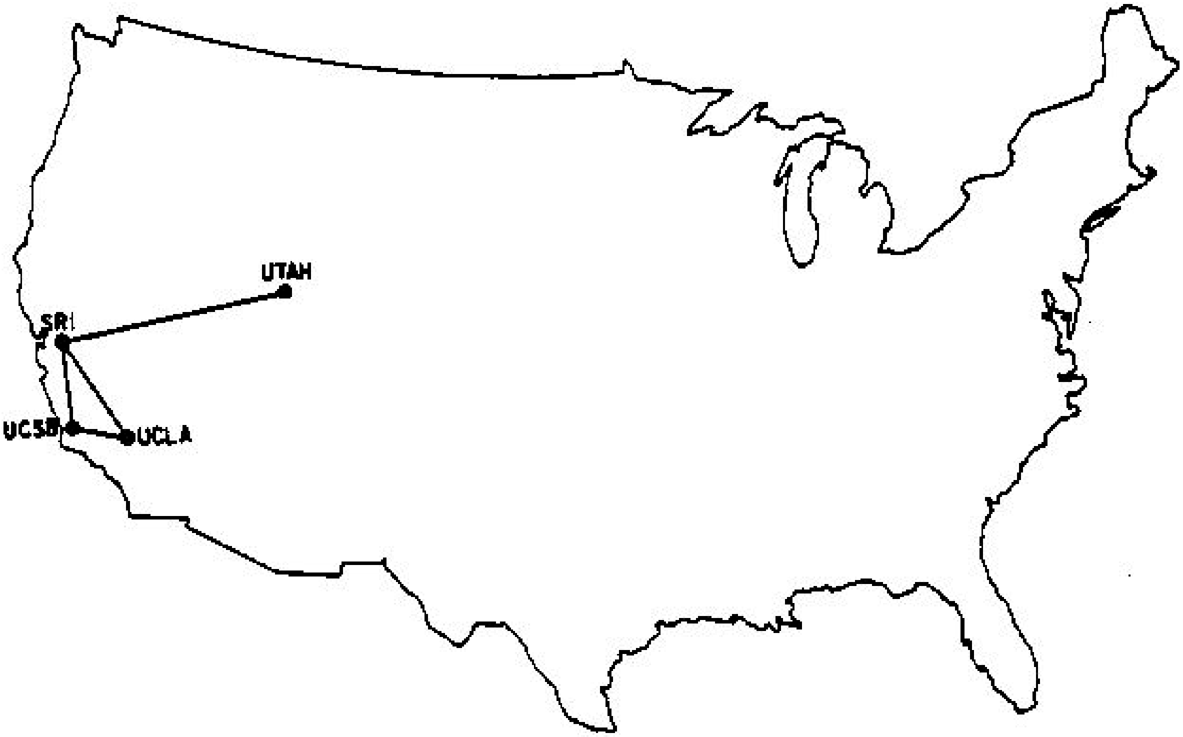


Fig. 7 – ARPANet in December 1969 (Bolt Beranek and Newman Inc., 1981, pp. III–77)

In response, the decision was made to migrate to the modern Internet's "network of networks" approach through developing autonomous systems. Autonomous systems include Internet Service Providers (ISPs), universities, or corporations which assign addresses and route traffic (Roberts et al., 2011). These are networks which communicate with other networks to create the essential structural foundation of the Internet. They also serve as the key points over which the state is able to exert direct control over wired Internet traffic. These systems determine Internet traffic flows between machines and to other autonomous systems using the border gateway protocol (BGP) to broadcast data-transit criteria to other autonomous systems.

Autonomous systems route traffic to the first available autonomous system on the shortest path. For example, the shortest hierarchical distance to transmit information from computer A inside autonomous system #1 to computer B in autonomous system #4 is through autonomous systems #3 and #2. This approach to routing information is a historical byproduct of a split in the early Internet between military (MILNET) and civilian (ARPANET) networks on the grounds that ARPANET lacked military-grade security (Roberts et al. 2011). Thereafter, should a computer in ARPANET need to communicate with one in MILNET, it need only understand how to transmit data to a MILNET gateway which would then route the traffic within the MILNET network.

The logic of autonomous systems lends itself to state control and surveillance. The above example of transmitting information from computer A to B is also the same path that a state would need to intercept or control to exert effective political control over the Internet within their effective jurisdictions. The early split of MILNET and ARPANET and the development of autonomous systems and BGP were political decisions necessitated by the need for different levels of controls over different networks (Roberts et al., 2011).

The legacy of control and surveillance facilitated by the autonomous systems and BGP routing structure is not something alien to the system; rather it is the foundation upon which the system was built. Thus, in the history of the Internet two themes can be identified: the technical system of order represented by autonomous systems and the inherent politics of packet switching. Each of these themes represents ways in which the Internet itself has an artifactual politics. For the technical system of order, autonomous systems represent a specific way in which humans must organize and relate to the Internet as a whole. The Internet was not designed to be a global cohesive medium, but rather a medium of discrete, separate networks which could communicate with one another. The development of autonomous systems enabled, prior to its implementation, a political logic which facilitated Internet filtering and control along national territorial boundaries.

Packet-switching, on the other hand, represents a particular approach to information which is inherently political within the context of telecommunications. Information, in the form of a packet, is the central artifact around which states articulate and craft their policies related to Internet filtering or openness. Echoing Winner, within this technical context, packet-switching is inherently political as it cannot be related to in any other way other than as an object whose creation, flow, and management are subject to explicitly political decisions. Packet-switching is inherently political because “There are no alternative physical designs or arrangements that would make a significant difference; there are, furthermore, no genuine possibilities for creative intervention by different social systems--capitalist or socialist--that could change the intractability of the entity or significantly alter the quality of its political effects” (Winner, 1980, p. 134). Attempting to renegotiate the way information is quantified would in no way alter the political relationship to packet-switching by states through Internet control. It is recognized as explicitly political because, while the logic of packet-switching could have minor alterations in its technical structure, it would still manage quantified information and function within existing territorial logics associated with spatializing information. However packet-switching would be dressed up or altered, its political function would not change.

Both autonomous systems and packet-switching demonstrate the artifactual politics at the heart of the Internet itself. In autonomous systems we see a political logic developed before its implementation which seeks to segment information along discrete and controllable networks which can communicate with each other. At the heart of the Internet's structural network logic is a political vision as to how information flows should be organized and controlled. That information, in the form of packets, is the focal point for the whole enterprise: how to create, quantify, deliver, and reassemble information becomes subject to broader political visions which are facilitated by the political structure of segmentation present in autonomous systems.

In both elements of political artifactualization the decision was made around the immediate needs of the United States military, supported by Department of Defense-funded researchers (Roberts et al., 2011). The quantification and packetization of information occurs as a means to address potentially fatal flaws in information flow and control in the event of a nuclear disaster.

It is worthwhile to note that after the split of MILNET and ARPANET, the state was largely absent from the Internet’s development and from cyberspace more broadly. Despite increasing attention in the media through popular films such as WarGames, little was done on a technical level for states to assert control or dominance in cyberspace. Control of key aspects of the Internet’s technical infrastructure remained with the academic communities which had been instrumental in the Internet’s early development.

This period of state aloofness to cyberspace came to an end within the United States in 1998 when the “Green Paper” was issued by the U.S. government essentially asserting its total effective control over the Internet’s root nameservers (Mueller, 2004). This explicit assertion of control, after over a decade of relative disinterest, was prompted by Jon Postel, one of the Internet’s technical pioneers. Postel was in charge of the Internet’s root nameservers, translating IP addresses such as 1.2.3.4 into UCLA.EDU and thus making them human-readable. However, as the Internet grew in importance and size, the U.S. government had slowly been migrating some of these nameservers away from Postel. These transfers had been done in a consensual and non-formal way, reflecting the loose power arrangements which had run the Internet for over a decade.

However, Postel had become concerned that the Internet's founders would be sidelined in the future, and sought to assert their authority through unilaterally revoking those transfers (Goldsmith & Wu, 2008). This was immediately noticed by U.S. national security authorities who considered pursuing legal action against Postel as a result of his attempt to transfer the root. The incident was resolved when Postel agreed to the demands of the United States, leading to a new era in direct state involvement and assertion in cyberspace.

Understanding Internet Filtering

The Internet's development, and its subsequent balkanization and ideological confrontation over closed and open, cannot be seen apart from the political circumstances which led to its creation and foundation during the Cold War. State adoption and implementation of the Internet must engage with the explicit political questions arising from its technical foundations.

This technical configuration, highlighting both the need for informational survivability and contiguity and the need to segment and control, migrate the Internet away from its normalization as a neutral backdrop for world communications and into a system which requires a political response and structure by states. This is not to say that the Internet at present is without borders, but that from a technical standpoint the computers which comprise the Internet recognize connections coming from any geographical location. Thus, this is a representation of the Internet rather than necessarily the reality. The attempt to normalize what later became the

Internet as open and free thus reflects an explicitly political choice by states which has transformed into a broader geopolitics of cyberspace.

The Internet is a domain through which the state can act or be acted upon politically, and thus the state approaches this domain through a geopolitical lens. This lens is grounded in the historic possession of land as property by the state**,** and also influences the way states approach other domains of action, such as the sea and the air (Butler, 2001; Graham, 2004; Kaplan, 2006; Mahan, 1987; Oxman, 2006; Williams, 2011). This territorial approach, in its modern conception, derives from the early encounter between the state and calculative space (Elden, 2010) though the development of the idea of territory itself was subject to significant historical development throughout Western history (Agnew, 2010).

Internet filtering is a condition where a state censors the information flowing into and within the cyberspace under its sovereign control (Deibert & Villeneuve, 2004). Geographically, information flows occur from the broader Internet into the state, from the state outwards to the Internet, and within the territorial state itself. State practice has evolved since the advent of the Internet to address the geographies of information flows through filtering, which leverages legal and social instruments and technical means to bound information in cyberspace.

The idea of controlling and regulating information flows is not a new one. States, societies, and human groups have long had a vested interest in the content and types of information which flow within their boundaries and cultures. For example, traditional oral aboriginal societies separate information by gender, with “women's knowledge” and “men's knowledge” (Bhathal, 2006) which are not to be spoken in the presence of the opposite gender. For Aristotle in Ancient Greece political space was a space where certain types of information was discussed and others were suppressed (Curry, 1999). The invention of the national census brought with it an idea that some information should be collected and categorized by and for the state (Curry, 1999, 2005). There are innumerable examples of the ways in which states and societies have regulated or demonstrated interest in the information they generate, consume, and spread. Thus, there has long been a geography of information which has manifested itself in demarcating information along the lines of historically-contingent cultural views on space and time.

These ancient traditions are often appealed to by states in constructing their filtering systems and enacting laws or other regulations to enforce a particular geopolitical vision of information. This targets specific content and information flows selected by the state for varying reasons, inevitably linked to some idea of how the nation, its culture, and its values are constructed. In China, the state with the world's largest level of Internet filtering, Internet censorship is termed “harmonization” because it is believed that disruptive (predominantly) foreign information influences can result in a society which has lost its harmonious nature and create significant social problems for the Chinese people (Wang, Juffermans, & Du, 2012).

Iran grounds Internet censorship within the state's interpretation of Islam, going so far as to label its censored Internet as “halal” or acceptable for consumption by Muslims (Aryan et al., 2013; Rhoads, Fassihi, & Gonzalez, 2011) despite the fact that websites associated with prominent and respected Shia clerics, such as Ali Montazeri, were routinely censored because of political views which the state disagreed with (Rahimi, 2007) . In Thailand the state routinely removes or filters sites which denigrate or ridicule King Bhumibol Adulyadej, in line with his important role in Thai society and its lèse-majesté laws (Evgeny Morozov, 2009c) which criminalize disrespect to the King. Other states censor pornographic content in defense of popular morals, some filter information related to politically sensitive disasters or during times of public unrest, and many liberal democracies filter content related to nationalism, gambling, or types of pornography (Deibert, Palfrey, Rohozinski, & Zittrain, 2008; Deibert, Palfrey, Rohozinski, Zittrain, & Haraszti, 2010). State Internet filtering, therefore, is an umbrella term which makes no claim against content, but rather represents a geopolitical vision states apply to cyberspace.

Filtering begins through a determination of the forms of content which should be filtered. The above brief examples above show that there are not uniform informational categories which states censor content around the world. For instance, gambling is not universally censored nor is pornography. Rather, information is classified and then controlled through technical and activity regulations as a vehicle towards establishing a geopolitics of cyberspace. According to the Open Net Initiative, a collaborative research group formed by the University of Toronto and Harvard University, censored content can be classified into political, conflict/security, social, and Internet tools (Deibert et al., 2008, 2010).

Political content is content which explicitly focuses on political topics, often with views in opposition to or critical of the sitting regime (Deibert et al., 2008, 2010). This can be diaspora opinion (Shichor, 2010), domestic political dissent, satire, or even academic research. The definition of political is, of course, not uniform as different states vary in what they consider political. For example, in Iran the idea of women's health and women in general is not only a social issue, but an explicitly political one due to the theocratic nature of the state and its theological interpretations through which religion and politics are co-mingled. For some time the word “women” was itself blocked by Iran's Internet filter (Sreberny & Khiabany, 2010). In China, discussions about environmental health can often be a veiled critique of the state and fall under political content categorization. What these categories share in common, and what makes them political for filtering purposes, is the presence of some critique of the political status quo.

Conflict/security content is in many ways an extension of the political, though with several important distinctions. This content category is specifically focused on existing domestic or foreign conflicts, separatist struggles, militants, terrorism, or other topics related to cyber or kinetic violence against the state (Deibert et al., 2008, 2010). This category, in other words, brings the political into the ideological and physical. Within China, websites associated with Uyghur independence or resistance are routinely attacked and blocked (Shichor, 2010). In Pakistan, websites associated with independence for Balochi or Pashtun peoples are routinely blocked as well as legislation drafted to block other websites associated with threats to Pakistan's internal physical security (Faris & Villeneuve, 2008).

The third category, social content, is concerned with drugs, alcohol, taboo social topics, human sexuality, gender, gambling, racism, bullying, and health (Deibert et al., 2008, 2010). Filtering based on social content often forms the initial impulse towards filtering, after which it is extended to include non-social topics, usually political. Some countries, such as Singapore, focus their filtering efforts almost exclusively on social categories (Deibert et al., 2008). Saudi Arabia has developed what is believed to be the world's most sophisticated pornography filter (Deibert et al., 2008) which it purports to filter in the name of upholding public morals. In western liberal democracies, we see social filtering with regards to child pornography and online gambling (Deibert et al., 2008, 2010) as well as selective political filtering during times of unrest such as the Occupy Movement. Nationalism and racism also serve as the foundation for social content filtering in countries like France and Germany which prohibit access to purchasing Nazi memorabilia or items online (Frydman & Rorive, 2012).

The final category, Internet tools, is natively digital (R. Rogers, 2010, 2013) as it is content about email hosting, domain name registration, filtering circumvention, anonymity software, and other natively digital products. This content purports to provide alternative communications tools and services outside what is sanctioned by the state. Further, this content often explicitly demonstrates how to circumvent censorship or provide tools to do so. For example, in China Google's caching system for viewing archived pages is blocked as it is a method which can circumvent traditional Internet filtering (Deibert, 2009; Zittrain & Edelman, 2003). Anti-censorship tools such as Tor or Psiphon have their websites and services blocked in Iran (Aryan et al., 2013) making censorship circumvention a cat and mouse game. UltraSurf and Freegate are popular circumvention programs used in China which are also blocked, and their developers targeted with physical threats and intimidation (Beiser, 2010).

These four categories are not rigidly demarcated nor should they be understood as such. As the case with Iran and women's issues demonstrates, what is social in one state can be considered political or both in another. These categories are, however, a method to separate and segment general trends amongst content which states filter, evidenced by substantive empirical research conducted by the Open Net Initiative. They provide a general template through which a state's attitude towards its cyberspace can be discerned, and a means by which scope and depth (Warf, 2011) of filtering can be determined. For example, Singapore has touted the sophistication of its filtering system yet only devotes significant energy towards filtering pornography (Deibert et al., 2008). Singapore can therefore be seen in a different light vis-a-vis filtering when compared to Iran, with a highly sophisticated filtering system whose scope and depth is substantive in all four categories.

Content classification forms the first part of implementing filtering. States have tendencies to classify information along these lines and then make judgments as to which categories will be emphasized for filtering. An important caveat to this is the availability of commercially-produced censorship systems such as Fortinet, Blue Coat, and Websense, developed by private corporations in the United States and Europe. These systems are sold to states such as Tunisia, Syria, Burma, and Yemen (Marquis-Boire, Dalek, & McKune, 2013) and the companies provide maintenance and support for the product. These western companies maintain centralized or recommended block lists of websites through their own investigations on behalf of their clients. These block lists are pushed to state clients who often accept them and implement the recommended filtering without examining the contents (Wagner, 2012). In Burma, 98.9% of the sites on Blue Coat's blocked sites list were filtered by the military junta and similar results were found in Syria, even after the start of its civil war (Markoff, 2013; University of Toronto, 2011)

Both states and commercial vendors classify content for the purposes of filtering it. After content classification, either done domestically, from an outsourced censor such as Blue Coat in California, or from some combination of the two, the state must then implement filtering. Filtering rarely exists apart from a legal and social infrastructure which normalizes filtering as something congruent with society and the state as a whole.

Where and how do states filter?

The rise of state Internet controls and Internet filtering has led many scholars and critics to assert that the modern state has found renewed vigor and life online (Deibert, 2009; Goldsmith & Wu, 2008; Villeneuve, 2006). The libertarian and utopian visions which surrounded the birth of cyberspace have given way to a colder realism whereby cyberspace is a prototypical global public sphere (Papacharissi, 2002) or global cyber commons (Choucri, 2012) becoming increasingly balkanized and segmented geopolitically. Censorship implementation and circumvention are industries worth billions of dollars in a global struggle to define the dominant communications medium of the 21st century.

The right to control information flows is a function of state sovereignty in its most traditional territorial sense (Goldsmith & Wu, 2008). Goldsmith and Wu (2008) argue that states sovereignty in cyberspace exists through two regulatory models: technical and activity regulation. Technical regulations are the technological protocols and methods used to block or restrict flows of information within the territorial state. States assert their right to a sovereign informational space through their ability to allocate and control the technical resources which give that space its existence. Activity regulations are the legal instruments and social norms or practices which provide the state with a normative framework through which it can moderate and control flows of information. Activity regulation provides the legal, social, and cultural rationale for the existence of technical regulation. In other words, the real or perceived values of the nation inform how that nation is to be constructed in cyberspace.

Activity regulations

Filtering regimes are preceded by the establishment of legal frameworks which restrict certain content or activities online. These regulations are often extensions of pre-existing restrictions on freedom of speech or other media controls rather than Internet-specific laws. Zittrain and Palfrey (2007) argue that these Internet content regulations take the form of five categories: content restrictions, licensing requirements, liability, registration requirements, and self-monitoring requirements.

Content restrictions are laws which forbid citizens from developing, consuming, or distributing certain types of content. Licensing requirements make filtering on behalf of the state a requirement for obtaining a license to be an Internet service provider (ISP), run a cyber cafe, or provide mobile Internet to smartphones and other devices. Liability is the imposition of penalties on ISPs and other Internet providers who are not filtering content effectively or efficiently in lieu of licensing requirements. Registration requirements mandate that users must register or provide information about themselves before obtaining home Internet access, domain names, web hosting, mobile data, or to use cyber cafes. Finally, self-monitoring is a form of self-censorship echoing Foucault's panopticon (Foucault & Sheridan, 2012) whereby the user, company, ISP, or other user or provider censors themselves or the content and Internet access they provide without prompting or intervention by the state. This often is accompanied by a general level of surveillance and monitoring by the state which facilitates self-monitoring and surveillance as a social norm.

In addition, other means of enforcing filtering can be employed against Internet access or users themselves. Content may be filtered through physical attacks, threats, or intimidation by security forces on publishers or reporters, cyber attacks against websites, hijacking of domain names or content delivery systems, or government threats against ISPs, infrastructure providers, or other who provide data (Deibert et al., 2008, 2010; Evgeny Morozov, 2012). Further, contracts may be awarded to individuals or organizations which agree to comply with government “suggestions”, states can engineer corporate takeovers of critical communications infrastructure, or further outsource censorship to upstream data providers who will do so on their behalf. Very few states are transparent about how and why they block content, with few releasing the content which is specifically blocked, and thus the full extent of the power mechanisms which underlie filtering may never be fully known.

As with content classification, these legal categories of filtering are not necessarily demarcated clearly nor is their existence mutually exclusive. A state may implement some or all of these categories in their own interpretation of how best to protect and create informational sovereignty. In Iran, ISPs must obtain licenses , web hosting and mobile data plans require home addresses and personal registration, and cyber cafes must also register users while being under the threat of liability or licensing requirements (Zittrain & Palfrey, 2007). In China, the state includes its content restrictions in domestic copyright laws (Zittrain & Palfrey, 2007), creating a sheen of legitimacy and the appearance of working with international copyright norms while regulating content domestically. Further, content restrictions may not only be aimed at an individual user, a university or other organization may be held liable by a state for facilitating objectionable activities online as evidenced by the numerous copyright lawsuits filed by the Recording Industry Association of America (RIAA) against U.S. university students.

Despite its often decentralized or federal appearance, Internet filtering decision making and deployment is heavily centralized with serious penalties or sanctions for ISPs which unreasonably delay implementation. Activity regulations can be therefore seen as part of the overall sense of how filtering occurs, with technical implementation dependent upon activity regulation and vice-versa. That is, without technical regulation the activity regulations are meaningless for Internet filtering, despite the presence of self-monitoring and social norms against sharing or consuming forbidden types of content.

Technical regulation

Technical regulations are the technical ways in which states actualize filtering. Filtering can exist as a rhetorical concept, as with Singapore, or as an openly acknowledged reality of cyberspace, such as with Saudi Arabia's open discussion of the importance of Internet censorship. Filtering can also exist as a set of activity regulations in the forms of laws, social norms, and soft power used to monitor and control information online. It is ultimately technical regulation which brings these concepts together and reifies the specific claims of the state about cyberspace and information within its geographical extent.

Technical regulation, and the technical specifics of Internet filtering are expansive and vast. Each method represents a philosophical perspective on the relationship between information, technology, individuals, and the state. That is, technologies do not exist in isolation from their broader social and political contexts, and Internet filtering technologies and techniques are likewise embedded within the broader society. Thus, the methods of filtering may appear to be objective and neutral but each method reflects an attitude towards how the geopolitics of cyberspace ought to be constructed.

The technical means of filtering influence both the concepts of scope and depth in filtering (Warf, 2011). Scope limits the extent of topics filtered while depth addresses the level of structural informational filtering. The specific technologies used to filter and erect information borders serve as the foundations for the circumvention tools utilized by activists and information-seekers. What information is available is a function of both activity regulations and technical regulations rather than an absolute which exists atop both. However, in order to bound filtering activity regulations must first issue or determine which resources are to be filtered.

Filtering methods and techniques

Technical filtering can be grouped into four broad categories (Murdoch & Anderson, 2008): in-line, DNS/domain tampering, denial of service, and national cyberzones. These categories exclude the ability of the state to completely disconnect from the Internet, as Burma, Syria, Libya, and Egypt have done during political crises (Howard, Agarwal, & Hussain, 2011; Villeneuve & Crete-Nishihata, 2012). Further, it presupposes that citizens can access the Internet, something illegal within North Korea (Hachigian, 2002). Each category approaches filtering from a different perspective and each has unique structural advantages and disadvantages. For example, in moments of political crisis the easiest method to intimidate and control information flows can be to attempt a denial of service attack either conventionally or through identifying weaknesses in an offending server/website and bringing it down. This is a rapid, brutal method for immediately disabling a site, unless the opposition has anticipated this and located itself within systems or networks which are specifically designed to resist denial of service attacks or hack attempts.

In-line filtering is itself comprised of two methods: proxy filtering and TCP/IP filtering. Proxy filtering seeks to insert another server between the user and the Internet. Users access this server which retrieves content on behalf of the user. Doing so allows the proxy server to cache content, increasing performance and speed for the end user while allowing administrators to have detailed abilities to block specific assets rather than entire domains (Murdoch & Anderson, 2008). This approach limits the user's ability to connect directly to the Internet, ensuring that virtually all content is localized within the territorial state.

TCP/IP filtering is the most commonly known method of Internet filtering. Data packets are inspected for specific attributes (IP address, Domain name, service port number, etc.) and this is checked against a defined block list, usually provided by the state. This level of analysis can occur at a router level or require a deeper level of inspection. Filtering at the router level will examine just the header, equivalent to the address on an envelope, of the information packet and block or allow that packet to continue to its destination. Examining the content of the data packet, equivalent to opening the envelope and reading its contents, requires more sophisticated technologies, called Deep Packet Inspection (DPI).

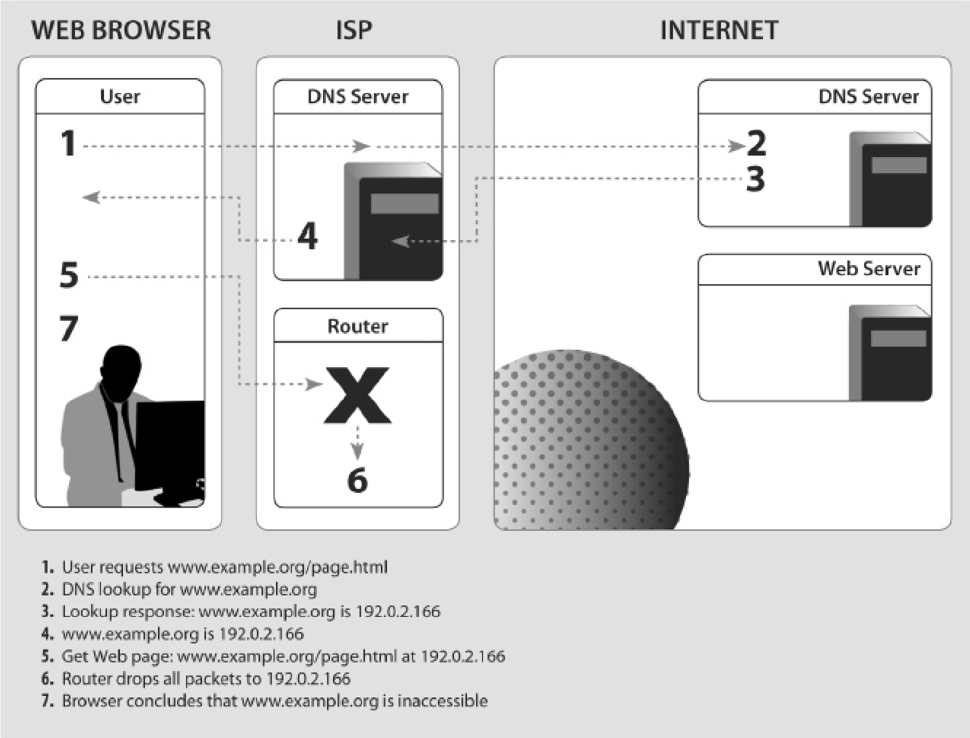

WEB BROWSER
ISP
INTERNET
User
DNS Server
DNS Server
Web Server
Router
1
2
3
4
5
6
7
1. User requests www.example.org/page.html
2. DNS lookup for www.example.org
3. Lookup response: www.example.org is 192.0.2.166
4. www.example.org is 192.0.2.166
5. Get Web page: www.example.org/page.html at 192.0.2.166
6. Router drops all packets to 192.0.2.166
7. Browser concludes that www.example.org is inaccessible

Fig. 8 – IP based blocking (Deibert & Rohozinski, 2010a, p. 60)

In the DPI method of TCP/IP filtering, the data packets are checked not only at the header level, but the actual content of the packet is checked for prohibited content, search queries, words, or other information. These are then checked against another list automatically via algorithm, to determine whether the packet should continue to its destination or be dropped or blocked. Depending on the sophistication of the algorithm, the censor can capture or monitor a tremendous amount of information at a highly granular level. This system can be used to not only identify content, but to address specific signatures and patterns in encrypted communications and block those packets, as evidenced by the repeated blocking of the Tor circumvention and anonymity tool in Iran (Aryan et al., 2013). What is critical about this system is that packets are examined in real-time (Bendrath & Mueller, 2011) and it allows for essentially total surveillance of the non-encrypted information flows through a network. States are implementing DPI as part of their standard filtering practices, facilitating unprecedented informational awareness and collection and the ability to filter content only limited by the sophistication of their algorithms (Bendrath & Mueller, 2011).

Most websites and online content are accessed using domain names, such as Google.com or UCLA.edu. However, these domain names are actually human-readable translations of Internet Protocol (IP) addresses such as 74.125.224.174 for Google.com and 128.97.27.37 for UCLA.edu. In order to effectively translate the human readable domain names into machine readable IP addresses, users must access their ISP's DNS server when requesting a website. This process is normally invisible to the user, but within a filtering regime the ISP's DNS server is fed with a list of specifically domain names which should be blocked. When a user attempts to access a website in a filtering regime with DNS tampering, they will be unable to see the page.

Domain modifications and tampering are the counterpart to DNS tampering. DNS tampering works to block a user within a national filtering regime from accessing specific content. However, users outside of the territorial filtering regime are still able to access that content. If, for example, a website located in the Sudan is reporting on atrocities within the Sudan, then users in the home country would be unable to access the content, but media such as CNN or the BBC would still be able to do so. Domain modifications involve removing the DNS entry for the domain name from the national DNS servers which outside users access in order to retrieve a domain. Thus, in doing so, the state effectively removes the site from the broader global Internet, though it may still be available to users who know the IP address.

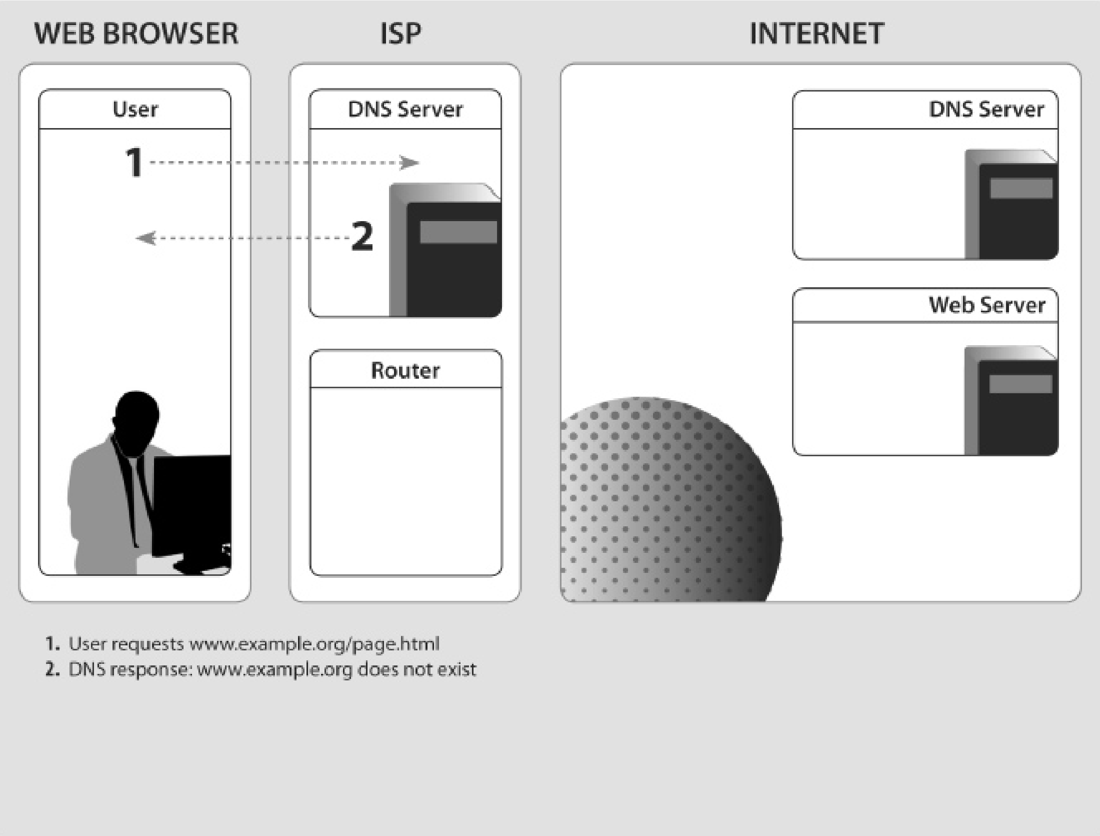

WEB BROWSER
ISP
INTERNET
User
DNS Server
DNS Server
1
2
Web Server
Router
1. User requests www.example.org/page.html
2. DNS response: www.example.org does not exist

Fig. 9 – DNS Tampering (Deibert & Rohozinski, 2010a, p. 61)

The final category, denial of service, involves a range of actions which states undertake to filter both domestically and internationally. The previous two categories, in-line filtering and DNS/domain tampering, are passive filtering methods. Centralized censors determine the content, categories, and concepts to be restricted, and then translate this into domain names, algorithms, and IP addresses which servers should automatically block. Denial of service methods, however, are explicitly offensive actions by the state against content to facilitate its complete removal from the domestic and international Internet. It includes distributed denial of service (DDoS) attacks, hacking, surveillance, and content takedown. The central logic of the denial of service category is that it uses violence and infiltration to remove or alter undesirable content, regardless of where it is located geographically. If content hosted in the United States was deemed sufficiently objectionable by Iran that in-line filtering or DNS/domain tampering was insufficient, then Iran would employ denial of service to remove the content.

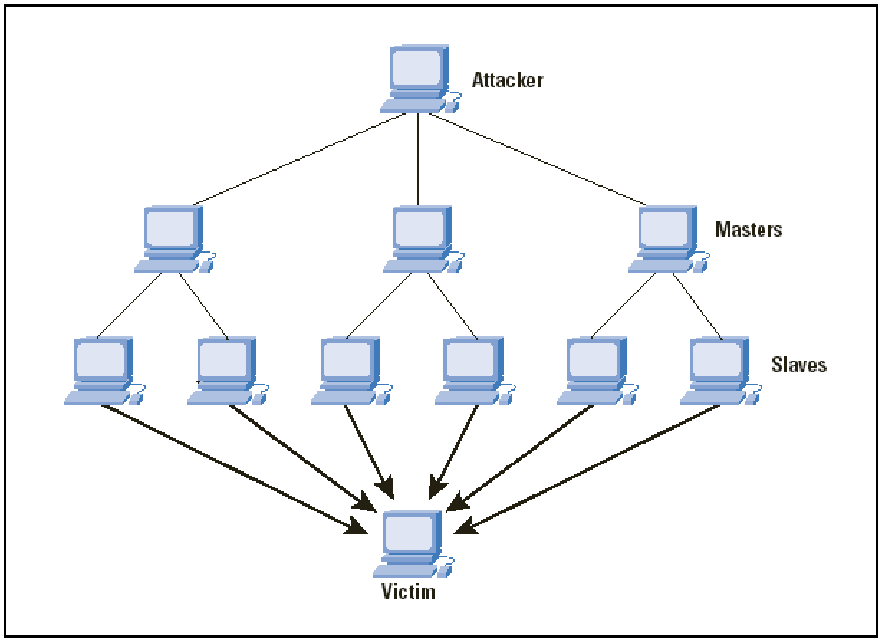


Fig. 10 –Distributed Denial of Service Attack (Patrikakis, Masikos, & Zouraraki, 2004, p. 20)

The DDoS attack dates from 1989 (Liska, 2014), and the earliest mass-produced tools developed in the late 1990s (Douligeris & Mitrokotsa, 2004). It is among the oldest and most cost-effective methods for disabling websites and remains a common tool utilized by both state and non-state actors (DeLuca, 2013). While there is tremendous diversity to DDoS attacks, its essential technical logic involves making multiple, rapid requests to a website to overwhelm the webserver and make it unable to serve content. Its effectiveness comes from the ability to scale to tens of thousands of attacking computers dependent upon a command and control infrastructure of “bots” and “bot herders”. Its distributed nature involves utilizing botnets, which are networks of individual "bots" or computers infected by malware, and which can be controlled by a central "bot herder" to attack websites. Botnets can range from a few dozen computers to over 5 million (Porras, Saidi, & Yegneswaran, 2007). These botnets are often acquired by cybercriminals and rented out on a black market to state, non-state actors, and criminal organizations to pursue their individualized objectives. States with low levels of Internet infrastructure, such as North Korea, often use external criminal botnets as a means to achieve both political objectives and to maintain plausible deniability (Nazario, 2009).

Hacking is another broad category of denial of service filtering which encompasses traditional hacking, defacement, and social engineering. These approaches attempt to directly compromise a server or content host in such a way as to remove, deface, or alter content or domain names. Hacking involves gaining access to systems protected by passwords or other measures. Gaining access can include exploiting vulnerabilities in server configurations, infecting users with malware and capturing passwords, physical intimidation of administrators to retrieve passwords, and impersonating users to gain access to systems among other methods. Once access has been gained, the attacker can remove content, deface existing content with messages, or alter content to reflect the attacker's politics. This approach removes or alters content at its source and in such a way to constitute a form of violence in cyberspace (J. Thomas, 2001), be considered an act of cyberwar, as well as to psychologically destabilize and demoralize content producers and the views they support (Bendrath, Eriksson, & Giacomello, 2007).

Surveillance is unique in that it does not constitute a direct method through which content is actively filtered or removed. It constitutes social, political, legal, and technical means to observe, collect, and classify information from the general populace and other targets which the state is interested in. These targets need not be located within the territorial state, as Chinese digital spying on the Uighur diaspora (Shichor, 2010) or Vietnamese malware surveillance of dissidents demonstrates (Cullum, 2010; Thayer, 2014). In-line filtering, especially through DPI, aids in surveillance as all aspects of data packets can be examined and then routed for storage and further investigation. Surveillance supports filtering because it acts as a digital panopticon (Foucault & Sheridan, 2012) whereby users are uncertain if they are being observed or monitored, and thus practice self-censorship of content (Deibert, 2003; Deibert & Rohozinski, 2010b) for fear of punishment or other sanction. Thus, surveillance as a filtering method must be supported by social or legal consequences otherwise it lacks ability to facilitate filtering. Within authoritarian states, digital surveillance alongside sophisticated filtering mechanisms is a highly effective method to filter as it both filters content and moves citizens towards self-censorship.

Content takedowns are a relatively new method of filtering which reflects the explosion of user-generated content known as Web 2.0. In this method, states and citizen sympathizers or paid actors "flag" or report objectionable content to content providers in the hopes of having the offending content removed and the uploader banned. If, for example, a protest video were uploaded to video sharing site YouTube, a content takedown would see state-affiliated actors register accounts and report the video to YouTube so that it would be removed automatically. This method takes advantage of corporate policies towards removing content and the algorithms which automatically remove content to target very specific content rather than filter or block popular websites such as YouTube.

Finally, the creation of national cyberzones (Deibert et al., 2010) marks a distinctly and explicitly territorial approach to information flows and Internet controls. This approach, seeks to develop an internal or “national Internet” whereby users can only access information located within their territorial borders by disconnecting from the broader Internet and relying on an exclusively domestic one. International connections still exist, but are restricted to elites or those with other forms of government approval. North Korea's Kwangmyong network is the oldest example of a national cyberzone where users can only access websites and resources located within North Korea and approved by state information ministries (Warf, 2015). Cuba and Myanmar have also implemented similar systems which ground the Internet in strict and literal territorial terms. In 2007, Russia first proposed the idea of a Cyrillic Internet which would be separate from the global Internet and focused on states which use the Cyrillic alphabet (Deibert & Rohozinski, 2010a). The most well-known example is Iran's recently proposed “Halal Internet” which would conform to its own theological interpretations of the Koran as applied to cyberspace, while being disconnected from the Internet at large (Aryan et al., 2013; Rhoads et al., 2011).

These methods of Internet filtering represent ways in which states create and implement geopolitical visions in cyberspace. The technical regulations reify abstract notions of restricted and permissible information through in-line filtering, DNS/domain tampering, denials of service, content takedowns, and national cyberzones. The state's territorial borders find analogous counterparts in cyberspace through the twin roles of activity and technical regulations. How a state envisions its territory and the broader geopolitical world which it inhabits is reflected by how it articulates its sovereignty in cyberspace and how it relates to global information flows.

The protocols which power the Internet allow it to have these varying properties. The Internet, as a global medium, is therefore both open and filtered and malleable given the flexibility inherent in its underlying protocols. This is an example of the “integral accident”, a concept argued by the philosopher of technology Paul Virilio (2007), in which technologies embody not only desired attributes but less desired ones as well. For example, to Virilio (2007) a train crash would not necessarily constitute a failure or error, but rather would be one of the things which trains can do. Thus, Internet filtering technologies contain within them the means by which they can circumvented or rendered functionally ineffective.   In the same way that software is developed to facilitate filtering, so too has software been developed which facilitates openness and filtering circumvention. The following section briefly discusses these technologies as technological counterpoints to filtering regimes.

Internet filtering circumvention

Internet filtering circumvention is the technical means and tools used to neutralize Internet filtering and reach the unfiltered, broader Internet. These tools are used by individuals and groups within states which practice Internet filtering in order to access information or protect their anonymity. These tools can also be used in states with Internet surveillance, like many liberal democracies (Greenwald, 2014) as a means to protect privacy and anonymity on the Internet. There are four categories of circumvention tool: proxies, VPN/tunneling, onion routing, and a final “catch-all” category (Callanan, Dries-Ziekenheiner, Escudero-Pascual, & Guerra, 2010; Maitland, Thomas, & Tchouakeu, 2012). States that promote an open Internet have provided substantive funding for many of these methods, though some are developed by hobbyists or activists in specific national diasporas (Evgeny Morozov, 2012).

Proxies ask users to connect to another computer which visits the site on the user's behalf. The computer which is accessed is geographically located within a jurisdiction where the content desired is not censored. Proxies may or may not have their data encrypted, possibly exposing users to Internet surveillance. A related category of circumvention, VPN/tunneling operates along a similar logic as proxies, with the main exception being that connections provide an encrypted “tunnel”. Users can therefore safely connect to computers in geographically different states through which they can safely and securely surf the Internet.

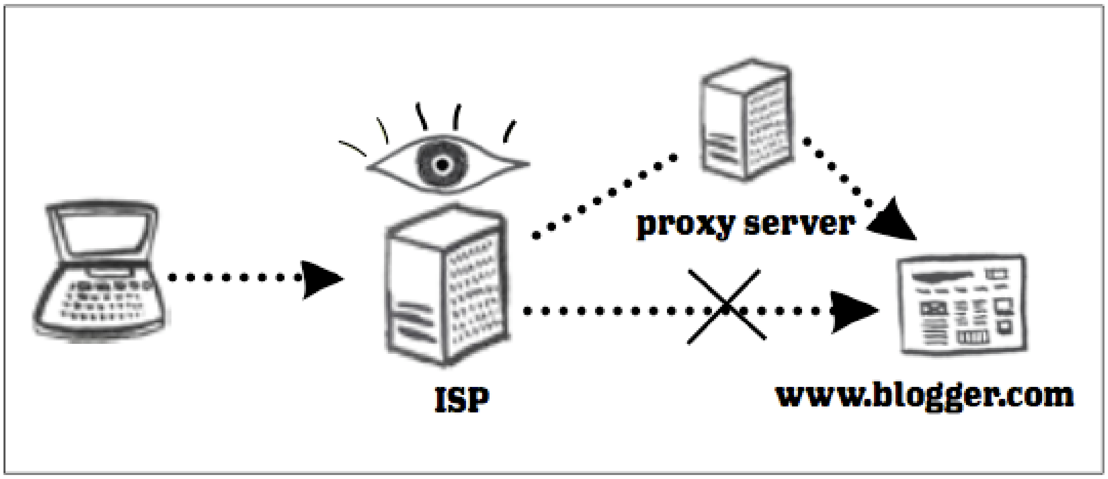


Fig. 11 – Proxy Server (Security-in-a-Box, 2012)

Onion routing is a method of tunneling with notable technological exceptions. Historically, it was developed as a project by the United States Navy, with support from the Defense Advanced Research Projects Agency (DARPA) to provide a method where information could be accessed and transmitted securely. The project was eventually opened to the public and development continued by the Tor Foundation. Onion routing operates by encrypting traffic with specific keys, and then routing the users request across three or more servers, each of which is randomly selected and does not know where the previous computer was located. In doing so traffic is anonymized and secured to such an extent that the U.S. National Security Agency considers onion routing to be "the King of high secure, low latency Internet anonymity" (Plak, 2014).

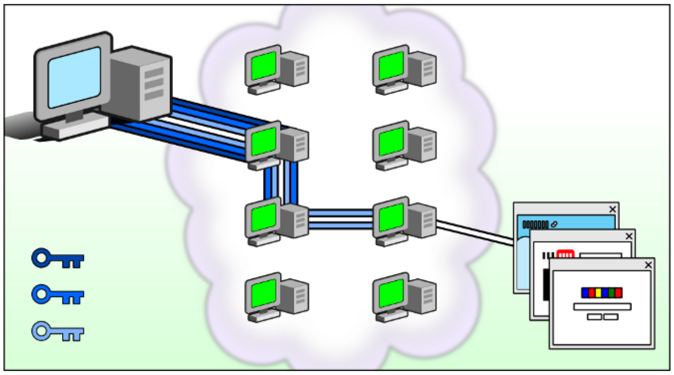


Fig. 12 – Onion Routing (Reporters Without Borders, 2013)

The final category of circumvention is a “catch-all” category and focuses on specific content exploits which individuals can use to circumvent filtering. This can include using Google Cache to return uncensored webpages (Leberknight, Chiang, Poor, & Wong, 2010), using RSS feeds to bypass censorship (Leberknight et al., 2010), using metaphors for filtered words (G. King, Pan, & Roberts, 2013; Qiang, 2011), or using email lists to retrieve content. This method takes advantages of technical oversights or errors in the implementation of filtering, ultimately transforming it into a game of “cat and mouse” between users and censors.

Circumvention technologies and methods are technical counterpoints to filtering technologies. Due to state involvement in their development, they also are technological embodiments of political perspectives for the geopolitics of cyberspace. Their development is inherently political, with an aim towards altering or challenging the cyberspace of another sovereign state. Circumvention tools work against multiple levels of filtering technologies and have developed increasing levels of sophistication alongside increasing sophistication of filtering.

Classifying Internet Filtering

Classificatory schemes allow for broad trends and patterns to be identified within certain political activities. Classification schemes can also represent a power perspective and be prescriptive rather than descriptive. However, the activity and technical regulations of the preceding sections have more in common than their broader roles as means through which filtering is implemented. The specific technical and activity regulations which compose filtering are not selected by states at random, but can be grouped and ordered with certain commonalities and approaches within these groupings. Democratic states, for instance, may choose to implement legal structures and DNS/domain tampering to protect copyrighted content, as in numerous Digital Millennium Copyright Act cases in the United States (Urban & Quilter, 2006). More authoritarian states may choose to implement traditional filtering alongside heavy surveillance and denial of service practices.

Filtering, both activity and technical regulation, has evolved and developed throughout the Internet's history and alongside political developments within countries. The earliest filtering regimes dealt with the Internet from a different sociotechnical context than states where the Internet had broader and more substantive penetration. Saudi Arabia's decision to allow the Internet only when it had developed effective filtering mechanisms demonstrates how a state supporting a closed Internet might have dealt with the Internet at its outset (Deibert et al., 2008). This is juxtaposed with a state like Iran which has wrestled with the Internet and implemented a variety of overlapping filtering mechanisms since its rapid uptake by urban citizens. To clarify patterns and trends in Internet filtering and their association with politics, Deibert and Rohozinski (2010a) proposes three broad generations.

The first generation of filtering encompasses in-line and DNS/domain tampering, as well as physical policing of cybercafes. These are reactive controls implemented early in a state's encounter with the Internet and most often associated with explicitly traditional authoritarian states. The second generation of Internet filtering expands upon the previous generation by including substantive activity regulations as well as incorporating denial of service as an explicit methodology for filtering. In this generation the state invests significantly in establishing or building upon social and legal norms regarding activities in cyberspace. The sheen of legal legitimacy aids the state in more aggressively pursuing online infractions, and is present not only in authoritarian states, but in flawed democracies and authoritarian regimes with democratic elements ("hybrid regimes"). These terms ("flawed democracies, etc.) originate from the Economist Intelligence Unit and are used by Deibert (2010a) to describe how various states rank in various elements of democratic governance. Finally, the third generation includes surveillance, national cyberzones, and other direct actions against information domestically and located abroad. This generation is often present in flawed democracies or hybrid regimes.

First Generation		Second Generation				Third Generation			
Internet Filtering	Policing Cybercafés	Legal Environment for Information Control	Information Removal Requests	Technical Shutdowns	Computer Network Attack	Warrantless Surveillance	National Cyberzones	State-Sponsored Information Campaigns	Direct Action

Fig. 13 – Generations of Internet Filtering (Adapted from Deibert & Rohozinski, 2010a)

These generations are grouped around similar themes: first generation controls seek to deny access through direct blocking; second generation controls seek legal controls and enhanced technologies to create normative filtering environments with plausible deniability and the sheen of legitimacy; and third generation controls emphasize the militarization of cyberspace (Deibert, 2003). The importance of these generations is in its utility to frame the controls states adopt in relation to their specific political construction. For example, many authoritarian states tend to adopt all three generations, whereas states with greater democratic elements emphasize second and third generation controls (Deibert & Rohozinski, 2010a). Thus, the examination of state Internet filtering regimes moves from technical and activity specifics towards the geopolitical development of cyberspace itself.

The libertarian idealism of the early Internet, which saw it a borderless digital world where ideas could be shared freely and anonymously (Barlow, 1996) has largely faded. Vestiges of these ideals remain in the West, however, in the form of mass movements against regulations such as ACTA or CISPA which sought to more directly affirm elements of filtering and surveillance in the pursuit of copyright and intellectual property protections. Regardless, research has shown that most countries offer some form of Internet censorship or surveillance (Reporters Without Borders, 2014), contributing to a balkanizing Internet arranged largely around territorial states. This serves as the underpinning of a binary view of an open and closed Internet, and with western states morally obligated to pursue an open Internet in the name of human rights worldwide. The United States, for example, has allocated more than $50 million (Glanz & Markoff, 2011) per year since the 2009 Iranian Green Movement protests inspired greater global action against Internet filtering.

States which practice filtering, however, argue that their sovereignty is being actively violated by other states which fund, develop, and deploy software designed to circumvent their Internet filtering. They believe that a state has a right to develop and control cyberspace in the same way as it controls territorial borders, continuing a longstanding trend towards a more volumetric geopolitics (Elden, 2013a). This is recourse to the traditional notion of the inviolability of territorial sovereignty, whereby a state, as representative of the nation, has the right to non-interference by other states within its boundaries. This is a founding principle of the international system, but a concept seemingly under pressure from the forces of globalization, migration, international law, and cyberspace. State sovereignty in cyberspace is, therefore, a domain in which notions of borders, sovereignty, and geopolitics are being redefined.

State territory is made and remade, and this includes the expansion of state territory to include the Internet. This expansion utilizes geographical and other techniques through technical and activity regulation to expand territory to the Internet itself. As part of Elden's broader argument, sovereignty and territory are de-linked and its linkage demonstrated as only a relatively recent idea and practice (Elden, 2009). Thus, a state may both engage with the Internet as territory as well as through the sovereignty regimes in which it is enrolled.

If the modern balkanized Internet reflects an Internet cut through with territory, then the structure of Internet filtering should in some way resemble the territory of states. This would be evidenced through ascertaining whether or not state political structure, ostensibly the way in which a state conceives of territory, borders, and sovereignty, reflects levels of Internet filtering. An authoritarian state embodying a traditional, classical sovereignty regime, should therefore seek to demarcate its Internet territory in a way which reflects the specific generation of Internet controls which are associated with strict and clear demarcation. A globalist sovereignty regime would, instead, rely on alternative means to engage with the Internet, through controls on copyright and intellectual property rather than explicit controls on information in ways which maintain or enhance a hegemonic position. Thus, the next section will demonstrate, through several empirical studies, the link between state government type and state Internet controls and in doing so demonstrate that states take an explicitly territorial view of cyberspace as a domain in which their varying sovereignty regimes can be realized. There is, in other words, a clear geopolitics to cyberspace.

State Political Configuration and Internet Filtering: Empirical Results

The state relationship to the Internet is a function of how it deploys infrastructural and despotic power. Forms of Internet controls should theoretically vary alongside different state sovereignty regimes, associated with state political configuration (Agnew, 2009a). The implication of this is that Internet freedom is less an absolute and fundamental aspect of the Internet and more a function of state infrastructural and despotic power configurations demonstrated through the concept of sovereignty regimes.

Research on Internet filtering is relatively new, and there are significant difficulties in acquiring data. Although crowd-sourced models for measuring Internet filtering do exist (Hwang, 2007), these are hampered by the inability to verify sources and biased towards individuals who are aware the Internet is filtered in the first place. Further, very few states openly discuss their filtering programs or regimes, resulting in direct in-country research being the only reliable method to determine the scope of global Internet filtering.

Researchers face two main challenges: test platform acquisition and spatiotemporal variance in filtering regimes. Test platform acquisition problems arise because researchers must have access to computers inside the country for a specific period of time and be able to run tests and access the Internet from those computers. This can present ethical concerns as to how these computers are acquired and how they are used. In some states, such as Iran, servers must be registered via ID cards to citizens of the country. Unauthorized access, especially from overseas, can be a political problem for the owner of the server or computer with serious repercussions.

The computers selected must be representative of the general filtering which occurs in the state, as regional and local geographic variations exist in filtering (Wright, 2012). Internet filtering also varies with time, as demonstrated with Iran's loosened Internet restrictions prior to the 2009 presidential elections and severely curtailed Internet access after the election. Researchers must therefore gather geographically disparate data which is also gathered at random times.

Academic research on Internet filtering in particular is sparse, with few studies and most research occurring at the Citizen Lab at the University of Toronto or with private organizations such as Reporters Without Borders (2014). Given this dearth of research, at the Citizen Lab, Deibert's analysis of Internet controls in the former Soviet Union (Deibert & Rohozinski, 2010a) is an influential one and has shown that first generation controls occur most often in states which are more overtly authoritarian. Second and third generation controls occur in states which are more democratic while first generation controls never appeared in those more democratic states. Additional research by Deibert (2009) has shown similar results in that states considered “Not

Free" by Freedom House (2013) tend to block a higher percentage of global and domestic websites.

Warf's (2011) survey of global Internet censorship merges statistical analysis with censorship research from Reporters Without Borders. He determines that there are three stages to Internet filtering, closely connected to state political configuration. The first stage corresponds with authoritarian regimes, and involves "brute force" blocking techniques as well as the development of national Internets, roughly corresponding with first generation controls under Deibert. As domestic Internet usage and development increases in sophistication, so do additional Internet controls according to Warf (2011). This second stage includes advanced filtering, and a more curated approach to the global Internet, in line with Deibert's second generation. Finally, the third stage involves legal and social norms as a means to police and control information similar to Deibert's third generation. Similar to Deibert's results, Warf demonstrates that political freedom is a salient variable for Internet adoption and Internet filtering in general. Again, the trend of increased filtering being associated with more authoritarian states and classic sovereignty regimes is evident. More democratic states and those associated with integrative or globalist sovereignty regimes tend towards having little or no overt political Internet filtering yet have social and legal norms established to control or filter specified types of content deemed economically detrimental, such as copyright violations.

Research by the Open Net Initiative (ONI) (Deibert et al., 2008; Deibert, Palfrey, Rohozinski, & Zittrain, 2011; Deibert et al., 2010), a partnership between Harvard University's Berkman Center, the Citizen Lab, and the SecDev group, echoes the results from Deibert (2009) and Warf (2011) whereby authoritarian states are associated with more explicit levels of Internet filtering and more democratic states are not. Freedom House's annual Freedom on the Net reports (2013) and Reporters Without Borders' annual Enemy of the Internet awards (2014) have also shown that authoritarian regimes tend towards greater levels of filtering whereas more democratic states have different implementations of Internet controls.

The empirical research demonstrates a strong connection between state Internet filtering implementation and state political configuration, which itself is associated with certain dominant sovereignty regimes as a function of infrastructural and despotic power. There is a clear geopolitics to cyberspace, grounded in the ways in which states enact their dominant sovereignty regimes in cyberspace through Internet filtering and associated controls. The strong narrative amongst the Internet's founders of an inherent attribute of openness to the Internet is demonstrated to be a possible political function of Internet technologies. Echoing Winner (Winner, 1980), then, the Internet appears as a fully political technology whose implementations reflects the dominant sovereignty regimes of states.

Authoritarian or less democratic states exhibit higher levels of infrastructural and despotic power, more closely aligning themselves with the classic sovereignty regime, which closely mirrors the conventional notion of strictly bounded state territory and absolute sovereignty (Agnew, 2009a). These states have tended to approach the Internet in a similar way, viewing it as territorially bounded and subject to the absolute sovereignty of the state, demonstrated through practice and rhetoric in states like China, Iran, and Russia (Aryan et al., 2013; Ashraf, 2011a; Deibert & Rohozinski, 2010a; MacKinnon, 2011). The geopolitical vision which the leadership in these states possess becomes articulated both in physical territory and the invention of informational territory as well. In the same way that space was increasingly subject to calculative reasoning and technical measurement (Elden, 2007), so too has knowledge become quantified information and then itself subject to calculative reasoning and technical measurement and regulation (Day, 2008).

Globalist and integrative sovereignty regimes, on the other hand, vary based on central state authority and state territoriality (Agnew, 2009a). Integrative sovereignty regimes, such as those within the states of the European Union, emphasizes weaker central state authority (infrastructural power) but more consolidated state territoriality (despotic power). Globalist states, such as the United States, have stronger state authority and a more open sense of state territoriality (Agnew, 2009a). The integrative sovereignty regime, though, has some complications associated with its open sense of territoriality within its borders (as in the European Union) but a strongly bounded sense of territoriality in the sense of the EU Common Agricultural Policy (Agnew, 2005, 2009a). The more circumscribed Internet available in many European countries, for instance through the restrictions of hate speech (Goldsmith & Wu, 2008), seems to reflect more strongly the sense of a consolidated territory. On the other hand, the globalist sovereignty regime, often associated with the United States (Agnew, 2009a), reverses the integrative model with a more open sense of territoriality and stronger central state authority. The globalist regime, like the integrative regime, is associated with fewer Internet controls and the complete lack of first generation controls.

What emerges is an ideological vision of the Internet, divided along the lines of open and closed, closely mirroring the ideological geopolitical divisions of the Cold War (Tsui, 2008**.** Cold War thinking pervades research on Internet filtering, demonstrated by Freedom House's (2013) categorization of Internet filtering into three categories: Free, Partially Free, and Not

Free. This is an echo of ideological geopolitics between the first, second, and third worlds respectively. Indeed, this mode of thinking has been demonstrated to exist in public pronouncements from global political figures and notably present in the confrontation over Internet governance at the United Nations' International Telecommunications Union (ITU) (Pfanner, 2012).

As the empirical data suggests, both "sides" of the information curtain in actuality are envisioning an Internet which aligns with their specific sovereignty regimes and political attitudes. An open Internet, for instance, furthers the economic and political aims of the United States by allowing for its well-entrenched and existing digital services to be extended into new markets while at the same time serving surveillance objectives (Greenwald, 2014). A closed Internet likewise furthers the political and economic goals of states who wish to maintain control over information or protect their nascent Internet economies (MacKinnon, 2011).

Although the present geopolitical situation is open to interpretation (Agnew, 2003), there nonetheless remains echoes of ideological geopolitics in cyberspace, demonstrated empirically by researchers and in-line with associated sovereignty regimes. Regardless of attempts to move past ideological geopolitics, a version of it remains firmly entrenched in cyberspace as control over information and intellectual property over the Internet becomes an increasingly valuable economic and political advantage.

States enroll the Internet within their own existing geopolitical visions and conceptions, transforming a territorial entity into an informationalized one, and bounding information by territorial concepts. These concepts reflect the state's existing attitudes towards territory and sovereignty, re-cast in activity and technical regulations. These methods of informationalizing territorial concepts were discussed in the first section of this chapter, and illustrate the varying ways in which the territorial ideas of security and opportunity (Gottmann, 1973) are converted into the state's informationalized territory. The multiple ways in which states approach the Internet through territorial practices and concepts are supported by the state's political configuration, financial expenditures, technical and activity regulations, and public political rhetoric through which the state performatively articulates how it territorializes information and how that acts as the spatial extent of sovereignty (Elden, 2009).

Political rhetoric and funding from the United States and European Union has emphasized an “Information Curtain” (MacKinnon, 2011) between liberal democratic states with an open Internet and authoritarian or semi-authoritarian states with a closed Internet. This rhetoric is grounded in a binary ideological geopolitics reminiscent of the Cold War, and through an appeal to popular geopolitics in the form of using territorial analogues (“open” and “closed”) to describe the global Internet (Tsui, 2008). A specific popular geopolitics of cyberspace is portrayed, through speeches, rankings (Freedom House, 2013; Reporters Without Borders, 2014), and special reports. Further, millions of dollars of funding from the United States and European Union is devoted to engaging with the geopolitics of cyberspace in a bid to aid in “Internet freedom” in countries such as Iran, Cuba, and China (Beiser, 2010; Glanz & Markoff, 2011). Funding for Internet freedom projects ranges from institutional programs, such as Harvard University's Herdict, to micro-grants for individual developers who have innovative approaches to Internet censorship (Embassy of the United States, London, 2013).

On the other hand, states which seek to enact Internet filtering pursue internal development on enhancing filtering practices and software, including large-scale rollouts as national cyberzones such as Iran’s Halal Internet or China's failed Green Dam project (Deibert, 2013). These states also purchase advanced filtering software from Western companies (Deibert et al., 2008, 2010; Marquis-Boire et al., 2013; University of Toronto, 2011) and adapt them to local contexts and use. In these states, political rhetoric and popular geopolitics describe an Internet which represents threats to national unity (Deibert & Rohozinski, 2010b), traditional values (Cohen, 1997), or as a means through which foreign powers can exert influence or destabilize domestic politics (Kalathil, 2003).

Appeals to territorial sovereignty and historical national values, as with Iran, China, and Russia (Ashraf, 2011a; Deibert et al., 2010; Deibert & Rohozinski, 2010a), seek to ground the geopolitics of cyberspace within existing territorial norms and portray Western Internet Freedom attitudes as hypocritically grounded in the idea that some states are more sovereign than others. These perspectives contest the idea that the Internet is open by default, and portray it as an extension of a state's existing sovereign communications infrastructure. The historical role of the United States in the development of the Internet, its remaining influence over Internet governance, and the explicit politicization of the Internet by the U.S. following the Iran Green Movement protests have played into the popular geopolitics of states which seek to maintain Internet filtering.

State Internet controls are not distributed randomly - they are strongly linked with the political configuration of states. The reality of Internet controls is less binary and oppositional and more reflecting a continuum with some liberal democratic states practicing degrees of Internet filtering and some authoritarian or semi-authoritarian states allowing open Internet access.

Conclusion

This chapter has demonstrated the existence of a geopolitics of cyberspace. Popular and political rhetoric has long sought to normalize the Internet as open and without geopolitics (Goldsmith & Wu, 2008). This began in the earliest pronouncements by Internet pioneers, and the Internet's technical founders, and continued with political positioning by liberal democracies. To challenge this, the chapter demonstrated the technological, philosophical, and political manifestations of Internet filtering and openness – supported by the empirical research in the field. In doing so it shows that the existence of a geopolitics to cyberspace which is, in many ways, an extension of the ideological geopolitics of the Cold War of open and closed territorial logics in digital terms.

It has done so by at first demonstrating that technologies are not neutral, rather that they embody certain artifactual politics and thus have vary aspects and degrees of politics with which they are associated. Thus, states acknowledge these artifactual politics when they deploy certain technologies in specific ways to support their political and territorial ambitions. This logic, of the state encounter with artifactual politics, is similar to the state encounter with calculative space (Elden, 2010) which was mediated by technological instruments associated with surveying and cartography (Sahlins, 1991).

The Internet as technology is conduit for information as flow. Thus, the state must approach the Internet through a lens of artifactual politics but information through developing a model by which it can be quantified and territorialized. The next section of this chapter dealt with the history of information as a quantifiable and measurable concept. This idea of quantified information, combined with artifactual politics, leads to a section on the history of the Internet –

which demonstrated how the development of the Internet was informed and infused by both logics mediated by the state itself.

The philosophical and historical background established frees the idea of geopolitics in cyberspace from the early cyber-libertarian rhetoric associated with a boundless and borderless Internet. In turn, this allows for substantive engagement with the mechanisms and methods through which the geopolitics of cyberspace is established: Internet filtering and control. This section demonstrated the ways states can control or manage information either through technical or activity regulation. Technical regulations are the technical ways in which the Internet can be either opened or controlled and activity regulations are the social and legal methods through which control is also effected. Together, these types of regulations form a state's vision for its domestic cyberspace within the broader Internet. The purpose of this was to illustrate that the Internet is not inherently technologically open, and that it is technologically, legally, and socially possible for it to be closed and restricted. Demonstrating this allows for specific sovereignty regimes to be associated with information policies enacted through both activity and technical regulations. Finally, through the empirical studies cited this chapter demonstrated how modes of sovereignty and visions of state territory are closely connected with the ways in which states filter and control their Internet.

The purpose of this chapter was to answer the research question does geopolitics manifest in cyberspace? If so, how? It has done so by demonstrating the philosophical, historical, technical, and empirical means through which a geopolitics is established and how states articulate the idea of territory in cyberspace. This is an important point in the dissertation, as subsequent chapters will demonstrate how state practice in cyberwar up-ends this structure, creating the cyber-geographical gap.

Chapter 4

What is cyberwar?

Introduction

The second section of this dissertation addresses the issue of how states engage in cyberwar, and how those actions exist in a spatiality of power model rather than the strictly territorial model of chapter 3. Cyberwar is a broad and complex field, and despite emerging into public consciousness in the early 1980s (Warner, 2012), there remains no generally accepted definition of cyberwar either in academia or international law (Hathaway et al., 2011). As there is no clear definition or understanding of what cyberwar is, ideas range from its complete non-existence to cyberwar as an omni-present existential threat to civilization. Further, the focus of this dissertation is on inter-state cyberwar, the definition used in this dissertation and developed in this chapter will reference states as the main actors of cyberwar, despite the presence of non-state and other actors. Thus, given the serious challenges to what constitutes cyberwar, it is important that definitional clarity be established given the prominence of cyberwar in underpinning the broader research goals of this dissertation.

The purpose of this chapter is to both provide definitional clarity for cyberwar and serve as a literature review for the concept itself. It defines cyberwar as actions undertaken by states to alter information, disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. By seeking to define cyberwar, this chapter allows for definitional ambiguity to be acknowledged and overcome, so that the substantive work of chapter 5 can demonstrate how cyberwar is prosecuted along a spatiality of power model.

Structurally, this chapter will at first provide a definition for cyberwar. Then, it will address the definitional ambiguity of existing cyberwar definitions and articulate the need for a model of cyberwar. A literature review follows, which highlights the varying attempts at establishing a definition of cyberwar in academic literature.

The literature review will demonstrate how cyberwar is often confused with cybercrime, cyberterrorism, and cyberespionage. Indeed, academic efforts at establishing a definition often resort to defining cyberwar by these subordinate categories, so much so that Rid (2012a, 2013) claims that cyberwar only consists of these actions and does not exist. This is addressed in a section which outlines what cybercrime, cyberterrorism, and cyberespionage are and how they are incorporated or separate from cyberwar.

This sets the stage for incorporating the existing academic literature into a three-part model centered on positions defined as alarmist, skeptic, and realist. The purpose of this model is to demonstrate how the existing attempts to define cyberwar are broadly separated into three conceptual categories, allowing for the compromise definition offered in this chapter to be clearly seen. The final section of this chapter will outline the definitional compromise proposed by the definition used in this dissertation, clearly outlining the actors, actions, geography, targets, and effects which constitute cyberwar. Thus, clearly establishing the definitional setting for chapter 5's exploration of how cyberwar is actually prosecuted.

Definitional Ambiguity – the need for a model

The contributing factors to cyberwar's definitional ambiguity are grounded in defining the actors, actions, geography, targets, and effects which constitute cyberwar. As a result, research on cyberwar must first understand the conceptual terrain of defining cyberwar and present a coherent definition of what is meant by the term. Defining cyberwar is dependent upon understanding if and how "offline" concepts which underpin historical definitions of war and violence are applicable to cyberspace. To that end, this chapter proposes to offer a definition of cyberwar while engaging with its definitional ambiguity, constituent elements, and the shortcomings of existing models.

Several elements contribute to the difficulty in defining cyberwar: actors, actions, effects and geography. Actors in cyberspace can be states, non-state actors, corporations, social movements, or individuals. Due to the relative parity of action in cyberspace, a small group of hackers can cripple a state's Internet, financial, or physical infrastructure – including the possibility of inflicting military or civilian casualties. Actions, on the other hand, are situated with existing conceptual frameworks for violence and force, such as understanding whether defacing the U.S. Department of Defense's website is a hostile or violent act or simply a new form of civil disobedience (Himma, 2005; Oliva, 2013). Understanding what a hostile action in cyberspace is versus civil disobedience or idle curiosity is vital to avoiding or escalating cyberwar.

This chapter proposes a definition of cyberwar which articulates actors, actions, and geography influenced by Clarke (2012), Rid (2013), Stone (2013), and Rosenfield (2009). It is composed of four points:

1. Cyberspace engenders different and contextually relevant understandings of force and violence.

2. Acts of cyberwar occur within a spatiality of power model rather than falling under strict territorial geographies.

3. Cyberwar can only occur between ICANN/ISO recognized states.

4. Cyberwar includes actions which are purposely intended to alter information, or disrupt computer systems, computer networks, or devices/information controlled or hosted by a computer. It can occur in lieu of, in concert with, or apart from kinetic conflict (S. Jones, 2014).

Cyberwar is actions undertaken by states to alter information, disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. This definition addresses the ambiguity surrounding actors, acts, and geography while situating cyberwar within a framework that respects the emergence of a new domain - one which shapes and re-shapes the geopolitics of conflict. For example, a state may own critical computing resources around the world, de-coupling cyberpower from territory yet retaining the idea of state power along a spatiality of power model, as with Chinese hacks of Google Hong Kong (Efrati & Gorman, 2011) or Iran's attacks on SaudiAramCo computers (Gross, 2013). The definition offered does not exclude that other forms of conflict or contention occur in cyberspace, such as cyberterrorism, but that they are not at the scale of cyberwar with regards to resources or geographic extent or spread.

Much of the debate on determining what is cyberwar focuses on the applicability of existing international law and state practice to cyberspace (Aldrich, 1996; Barkham, 2001; Brown, 2006; Buchan, 2012; Delibasis, 2007; DeLuca, 2013; Doswald-Beck, 2002; Fidler, 2011; A. C. Foltz, 2012; Goldsmith, 2011; Greenberg, Goodman, & Soo Hoo, 1998; Hathaway et al., 2011; Johnson, 1999; Tsagourias, 2012). This perspective believes that state actions in physical space have analogies in cyberspace, and that actions in cyberspace can be understood in terms of conventional territorial logics. Certain types of cyberattacks, such as those against critical infrastructure, are considered analogous to armed attacks because they can cause significant harm to both military and civilian populations. They would be explicit acts of cyberwar, allowing a state to be entitled to act in self-defense. The potential for such attacks falls under the international legal concept of *jus ad bellum*, how a state justifies that self-defense. In following this logic, once cyberwar has begun, then cyberattacks fall under the concept of *jus in bello*, or the rules governing the process of warfare. How *jus ad bellum* and *jus in bello* apply to cyberwar is constrained within existing United Nations charter (Articles 2(4), 39, 41, 51) and other relevant international legal regimes **(**Appendix I).

However, existing international law has no clear definition for war, indeed it only articulates the means through which a state may engage in self-defense (Hathaway et al., 2011; Schmitt, 2013). Existing legal frameworks are only partially relevant to the broad range of actions in cyberwar which do not fall under *jus ad bellum* and *jus in bello*. These hostile actions can be governed by different sets of laws, such as: a) specific existing international agreements on cyberspace; b) location-based agreements through which the means of cyberwar are governed, such as the law of the sea, and international legal frameworks governing outer space, transnational communications, and aviation; and, c) international law of countermeasures which regulate how states respond to violations which do not meet the threshold justifying the use of force.

Applying existing legal regimes, territorial law and the notion of jurisdiction to cyberwar situates it within a cyber-realist perspective (Manjikian, 2010) which constructs cyberwar within the existing legal-territorial framework. However, a significant number of non-geographic actions occur outside of this legal-territorial framework. These attacks operate from a legal frontier and liberal-utopian position (Manjikian, 2010) where cyberwar operates freely and openly across international legal boundaries. The paradox of realist structure and liberal-utopian action is central to the efforts of states and national governments to apply a legal-territorial framework to cyberwar. These actions can be seen to operate across a "spatiality of power" (Agnew, 2003) where power and actions as not confined to the limitations of a "territorial trap" (Agnew, 1994).

Attempts to define cyberwar

The definitional ambiguity of cyberwar has not deterred academia, the military, or government in attempting to define cyberwar. Indeed, early definitions and popular media, such as the influential 1983 movie WarGames, have helped to define cyberwar before a critical engagement with this new conceptual terrain could begin. In the early and seminal work *Cyberwar is Coming!* by Arquilla and Ronfeldt (1993) argues that:

> “Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to “know” itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the “balance of information and knowledge” in one’s favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended.” (Arquilla & Ronfeldt, 1993, p. 30)

This definition is one of the most influential definitions of cyberwar, coming at the dawn of public awareness of cyberwar in 1993. It immediately established a class of “alarmist” definitions which argued that cyberwar was imminent or actively occurring and represented a fundamental threat to U.S. interests, in line with the popular geopolitics of the Cold War. The United States and its allies were portrayed as under constant threat or attack by various enemies, necessitating a strong defense and advocating for viewing cyberspace as a domain in which the United States could achieve and maintain dominance (Lynn, 2010). This was supported by military thinkers and policy which advocated a similar response to the real and perceived threats in cyberspace.

Alarmist definitions are not confined to the Internet's early development, but continue to be a dominant and recurrent theme in cyberwar thought and policy. One of the most influential thinkers, former White House counter-terrorism advisor Richard Clarke, argued in his 2010 bestselling book *Cyber War: The Next Threat to National Security and What to Do About It* that cyberwar was "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke & Knake, 2012, p. 6). Clarke's definition and book proved to be highly influential in cyberwar research, it is the one of the most highly cited (in Google Scholar) treatises on cyberwar, falling behind two other alarmist works from the 1990s by Arquilla and Ronfeldt (1993).

Mehan (2009) extends the alarmist model into categories which seek to articulate different classes of cyberwar based on broad-based definitions of actions. Class I cyberwar deals with personal informational security (similar to concepts of cyberwar during the 1960s); Class II emphasizes espionage, be it corporate or state-based; Class III includes DDoS and other disruptive actions and equated to cyberterrorism; and Class IV incorporates classes I-III in addition to overt military cyber operations in support of military offensive actions. At no point does Mehan (2009) specify the nature of the actions or the actors involved, leaving cyberwar open to talented individual hackers, anonymous collectives, social movements, terrorist organizations, corporations, military alliances, and states.

These definitions are alarmist, asserting that cyberwar is imminent/occurring while at the same time seeking the broadest possible interpretations for cyberwar. They are supported by military and defense policies and statements which warn against an imminent “digital Pearl Harbor” (Lindsay, 2013; Stohl, 2006) and statements by the Chairman of the Joint Chiefs of Staff that "A cyber attack could stop our society in its tracks" (Bender, 2012). This is coupled with aggressive budgeting of over $4.5 billion in pursuit of gaining strategic advantage in cyberspace.   Alarmist definitions have little mention of actors or actions in these, though there are many examples consistent with the amalgamated sense of what cyberwar is: everything to anybody at any time and a world in which the West is under imminent existential threat (Mullen, 2011).

Another class of scholars, known as cyberskeptics, argue that the threats of cyberwar are blown out of proportion and are a continuation of Cold War “missile gap” fear-mongering between the US and USSR (Brito & Watkins, 2011). To them, cyberwar has been hyped up to benefit military defense budgets and a cyber-industrial complex (Brito & Watkins, 2011; Geer Jr, 2011) of software and security firms looking for government grants. Some skeptics, like Thomas Rid (2012) prefer definitions of cyberwar grounded in traditional state-centric understandings of war. For Liff (2012) the realities of cyberwar limit its actual effectiveness into something which can only emphasize pre-existing political leverage or power. At their cores, these approaches emphasize 19th century theorists, such as Clausewitz, who developed highly specific definitions of war. For Rid (2013) these definitions are enough and though they emerged during the height of the nation-state, they nonetheless are sufficient to cover today’s conflict domains.

As Rid (2013) further argues, Clausewitz states that war must be: violent by using force; instrumental in seeking to force an enemy to change; and with political aims. For cyberwar skeptics like Rid, there has yet to be any action or grouping of actions in cyberspace which could satisfy Clausewitz’s definition of war. The actions which have taken place and which can take place given technical limitations can be classified as espionage, sabotage, or subterfuge but nothing that could resemble what is broadly understood by the word “war”.

Rid’s approach is an ends-based approach which focuses on war when it emerges rather than what contributes to causing war (Junio, 2013). Thus, following Rid’s Clausewitzian understanding, Gh0stNet would not be an act of cyberwar, nor would StuxNet. Both events lacked the critical element of lethal force, and therefore fall short of Clausewitz’s definition.

Further, the plausible deniability inherent in much of cyberwar makes determining the political or instrumental reasoning behind these acts difficult, reinforcing the Clausewitzian position.

A final set of scholars seeks to ground cyberwar within existing legal regimes and structures. These scholars argue that existing international law is sufficient to define and understand what cyberwar is and isn't. This perspective includes official publications from NATO which determines how international law applies to cyberwarfare (Schmitt, 2013). Manjikian (2010) argues that this perspective adopts a realist interpretation of cyberspace, seeing it as something which exists within existing power structures and geographies which can be adapted to existing law, with minor modifications. The legalistic perspective is, ultimately, predicated upon the state as the final legitimate geopolitical unit.

Hathaway (2011) and the Tallinn Manual (2013) situate combat as occurring between states grounded within the United Nations charter and international legal agreements. This is buttressed by recent international legislation on cybercrime in Europe (Clough, 2012) and in Clarke's (2012) prescription of basing international cybersecurity upon existing state behavioral precedents. Non-state actors are treated as aberrations, regardless of whether these non-state actors are assisting states in upholding or violating international law. Crowdsourced DDoS attacks, such as those which occurred against Iran in 2009 (Nazario, 2009), against various Arab states in 2011 (Sabadello, 2011), or against financial firms which declined to process payments for WikiLeaks (Beyer, 2014; Mackey, 2010), are examples of when this approach encounters problems. Using established legal precedent predicated upon the international financial system, states that sanction such activities by not pursuing legal action or aiding in investigations would be disconnected from the Internet until such a time as the attacks stop (Clarke & Knake, 2012).

However, this approach would create a nearly permanent unstable Internet and negates the issue of scale associated with non-state actors which may operate across multiple international legal jurisdictions. Further, cybercriminals harnessing botnets to launch attacks could falsely implicate states in attacks by non-state actors when no such activity is taking place.

These definitions take the state to be the only geographical unit of analysis. No actors outside of states have the financial and technical resources to have develop the world's first cyberweapon: StuxNet. Indeed, Lindsay (2013) and Betz (2012) argue that only states have the resources to conduct cyberwar or develop cyberweapons of sufficient complexity such as StuxNet, DuQu, or Flame. However, there is abundant empirical evidence which demonstrates that states outsource cyberwar to industrious hackers, quasi-government organizations, outraged private citizen groups, terrorist organizations, and the criminal underworld (Klimburg, 2011; Korns & Kastenberg, 2008). Different actions involve different actors, largely dependent upon technical skill and attributability. These actions, such as exfiltrating classified documents, defacing or disabling websites, or infecting critical computers with malware, fall under alarmist definitions of cyberwar most often as cyberespionage, cyberterrorism, and cybercrime. Thus, to understand cyberwar more clearly an understanding of what these actions are and how they differ from cyberwar is crucial.

Understanding Cybercrime, Cyberterrorism, and Cyberespionage

For some skeptical scholars the history of cyberwar is only a history of cybercrime, cybeterrorism, and cyberespionage (Rid, 2013). However, alarmist scholars argue that these are three distinctly different concepts that states could or could not choose to engage in. Skeptics take evidence of state outsourcing of cyberattacks, such as North Korea, Russia, or China

(Clarke & Knake, 2012; Klimburg, 2011; Korns & Kastenberg, 2008; Warf, 2015) as demonstrating the viability of non-state actors and the non-existence of cyberwar. While these actions may not constitute acts of cyberwar, the resources to successfully pursue them on a significant scale constitutes a reconceptualization of violence in cyberspace (Stone, 2013).

Disentangling cybercrime, cyberterrorism, and cyberespionage from cyberwar frees cyberwar conceptually to focus on ends rather than means. Table 2 presents a matrix which outlines the commonalities and differences between the three.

	Explanation	**Cybercrime**	**Cyberterrorism**	**Cyberespionage**
Actions	What constitutes the act(s)	Identity theft, malware development and infection, phishing	Hacking, logic-bombs, infiltration, defacement, malware	Infiltration, malware, spear-phishing, hacking
Actors	The actors which most typically engage in the act(s)	Non-state actors, groups, criminal organizations, individuals	Non-state actors, terrorist groups, individuals	States, multi-national and domestic corporations, individuals
Direct and indirect effects	The object or concept of focus and its effects.	Credit card fraud, test concepts for cyberweapons	Politically motivated, designed to reduce trust in existing social institutions	Visible effects undesirable; loss of economic advantage; intelligence gathering
Location	Geographical and/or spatial aspects	Cyberspace exclusively	Cyberspace to influence physical space, physical space as vector for acts	Cyberspace, physical infiltration
Targets	Who/what is targeted?	Individuals, corporations.	Politically relevant information, computer systems, computer programs, and data.	State or corporate computer systems.

Table 2: Aspects of Cybercrime, Cyberterrorism, and Cyberespionage

Cybercrime

The costs of cybercrime are tremendous: over $100 billion per year in the United States alone (Lewis & Baker, 2013). Cybercrime has multiple components and overlaps with cyberespionage and can feed into cyberterrorism. At its most basic, cybercrime involves conducting criminal activities over the Internet (Moore, 2011; Sood, Bansal, & Enbody, 2013). While this definition is broad and vague, most of these criminal activities are financial in nature, emphasizing identity theft, credit card fraud, and customer database hacking. For cybercrime, the Internet is an integral component of conducting the criminal act, facilitating crime through relative anonymity and technical sophistication.

An expanded definition includes the use of the Internet as a means to facilitate a traditionally offline crime. The use of strong anonymity and encryption tools, such as Tor or FreeNet, facilitate an expansion of the illegal drug, endangered species, and child pornography trade on the Internet (Bradbury, 2014). Websites can be established which are known and available only to users who have the unique randomized address. Users pay a premium for membership in exchange for security, privacy, and anonymity to pursue activities known to be illegal in most jurisdictions.

Cybercriminals also develop malware to infect machines and then use those machines (called “zombies”) to perform activities on behalf of the criminal organization. These zombies can be used to attack websites as part of a “botnet”, or network of zombies (Cooke, Jahanian, & McPherson, 2005), and can be used to retrieve confidential files from infected computers which are then sold on the black market. Botnets can be rented or sold resulting in an active market for elements of cyberwar with both states and non-state actors as buyers while allowing for plausible deniability (Li, Liao, & Striegel, 2009).

Infecting these computers requires sophisticated software development skills, and cybercriminals are tapped by states to provide details about exploits, develop malware, or to serve as software developers for the next cyberweapon, a situation which scholars have dubbed the "malware-industrial complex" (Simonite, 2013). For instance, cybercriminals discover previously unknown vulnerabilities in servers and software in order to successfully exploit them to infect computers. These exploits are known as "zero day exploits" and are vital to state espionage – states can often pay over $50,000 per exploit on the black market (Ablon, Libicki, & Golay, 2014**).** Thus, cybercrime encompasses not only activities which are harmful to states and their citizens, but the pursuit of those criminal activities also benefits states (Simonite, 2013).

Zero day and other exploits can also be used by cybercriminals to gain access to customer databases for the purposes of stealing confidential information such as credit card and social security numbers. These data are then resold on secondary markets or used by the cybercriminals themselves to make fraudulent transactions or financial advances. Recent examples of cybercrime include hacks of Target resulting in the theft of more than 40 million credit card numbers (Yang & Tsukayama, 2013), as well as the hack of Anthem Healthcare's database leading to the theft of "…80 million records that included Social Security numbers, birthdays, addresses, email and employment information and income data for customers and employees, including its own chief executive" (Abelson & Goldstein, 2015, p. 1).

Cyberterrorism

The fear that terrorists and other non-state actors who use violence to achieve political aims or make political statements, could use the Internet to wreak havoc on the United States is among the earliest concerns with information security in the 1980s (Greenhouse, 1987). Cyberterrorism was repeatedly mentioned as a concern during congressional testimony in support of increased information security during the administration of Ronald Reagan as well as fitting within an existing geopolitical framing of the United States as being under imminent existential threat (Warner, 2012). Pollitt (1998) offers a highly-cited definition of cyberterrorism as "the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents" (Pollitt, 1998, p. 67).

Foltz (2004) suggests that the actions associated with cyberterrorism could involve sabotaging the power grid, interference in a domestic financial system (Embar-Seddon, 2002), attacking computer systems, or crippling national infrastructure. However, these actions are also consistent with definitions of cyberwar (Clarke & Knake, 2012). Further complicating the issue is the employment of non-state actors by states to carry out acts of cyberterrorism rather than outright cyberwar. For instance, the Syrian Electronic Army's hack of the Associated Press (Fisher, 2013) or the Iran-backed 2013 string of attacks against U.S. financial institutions (Perlroth & Sanger, 2013) were actions treated as cyberterrorism, regardless of state sponsorship or affiliation. This approach seems to rely on the act and the political motivation rather than financial support, or proclaimed allegiance, or other avenue of attribution.

Similar to earlier definitions of cyberterrorism, the U.S. military defines cyberterrorism as "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives" (U.S. Army Training and Doctrine Command, 2005). This argues that terrorist acts in cyberspace are analogous to terrorist acts offline (Gable, 2009).

Noted security expert Eugene Kaspersky has stated (Shamah, 2012) that it is difficult to discern the difference between what constitutes an act of cyberwar versus an act of cyberterrorism. Kaspersky goes so far as to state that all acts of cyberwar are cyberterrorism, given their explicitly political aims and goals of information destruction or dominance. The general definition of terrorism is highly contested (Schmid, Jongman, & Horowitz, 2005), and attempting to broaden or narrow this definition by incorporating a computer element complicates efforts at understanding exactly what cyberwar is. This is an approach offered by Denning (2007) whose influential definition of cyberterrorism asserts that it is "highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social" (D. Denning, 2007, p. 2). Like Pollitt (1998) she argues that the difference between cyberwar and cyberterrorism is that the former concerns states and the latter non-state actors. Thus, what defines cyberterrorism is less the specific actions, which are similar to earlier definitions of cyberwar, but rather the political geographical structure of the principal actors involved.

Due to the contentious nature of the political in cyberterrorism attacks, examples are controversial without an ability to examine the financial or power trails which might induce actions. However, recent examples of cyberterrorism are exemplified by their desire to cause harm or disruption in furtherance of explicitly political goals by subnational groups. In Japan, in the year 2000 it was discovered that large numbers of government agencies had been using software which had been installed by the Aum Shinrikyo group, which had earlier killed a dozen people in a sarin gas attack in a Tokyo subway (Sims, 2000). The purpose or reason of the software was not known, with officials speculating the software may be used by the sect in planning future terrorist attacks (Sims, 2000).

More recently, Sony Pictures was hacked by an unknown group purported to have ties to North Korea (D. E. Sanger & Perlroth, 2014), though significant doubts have been raised about that assertion (Faughnder & Hamedy, 2014; Rayman, 2014). This attack was conducted by a group called the Guardians of Peace, and saw many Sony movies released for free on the Internet. Internal emails, financial information, and other Sony corporate secrets were released in an apparent bid to stop the studio from releasing a movie about the murder of North Korean dictator Kim Jong Un (D. E. Sanger & Perlroth, 2014).

Cyberespionage

Cyberespionage has the longest and most diverse history of concepts relating to cyberwar. The earliest known act associated with physical cyberespionage took place in 1968 when East German spies were arrested by West German police at IBM's regional subsidiary (Warner, 2012). Cyberespionage of exclusively digital assets is traced back to 1982 when Soviet spies infiltrated a Canadian firm (Singer & Friedman, 2014). Numerous other actions and events have taken place which likely remain classified and range from exclusively digital acts to complicated cyberespionage operations involving physical security.

Acts of cyberespionage are motivated to discover and retrieve information rather than cause disruption or harm (Ophardt, 2010). It is the most pervasive offensive digital action taken by states (Carr, 2009), and represents a significant threat to both state and industrial secrets. It is estimated that cyberespionage costs the global economy between $300 billion to $1 trillion dollars annually (Lewis & Baker, 2013). The U.S. Office of the National Counterintelligence Executive estimates cyberespionage costs Germany $28-71 billion annually and South Korea $82 billion, while more than 85% of Canadian firms had been victims of cyberespionage at some point (Office of the National Counterintelligence Executive, 2011). The economic damage is significant due to the theft of intellectual property and the subsequent use of the information to create lower cost alternatives in countries such as China (Freeze, 2012). Recent research has argued that cyberespionage is a way for states such as China to compete internationally as well as a powerful method to gain economic and strategic military advantage (Clarke & Knake, 2012).

The costs of cyberespionage translate directly into lost jobs, such as with Nortel Networks. Nortel Networks was a major international telecommunications firm which employed more than 90,000 people worldwide (Austen, 2013). Since the year 2000 Nortel had been seriously compromised by hackers in possession of the passwords for the CEO and six other top executives while exfiltrating thousands of documents, emails, and R&D reports (Deibert, 2013). At the same time, Chinese-based competitors such as Huawei began to aggressively develop new technologies and products which eventually forced Nortel to declare bankruptcy (Freeze, 2012).

Security researchers have claimed that Huawei and other Chinese firms directly participated in and benefitted from cyberespionage against Nortel for a decade (Freeze, 2012; Gorman, 2012; Schecter, 2013). Indeed, Huawei was implicated in a report issued by the Permanent Select Committee on Intelligence in the U.S. House of Representatives in cyberespionage and representing an intelligence and security threat to the United States (M. Rogers & Ruppersberger, 2012; Spade, 2011).

The security threat of cyberespionage is further highlighted by massive exfiltration of data for the confidential F-35 fighter, with internal networks so severely compromised the hackers were actually able to gain access to the plane while it was in the midst of a test flight (Singer & Friedman, 2014). The theft of the data resulted in costs of billions of dollars to re-engineer the plane, resulting in delays and additional costs to taxpayers and firms involved in a major project.

Cyberespionage itself is focused on discovering vulnerabilities, infiltrating networks, and exfiltrating data. It can also involve the collection and collation of “open source intelligence”, intelligence and information gleaned from social media and blog posts (Bradbury, 2011), as well as from “spear-phishing” through targeting high-profile individuals for their strategic intelligence value. As the Gh0stNet case and the above examples illustrate, cyberespionage can be perpetrated by state or non-state actors targeting both state and non-state actors.

China is the leading country which engages in cyberespionage (Carr, 2009), as in the Gh0StNet case, and other cases of cyberespionage against state targets such as Operation Aurora which in 2010 which forced Google to leave China and severely compromised Adobe Systems, Symantec, Yahoo, Northrop Grumman, Dow Chemical (Cha & Nakashima, 2010), and Morgan

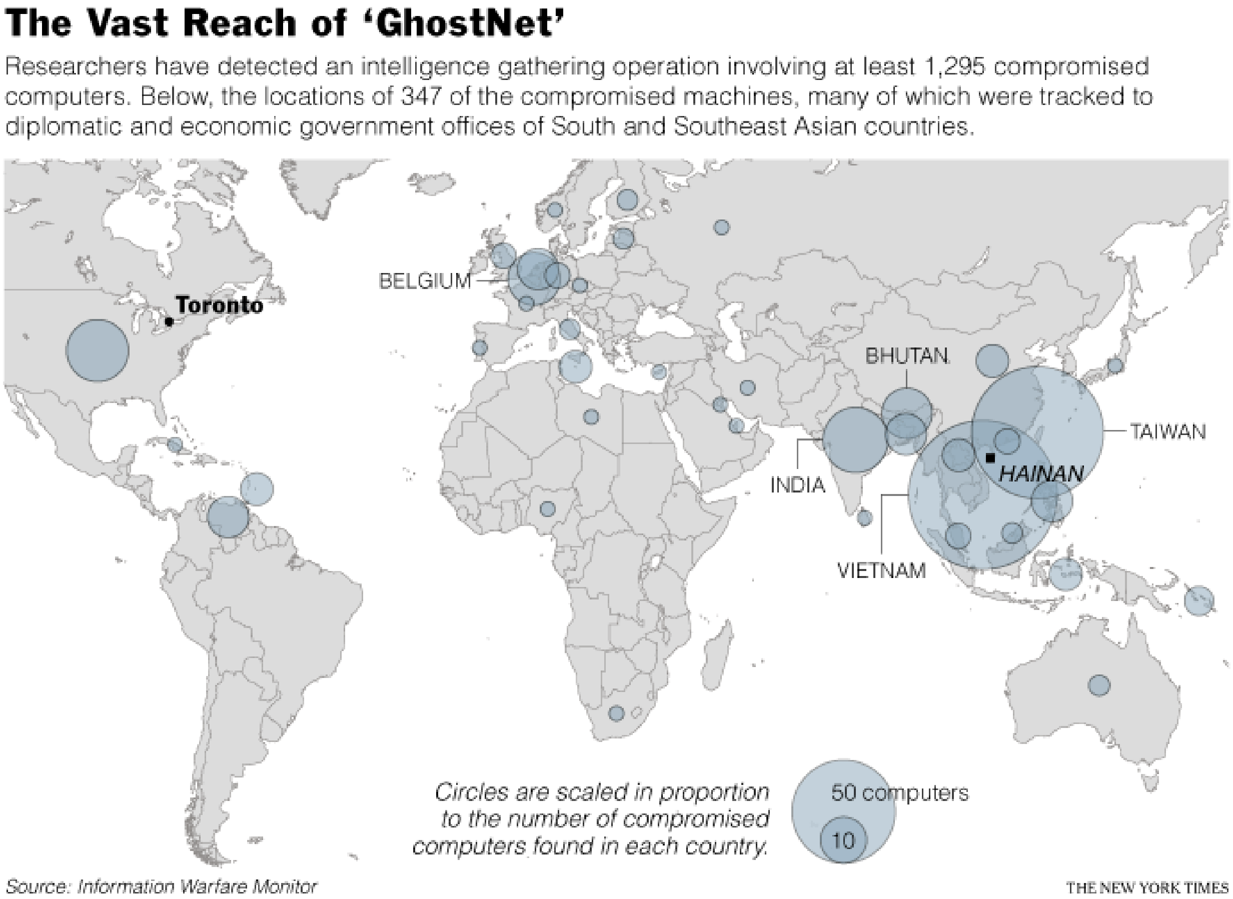
Stanley (Schwartz, 2013). The severity and persistence of the attacks continues despite high-level warnings from the United States as well as calls for arrests of specific Chinese individuals in 2014 (M. S. Schmidt & Sanger, 2014), which serves to demonstrate the limitations of conventional diplomacy when plausible deniability is a fundamental feature of cyberespionage.

Authoritarian states use cyberespionage to develop profiles of key activists and develop maps of their activist and social networks (Evgeny Morozov, 2012). Increasingly Western states are using cyberespionage, as the leaked Edward Snowden files assert that there were in excess of 200 cyberespionage operations by the CIA and NSA in 2011 alone (Singer & Friedman, 2014). Cyberespionage is a vital part of state intelligence gathering operations as well as an asset for strategic and economic gain. Private corporations engage in cyberespionage between each other or in cooperation with national governments, as in the case of Huawei. Further, the elements of cyberespionage, such as infiltration and network penetration testing, are common elements in cyberwar and also serve as the technical underpinning for cybercrime and cyberterrorism.

Thus, examples of cyberespionage are oftentimes interwoven with acts of cyberwar between states. For example, the success of the StuxNet, Duqu, and Flame malwares (Gross, 2013) involved elements of cyberespionage to identify strategic assets within Iran’s nuclear infrastructure for future attack. Cyber-espionage is rarely publicly acknowledged, but this trend was reversed by the recent call by President Obama on China to cease its substantial cyberespionage efforts: “Increasingly, U.S. businesses are speaking out about their serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber-intrusions on an unprecedented scale,” (Nakashima, 2013). Experts believe that the recent Chinese efforts at cyberespionage are substantial enough that most institutions in Washington have been compromised (Timberg & Nakashima, 2013).

Perhaps one of the most famous and damaging cases of cyberespionage occurred in 2009 when researchers at the Citizen Lab in the University of Toronto discovered a widespread espionage network, dubbed Gh0stNet, targeting 103 countries and critical ministries, embassies, government agencies, international media, and high-value individuals (Deibert, 2013). The attack had been uncovered when researchers were contacted by the offices of the Dalai Lama about concerns that their computers were being hacked or monitored.

Through a sophisticated investigation the researchers were able to find the main command and control server for the entire operation. From there they were able to determine that the hackers had accessed ministries of foreign affairs offices of countries such as Germany, Iran, Pakistan, and Taiwan (Deibert, 2013). The attackers also had access to computers at the United Nations, ASEAN, NATO, the Prime Minister of Laos' office, and the email server for the Associate Press in Hong Kong. The scale of the compromise was enormous, giving the attackers an unparalleled ability to have an “informational pulse” of major news organizations, international alliances, and foreign ministries of over 100 countries.



The Vast Reach of 'GhostNet'

Researchers have detected an intelligence gathering operation involving at least 1,295 compromised computers. Below, the locations of 347 of the compromised machines, many of which were tracked to diplomatic and economic government offices of South and Southeast Asian countries.

Circles are scaled in proportion to the number of compromised computers found in each country.

Source: Information Warfare Monitor

THE NEW YORK TIMES

Fig. 14 – The Vast Reach of the Gh0stNet cyberespionage network (From Markoff, 2009)

The attacks appeared to originate from China's cyberspace and further research seemed to confirm China's involvement – either explicitly or implicitly (Deibert, 2013). The Gh0stNet cyberespionage affair was the largest and most geographically diverse cyberespionage ring ever discovered. The breadth and scope of the operation was tremendous and the information gathered from around the world was invaluable to the attackers and set a new standard for sophistication in cyberespionage operations.

Cyberwar and its constituent elements

Cybercrime, cyberterrorism, and cyberespionage are considered in some academic, military, and policy literatures as being separate yet interrelated concepts, intimately related to cyberwar. Understanding where these concepts begin or end is problematic and has contributed to definitional ambiguity, as demonstrated in Rid's (2013) assertion that cyberwar only consists in these three acts and consequently doesn't exist or in understanding that cyberespionage is a key element in a broader cyberterrorist or cyberwar campaign, such as planting logic bombs.

The key variables for determining the boundaries between these concepts are not technical means, but motivation, financial support, or end use. While the skeptical position argues that these are not part of a broader concept of cyberwar but separate concepts, the alarmist position sees them as integral to cyberwar, while realists seek to situate them within existing concepts of terrorism, crime, and intelligence services actions.

Each of these concepts are integral to certain definitions of cyberwar yet can also stand alone. The individual technical acts, when taken out of political or social contexts, are identical and become difficult to differentiate. The motivations of individuals, groups, non-state actors, or states also does little to clarify whether or not an action is one of cyberwar, cyberterrorism, or something else. States will utilize all the available resources and actions at their disposal in the prosecution of cyberwar as each serves a unique and distinct role, and only states have the financial and technical resources to make these endeavors fruitful (Betz, 2012; Lindsay, 2013).

Understanding cyberterrorism, cyberespionage, and cybercrime allows for cyberwar to be seen as an independent concept and phenomenon. Although states may utilize the techniques associated with these concepts in the prosecution of cyberwar, these elements do not constitute cyberwar itself in the same way that international sanctions, or financial seizure in support of conventional kinetic war do not represent acts of war, in keeping with the state behavior precedence model (Clarke & Knake, 2012).

Failure to define cyberwar

Each broad camp in the literature presents arguments for the actions, actors, effects, geography, and targets of cyberwar. The definition of cyberwar presented at the start of this chapter incorporates elements from all three camps to develop an understanding of cyberwar as a distinct event framed by specific political geographies, actors, and actions.

The common thread in the literature has been an emphasis on a means or ends based definition of cyberwar. That is, cyberwar is only considered cyberwar if the means or ends are configured in a certain way. For example, to Rid (2013), cyberwar must meet Clausewitz's definition which sees war as necessarily being violent by using force; instrumental in seeing to force an enemy to change; and with political aims. For Clarke (2012) it must be "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.". Still others define cyberwar within a pre-existing international legal framework which they argue will fit cyberwar with only minor modifications, in other words adopting a legal-realist framework towards cyberwar (Manjikian, 2010). At the same time other scholars (Deibert, 2013), argue that cyberwar is a contentious topic and frontier – subject to daily redefinitions of what it is and who the actors are with no clear definition possible.

In the surveyed literature, three key variables underpin the arguments scholars make in understanding cyberwar: actors, actions, and geography. Actors represent the dominant entities between which cyberwar can occur. These actors pursue specific actions against targets and for specific effects. Both actors and actions occur within and transcend or are juxtaposed against various political geographies. An adequate definition of cyberwar must address these themes.

This dissertation proposes that cyberwar is actions undertaken by states to alter information, disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. This definition is established by four elements:

1. Cyberspace engenders different and contextually relevant understandings of force and violence.

2. Acts of cyberwar occur within a spatiality of power model rather than falling under strict territorial geographies.

3. Cyberwar can only occur between ICANN/ISO recognized states.

4. Cyberwar includes actions which are purposely intended to alter information, or disrupt computer systems, computer networks, or devices/information controlled or hosted by a computer. It can occur in lieu of, in concert with, or apart from kinetic conflict (S. Jones, 2014).

These four elements can used to define the categories in terms of actors, actions, and geography:

Alarmist: Argue that cyberwar is real and the United States and its allies are under immediate existential threat.

Skeptic: Skeptics argue that cyberwar is, at best, a contested idea predicated upon hype to benefit political elites.

Realist: Some form of conflict in cyberspace exists, and seek to classify or understand it through existing international legal structures and state behavior norms.

Each of these three themes articulates different structures to force and violence in cyberspace, with alarmists seeing cyberwar as present, skeptics questioning if cyberwar exists, and realists attempting to ground cyberwar into existing international legal and political frameworks.

The three perspectives

The table below summarizes the three themes of cyberwar literature and the state-based definition proposed in this dissertation:

Question	Explanation	Alarmist	Skeptic	Realist
Actions	Nature of hostile actions in cyberspace	Cheap and widespread	Expensive and complicated	Both
Actors	The “legitimate” actors in cyberwar.	Anyone/anything; final responsibility is with states	States	Anyone/anything
Effects	Possible effects of cyberwar	Large-scale disruption or destruction, military decapitation	Small-scale, local disruption	Legal implications for international state system
Geography	The constituent elements of the theatre(s) where cyberwar takes place.	Cyberspace is separate, but may intersect with physical space	Cyberspace is only proxy for physical space	Cyberspace and physical space are legally and practically indistinguishable
Targets	The targets of cyberwar.	Critical state or military infrastructure/information	Human beings	Military targets, individuals, corporations, states

Table 3: Alarmist, Skeptic, and Realist positions

Constituent Elements

The constituent elements of each definition are actions, actors, effects, geography, and targets. These are explained below:

Actions: Defining cyberwar entails defining what actions are or are not considered part of cyberwar. During the 1990s, for instance, DDoS attacks and website defacement were considered hostile acts which could cripple vital communications internationally and domestically. During Russia's 2008 invasion of Georgia and the 2007 cyberwar with Estonia, these tactics were used to great success in order to create “information dominance” (Heickerö, 2010; Mowthorpe, 2005). However, more recent research has argued that these acts have changed in nature as robust defenses become more common – they are acts of disobedience or mild disruption. Thus, it becomes vital to understand how each definitional category understands and sees the technical actions associated with cyberwar.

Actors: The defined actions of cyberwar have as their origin and destination human actors, regardless of intermediary destination. Defining and articulating actors represents a way in which legitimacy is conferred in cyberwar, requiring or allowing certain responses in line with how the actors are classified. For example, the 1999 attacks against NATO computers had in their origin Chinese-sponsored groups portrayed as “patriotic citizens”. Rather than attempting to engage with the individual citizens or their actions, NATO chose to recognize China as the entity which had ultimate control over the attacks – legitimizing the state as a vital actor in cyberwar

Effects: Actions and actors seek outcomes and their associated effects, and those effects are classified differently dependent with implications for structuring what is an offensive or defensive action which could precede cyberwar. Clarke, for instance, argues that the desired effects of cyberwar are widespread destruction with concomitant societal collapse or severe disruption (Clarke & Knake, 2012). On the other hand, Rid (2012a, 2013) argues that the desired effects are localized intelligence gathering or mild disruption in information flows within closed organizational structures. Anticipated effects, therefore, provide a destination within the definitional stance for both actors and actions.

Geography: Since the earliest days of the Internet it has been conceived of as ranging from new and separate space to intimately tied with modern, everyday life and an extension of the ordinary. Understanding how definitional categories construct cyberspace guides the ways in which governments structure responses to cyberwar. For instance, the alarmist position sees cyberspace as a distinct and separate domain, with this idea embraced by the United States military by creating a separate “Cyber Command” to oversee cyberwar and defense related actions in cyberspace. Each definitional category constructs a different vision of cyberspace which reflects the actions, actors, and anticipated effects of cyberwar.

Targets: Ultimately, actions, actors, effects, and geography are also structured around the types of targets for cyberwar actions. This differs from actors as the target may or may not exercise agency. For example, alarmist definitions view critical infrastructure, such as electrical power plants, as prime targets for cyberwar. On the other hand, skeptics argue that these targets are already well-protected and that the only target which can conceptually exist is vulnerabilities in human trust. Targets serve to reinforce and ground the geographical visions of each definitional category.

Each of these five elements of cyberwar represents a structural element which has gone into developing national cyberwar and cyberdefense standards, and as such each definitional category is evaluated for similarities and differences in each aspect below.

Alarmist

The alarmist perspective argues that cyberwar is either imminent or currently occurring and represents an existential threat to Western democracies. Within the literature these scholars advocate for immediate action to address cyberwar, leveraging a Cold War geopolitical framework alongside Cold War experience and expertise to re-frame traditional opponents such as China and Russia. These scholars revive a Hobbesian worldview, seeing cyberspace as the digital spatial equivalent of “all against all” in contrast with cyber-utopians and other actors who see collaborative potential in cyberspace.

Actions: Alarmists believe that the specific technical knowledge and attack methods of cyberwar are cheap, easy to duplicate, and widespread. Framing actions in this way allows alarmist scholars to situate the United States as surrounded and infiltrated by hackers who could seriously compromise vital national infrastructure. Defenses, however, are positioned as costly and requiring concerted national effort to secure critical infrastructure. The United States and its allies are believed to be highly vulnerable to attacks of varying destructive capability. The emphasis is on actions which are primarily destructive rather than disruptive.

Actors: The alarmist rationale that actions in cyberspace are cheap and widespread lends itself to the belief that actors which would harm the United States are widely dispersed globally and domestically. These actors include individual hackers, terrorists, states, social movements, and corporations. Infected computers or devices connected to the Internet can also be seen as actors, programmed to automate attacks or discover exploits. The multiplicity of actors, however, does not imply that all actors are equal or legitimate. The emphasis within alarmist literature is on states as hostile actors who can and do employ various non-state actors on their behalf as a means to ensure plausible deniability. For alarmists the ultimate responsibility for these actions resides with the state through financing the attacks allowing use of their national cyberspace assets in pursuing the attack (Clarke & Knake, 2012)**,** or refusing to cooperate with investigations after attacks had been launched. Thus, despite the presence of multiple actors, final responsibility resides with a state if that state knowingly allows actions associated with cyberwar within its digital and physical territory, or refuses to cooperate with investigations/prosecution of actors within its sovereign territory which are associated with those actions.

Effects: Alarmist scholars emphasize the *destructive* aspects of cyberwar (Rosenfield, 2009). Technical and infrastructural destruction will have unforeseen consequences for society, necessitating an emphasis on defending from physical violence facilitated by cyberspace and responding with physical force, if need be, to cyberwar (Forman & Barnes, 2011)**.** The alarmist school of thought believes that the vulnerability of technical systems could cause power outages, water processing malfunctions, air traffic control shutdowns, and railroad collisions, among other infrastructural threats (Brito & Watkins, 2011; Wilson, 2014). In addition, based on early military simulations alarmist scholars believe that cyberwar can also be used to decapitate military command and control, resulting in battlefield chaos with the potential for significant casualties during combat operations (Adams, 2001; Arquilla, 2012; Arquilla & Ronfeldt, 1993)

Geography: The geography of cyberwar for alarmists is bifurcated between digital and physical space. Cyberwar occurs purely in cyberspace with spillover into physical space, but is a separate domain in terms of defensive and offensive actions. Nonetheless, as articulated by the United States Department of Defense:

> “A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” (Chairman of the Joint Chiefs of Staff, 2013, pp. III–15)

This domain requires man-made technologies to enter and exists apart from other domains in the electro-magnetic spectrum or as a man-made domain which nonetheless requires technologies to enter (Kuehl, 2009b). As a separate domain of operations which has consequences for other domains (land, air, sea, space) it requires specific and unique rules of engagement and operations, which have already been codified in the world's militaries, beginning in the 1980s (FitzGerald, 1997; T. L. Thomas, 2000; Warner, 2012).

Targets: The targets of cyberwar are critical national infrastructure. National infrastructure is considered a broad concept including physical infrastructure such as electricity and transportation, finance, information and media, corporate research and development, and general communications (Clinton, 1996; Jensen, 2002; Moteff & Parfomak, 2004). Because this infrastructure is diverse with varying levels of investment in cybersecurity, it is seen as both vulnerable and vital, an attractive class of targets during cyberwar. There is a firm sense of the state as spatial container of cybersecurity and violation of that space represents a physical threat to the state itself, in-line with Agnew's (1994) territorial trap.

Summary: The alarmist perspective articulates clearly defined national boundaries which are a container for vulnerability while demarcating a border to be strengthened through investment in cybersecurity. At the same time, the domain of cyberspace is separate from physical and political geography but conflict in this domain has potentially serious effects in the offline world. The national homeland is envisioned as being under threat from external cyberattackers who, due to cheap and widely-available cyberattacks, are engaged in cyberwar at present or will be in the near future. At stake is critical national infrastructure with the potential for destruction, resulting in serious national disruption of daily life and the functioning of society.

While more recent research has questioned the extent to which cyberwar threatens Western society, the alarmist position has found resonance in governments around the world who have allocated billions of dollars towards defending "national cyberspace" against real and perceived threats. By using a well-tested geopolitical logic framed around an omnipresent and threatening "other" in cyberspace, alarmists have been highly influential in developing national security policy and military doctrine.

Alarmists make use of a range of vulnerabilities in national cybersecurity to bolster their perspectives. One of the prominent examples used is an operation codenamed *Moonlight Maze* (Adams, 2001; Joyner & Lotrionte, 2001). The operation targeted the U.S. Air Force, NASA, the Departments of Energy and Defense, and major universities and research laboratories across the country (Delibasis, 2007; Rid, 2012a) Highly sensitive data was exfiltrated by the attackers, including maps of military installations and military hardware schematics (Rid, 2012a). Other similar attacks which are used by alarmists to demonstrate the high levels of vulnerability and widespread nature of cyberwar include the Gh0stNet cyberespionage ring (Deibert, 2013) and Titan Rain (Deibert, 2013) which both highlighted the vulnerability of critical government services to foreign attacks.

Skeptic

The alarmist position gained traction due to its influence in early policy circles when the Internet was in its infancy. These entrenched attitudes have been challenged by skeptics who contest the existence or scope of existing definitions of cyberwar. Skeptics argue for critical engagement with the idea of cyberwar itself, attempting to deconstruct the word and its actions in order to more clearly understand cyberwar. The level of critical engagement ranges from outright denial that cyberwar exists to reconceptualizing human violence in digital terms. What these scholars share in common is skepticism towards the various claims put forth by alarmists, and a desire to shift the debate from the entrenched "inevitability of cyberwar" discursive logic towards one which seeks interrogate the idea of cyberwar itself.

Actions: Skeptical scholars argue that the acts of cyberwar are not widespread and inexpensive, but costly and expensive. They cite the significant investment in a technology like StuxNet or the extensive insider knowledge needed to hack into an electrical power plant as examples of the extremely high barriers to entry to disruptive actions in cyberspace (Rosenfield, 2009). These high barriers to entry prohibit actors other than states from engaging in any actions which would be considered as existential threats (Rid, 2012a, 2013; Rosenfield, 2009). These actions, further, are not explicit acts of war but rather are disruptive (Rosenfield, 2009) and highly focused acts of sabotage, espionage, and subversion and thus do not represent an act of war as commonly understood, but rather traditional covert state behavior migrating to cyberspace.

Actors: Due to expense and complexity, cyberwar is restricted exclusively to states. States may outsource certain cyberwar actions to mercenary groups or talented individuals, but only states have the financial wherewithal to fund and support long-term and large projects like StuxNet. Shorter term events, such as activist group Anonymous hacking websites of major U.S. financial firms, are limited due to lack of sustained interest and funding. The engagement of other elements, such as motivated citizens, universities, private corporations, and para-military units are still framed under a state-based rubric and are considered by skeptics as constituent components of a state's cyberpower, its ability to leverage domestic resources in pursuit of its international political goals (Klimburg, 2011). While these elements appear independent to outsiders, they are assets deployable by and beneficial to the state.

Effects: Skeptic scholars contest the alarmist claims that cyberwar has the potential to be an existential threat to states (Evegeny Morozov, 2010). Concerns over about lax security and vulnerabilities in critical national infrastructure are tempered by assertions that exploiting those vulnerabilities requires expert knowledge which few individuals have (Rosenfield, 2009). Critical infrastructure, they argue, has emergency measures in place for malfunctions or other catastrophic failures and are well-prepared to address any issues related to cyberwar (Rosenfield, 2009). The effects, if any, of cyberwar will be limited and highly localized rather than significant and widely destructive.

Geography: Alarmists posit that cyberspace is a separate and distinct domain for conflict, with effects felt in the physical world. Skeptics argue that cyberspace is another channel through which states pursue limited political aims, firmly anchored in existing political structures, an extension of the cyber-realist position (Berkowitz, 2003; Moseley, 2007). To that end, there is nothing unique or special about cyberspace – it is simply another channel through which states pursue actions associated with subversion, sabotage, and espionage (Moseley, 2007; Rattray, 2001; Yin & Taylor, 2008). Indeed, it is a channel which expands the abilities of states to engage in these lower-level actions in cyberspace with increased potential for open-source intelligence, plausible deniability, and lack of attributability. The establishment of cyberspace as a separate domain for warfighting reflects the interests of lobbyists and power elites rather than any inherent attribute of cyberspace itself (Evegeny Morozov, 2010).

Targets: In-line with the skeptic belief that cyberwar is of limited scope, its targets are of limited scope as well. StuxNet, although its ultimate target was the nuclear reactors, had as an intermediary target a human being who could transport the malware onto the air-gap secured Natanz network or who could be sufficiently targeted via phishing (Gross, 2011). Other skeptical forms of cyberwar (espionage, subversion, sabotage, or disruption) require human failings or specific expertise to succeed, and only then can any secondary effects manifest. The restricted sense of cyberwar offered by skeptics limits cyberwar's targets to individuals which represent the weakest link and most easily exploited target in cyberwar.

Summary: Skeptical scholars argue for a less Hobbesian worldview than alarmists, and question the saliency of claims that cyberwar is imminent or an existential threat. Cyberwar exists as discrete components – espionage, sabotage, or subversion – and focuses less on destruction and more on disruption (Klimburg, 2011). However, these actions are expensive and require specialized knowledge, limiting them to being supported by states exclusively. Because of high barriers to entry and the precautions already in place in most national critical infrastructure projects, the effects of cyberwar are limited and local, not widespread chaos. Although cyberwar can have limited physical world effects, it does not constitute cyberspace as a separate warfighting domain. Cyberspace is an extension of the physical domain and political actions which occur in it. The existence of the domain reflects lobbying efforts by cyber-security firms, and functions as a conceptual creation of military and policy elites (Evegeny Morozov, 2010).

Skeptical claims center on research which demonstrates that the cost of attack, such as StuxNet, could only be borne by a state or that case studies demonstrate the lack of explicit physical violence and harm from cyberattacks. For instance, Rid (2012a) claims that the aforementioned *Moonlight Maze* doesn't represent a case of cyberwar or existential threat to a technologically-dependent and unprepared United States. Rather, it is simply an example of cyberespionage. Likewise, the attacks on Georgia and Estonia by Russia (Rid, 2012a) whose use of rented botnets, malware, and website defacement simply represent, to skeptics, a nuisance rather than any existential threat.

The skeptical position has recently found greater resonance in popular media (Rid, 2012b; Schneier, 2010; The Economist, 2012). The lack of any significant domestic cyberwar event, despite considerable hype by alarmists, has contribute to greater skepticism amongst these groups that cyberwar – as envisioned by alarmists – will occur. National security experts continue to argue for a more alarmist-based position but temper these warnings with some consideration from skeptical scholars, emphasizing the idea of cyberwar as disruptive rather than destructive (Gjelten, 2013a).

Realist

The third theme in cyberwar literature involves scholars and practitioners who emphasize that cyberwar exists within a modified realist framework (Manjikian, 2010). These scholars do not dispute the fact that some form of conflict exists in cyberspace nor do they dispute that its structure and components are contentious. Rather, these scholars see it as a conceptual, practical, political, and legal frontier which can be understood within existing state practice and international legal structures (Nunes, 2005). In other words, cyberwar does not represent something fundamentally new, nor is it something which doesn't exist or can be classified away (Krishna-Henzel, 2007). Instead it must be understood or viewed through the lens of the current international system.

Actions: Realist scholars do not make distinctions between expensive or complicated actions and cheap or widely available ones. Actions are seen as precipitating an understanding of the legal and state behavior contexts in which they should be properly situated – only then can they be understood (Yurcik, 1997). The content of the actions is not of primary importance, instead it is the extent to which actions can be categorized and framed within existing structures. To an extent, this is an argument which echoes skeptical contentions about the nature of cyberspace and actions in it, but instead reframes that analysis by situating the debate not within concepts around information content and travel. Rather, realists see debates as centered around definitional ambiguity and a tendency towards a “metaphysical” view of cyberspace and its actions.

Actors: The realist conception of actions lends itself to a broad conception of cyberwar – individuals, non-state actors, states, social movements, corporations, and others can all freely engage in cyberwar (Lachow & Richardson, 2007; Nunes, 2005). This is an actor-centric specific model which places emphasis on individual actors, groups, and networks in cyberspace rather than restricting or limiting who is or isn't a legitimate actor. Thus, a highly motivated individual could conceivably engage in cyberwar, as well as a state or a transnational social movement (Moseley, 2007). What is important, rather, is the way actors relate to each other within the broader context of the existing international system and how that system's norms and guidelines reflect and are able to include those actors.

Effects: At its core, the realist position is concerned for the implications of conflict in cyberspace for existing international law and politics. The effects may be disruption, destruction, subversion, espionage, or sabotage but the impact is ultimately felt on future interactions between individuals, groups, political and financial structures, and intellectual property and trade regimes (Campen, Dearth, & Goodden, 1996; Moseley, 2007). The effects of actions in cyberspace are less associated with the actors than with the broader system, and the worlds which such actions can enable (Winner, 1989). Thus, understanding where a state begins in cyberspace or how to interpret StuxNet in light of the United Nations charter are the effects of hostile actions in cyberspace (Nagl, Amos, Sewall, & Petraeus, 2008).

Geography: The realist position sees cyberspace as a domain where unique actions take place, but those actions are grounded by physical, political, and legal geographies (Milone, 2003; Rattray, 2001). It is indistinguishable from the existing international system and must be seen, evaluated, and acted upon as an ordinary feature of the world. This perspective would contest the U.S. Department of Defense understanding of cyberspace as a separate warfighting domain or the skeptical position that cyberspace is only a proxy or cultural metaphor for physical space. There is nothing which occurs in cyberspace which is not intimately entwined with geography and the rights, rules, and obligations which that entails.

Targets: The primary focus of cyberattacks are any and all elements and assets which can exist within bounded sovereign territories and internationally-recognized legal jurisdictions (Moseley, 2007). This includes individuals, corporations, military networks, and government computers, which will be situated within existing international legal structure. What is relevant is less the targets but the legal and conceptual situation of those targets, specifically as they relate to international law.

Summary: Realist scholars are concerned with the implications of conflict in cyberspace on existing international law and state practice. The precedents established by actions can have unforeseen consequences for international stability and careful analysis must be undertaken to properly situate these actions within broader and existing logics (Barkham, 2001; Greenberg et al., 1998; Hathaway et al., 2011). Thus, for realists cyberwar is not unique nor does it not exist, rather it represents a specific way in which actors within certain legal jurisdictions interact which serves to legally guide future interactions. To that extent, realists are less concerned with whether actions are cheap and widely available or expensive and technically demanding. The actions can be both, and likewise the actors need not only be states. States are relevant insofar as they serve as the structure for the international system and the legal implications of actions between or within them has direct bearing on the structure of the system as a whole. Cyberspace, therefore, is not a separate domain which exists apart from the real physical world nor is it a domain which is only a conceptual proxy for physical space. Cyberspace is firmly grounded in the world and actions which occur within cyberspace are indistinguishable from actions which occur outside of it.

The realist position is largely composed of legal scholars and academics who see the debate between alarmists and skeptics as focused on language and classification rather than on understanding actual events. Whether or not cyberwar exists is seen as an issue relating to how cyberwar is defined rather than centered on what is occurring in cyberspace at present. StuxNet, for example, may or may not be an act of cyberwar or simply one of sabotage, but the development and deployment of a technology which can destabilize nuclear reactors without proper attribution and within a legal structure to situate the actions within international law represents a threat to international stability. In addition to StuxNet, realist scholars emphasize the changes associated with concepts of neutrality, such as the relocation of official Georgian state digital assets to a neutral state - the United States - during the 2008 cyberwar (Korns & Kastenberg, 2008) and its implications for neutrality. In both examples, realists are interested in interpreting events within existing international conventions rather than seeing whether cyberwar exists or is an immediate existential threat.

Three Perspectives – Conclusion

These three perspectives represent the dominant narrative threads in the literature on cyberwar. Despite the presence of significant definitional ambiguity, specifically international law and cyberwar, preparation for cyberwar amongst states continues apace, with billions of dollars spent on training, zero day exploits, and the establishment of cyberwar units within various state militaries and security services. Likewise, non-state actors continue to remain a potent force for the discovery of zero-day exploits, deployment and development of malware, and for their ability to be harnessed for DDoS attacks.

The lack of a consensus definition does not preclude the existence of a situation which necessitated the broad scholarly effort at defining cyberwar. Regardless of definitional ambiguity, there are actions and events occurring in cyberspace which can be associated with state conflict and hostile engagement. These three perspectives seek to situate these actions and events within cohesive frameworks which can be used as a conceptual tool to understand those actions and events. To that end, any discussion of cyberwar must articulate a definition of cyberwar which acknowledges these three perspectives.

The alarmist position acknowledges that there are threats and dangers associated with the spread of the Internet and lax security protocols and policies. By drawing attention to inconsistent security protocols, real and on-going hacks and attacks, and the investment by other states in cyberwarfare capabilities, the alarmist approach seeks to effect changes in both policy and practice. In doing so, the alarmist position uses older geopolitical logics which situate the United States and Western world as imperiled from Islamic and formerly/current Communist states.

The skeptical position cautions policy makers to avoid escalation in pursuit of nebulous or perceived threats, specifically highlighting the alarmist position as questionable. Skeptics argue that threats are overstated and that robust security precautions already exist in critical national infrastructure. While acknowledging that threats do exist in cyberspace, skeptics argue that they are manageable and less serious than alarmists make them out to be.

Finally, the realist position attempts a middle approach. It does not deny that critical threats exist, but rather that the nature of those threats has implications for the international system. These threats are not separate from conventional politics or the offline world, but are an extension of it and must be seen as situated within a spectrum of broader conventional threats which states face. This approach seeks to engage more directly with the nature of what actions are occurring in cyberspace and how those actions can be classified and understood in contemporary international law and state practice rather than on the size or scope of threats which exist or philosophical debate.

Each of these perspectives also obscures when they seek to clarify. Alarmist positions obfuscate the multiplicity of actors and the size and scale of threats under a Cold War type geopolitical logic. Skeptics situate cyberwar as an overstated concept, obfuscating the significant financial investments by states under a rubric of mis-classification of conflict. In an effort to strengthen international law, realists tend to hide the new and novel aspects of cyberwar.

Understanding the three perspectives in terms of actions, actors, effects, geography, and targets also allows for limitations to these three perspectives to be isolated and a definition crafted. A nuanced understanding of cyberwar sees the limitations of each perspective and is not locked into the ideological or political battles which have characterized the field.

Cyberwar: A Definitional Compromise

The three perspectives provide a theoretical foundation for understanding cyberwar. The definition used in this dissertation sees cyberwar as actions undertaken by states to alter information, disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. This definition can be understood within the categories used to understand the alarmist, skeptic, and realist positions.

Actions: In line with skeptical positions, the actions associated with cyberwar are expensive and complicated. Critical infrastructure has well-established protocols and procedures for dealing with emergency situations (Rosenfield, 2009). Further, to seriously hamper or disrupt a state's physical or communicative infrastructure requires specialized knowledge and access to advanced plans or technical specifications, precluding all but the most well-funded and technically sophisticated cyberwar organizations. Other acts, such as website defacement or lower-intensity DDoS have become commonplace enough to be understood as forms of civil resistance (Sauter & Zuckerman, 2014) or non-violent protest (Oliva, 2013) rather than acts of cyberwar which are highly destructive or significantly disrupt key communications infrastructure.

Actors: Cyberwar can only take place between states. The skeptical reasoning emphasizes the costs and complexities of cyberwar as the rationale behind limiting any notion of cyberwar to states. Non-state and other actors lack the resources to develop the types of attacks needed to harm critical infrastructure or disrupt communications. To date, the best known actions associated with cyberwar have required the explicit or implicit support of states to succeed and as global investments in cybersecurity continue to increase complexity and the technical sophistication needed to launch successful attacks must increase (Gross, 2011, 2013; Rosenfield, 2009).

Effects: The sophisticated security precautions and complex insider knowledge which skeptics argue precludes serious destruction is embraced, implying that cyberwar is primarily disruptive rather than physically destructive. Skeptical scholars have argued that the nature of violence in cyberspace is different than in the offline world (Stone, 2013), and that attempting to ground cyberwar a framework of violence to which it is not suited is counter-productive. Disruptive acts, such as the Syrian Electronic Army hacking the Associated Press' Twitter account resulting in over $130 billion in losses on the S&P 500 index (Foster, 2013) should be seen as a model for a redefinition of violence and its effects in cyberwar rather than continuing to ground the idea of violence in cyberspace on kinetic violence more suited to tanks and bombs rather than keyboards and bytes.

Geography: Cyberspace is a separate domain with protocol-based limitations (DeNardis, 2009) which govern which actions can or cannot exist online. However, that domain does not exist separate from its physical and political geography – as argued by the U.S. Department of Defense: “Although cyberspace is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space” (Gates, 2010, p. 37) which links cyberspace to other physical domains, regardless of any human-made attributes. Cyberspace as a warfighting domain entails different rules of engagement predicated upon the technical limitations of the domain. Certain actions can take place in cyberspace and others cannot, and this provides a technical boundary to the geography of cyberwar. At the same time, however, Internet filtering, legal allocation of Internet infrastructure to states, and transnational Internet data transit agreements (Cowie, 2011) situate the Internet within broader geographical contexts where Internet traffic is altered or contingent upon the geography from which it originates or crosses.

Targets: The targets of cyberwar will be elements of national cyberpower. The three perspectives each seek to segment targets of cyberwar into discrete categories. These components, such as corporations or government computing systems, when viewed geographically are constituent elements of a state's general cyberpower, a term developed to include those domestic elements which allow states to project power in cyberspace internationally (Kuehl, 2009b). Cyberpower can include private corporations, military networks, talented individuals, universities, security organizations, and social or political citizen movements (Klimburg, 2011). In terms of present actions, the targets of other states have tended to be large and critical corporations, government networks, universities, and key private individuals (Arquilla, 2012; Arquilla & Ronfeldt, 1993; Clarke & Knake, 2012). Thus, the targets of cyberwar have historically and are at present elements of cyberpower.

Examples of the definitions of cyberwar offered in this dissertation form the basis of chapter 5, and include the cyberwars which pitted Russia against Estonia in 2007 and Georgia in 2008, as well as the cyberwar between Iran and the United States from 2010 to the present. In each of these cases, the actions taken by states alter information, disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. Table 3, on the following page, summarizes the three perspectives and also includes the definition argued by this dissertation.

Expanding the definition

This definition of cyberwar seeks to incorporate elements from the various perspectives so as to overcome limitations in their reasoning and structure. This definition makes a number of assumptions:

Cyberspace engenders different and contextually relevant understandings of force and violence.

Throughout the historical development of literature attempting to define cyberwar, alarmist scholars have emphasized the physical vulnerability of states to cyberwar as a motivating factor for increased investment and awareness. Skeptics such as Rid (2012a, 2013) believe that this lack of explicit physical violence precludes cyberwar from being a coherent concept. On the other hand, Stone (2013) has argued that traditional notions of violence may not pertain to cyberspace. That is, cyberwar as a technical series of actions should be seen an evaluated on its own technical terms rather than bounding it within conventional non-digital forms of violence. The idea of disruption as cyberwar's main aim derives from Rogers’ idea that actions within technical systems need to be understood within those systems in terms of scope, potential, and effects (R. Rogers, 2010, 2013).

Skeptics argue that both physical and digital violence must be understood in the context in which it is situated, and thus information or financial disruption rather than physical destruction is closer to the “nature” of cyberwar. This dissertation's definition of cyberwar embraces the view that disruption is the primary focus of cyberwar.

Question	Explanation	Alarmist	Skeptic	Realist	*Dissertation*
Actions	Nature of hostile actions in cyberspace	Cheap and widespread	Expensive and complicated	Both	*Expensive and complicated*
Actors	The “legitimate” actors in cyberwar.	Anyone/anything; final responsibility is with states	States	Anyone/anything	*States*
Effects	Possible effects of cyberwar	Large-scale disruption or destruction, military decapitation	Small-scale, local disruption	Legal implications for international state system and cooperation	*Large and small-scale disruption*
Geography	The constituent elements of the theatre(s) where cyberwar takes place.	Cyberspace is separate, but may intersect with physical space	Cyberspace is only proxy for physical space	Cyberspace and physical space are legally and practically indistinguishable	*Cyberspace is separate, but intersects and is part of physical space*
Targets	The targets of cyberwar.	Critical state or military infrastructure/information	Human beings	Military targets, individuals, corporations, states	*All elements of national cyberpower*

Table 4: Alarmist, Skeptic, and Realist positions and the dissertation’s definition

Acts of cyberwar occur within a spatiality of power model rather than falling under strict territorial geographies.

The spatiality of power model (Agnew, 2003) argues that power need not be vested in only the territorial state. Power, in this understanding, is decoupled from the territorial state and has varied throughout history based on changing technologies and political-economic structures.

Power's spatiality is historically contingent, and Agnew (2003) proposes several historical models: ensemble of worlds, field of forces, hierarchical network, and the world society. While the other models are discussed elsewhere, the world society model sees power at a global scale and global-scale problems (such as climate change) organized in a network-like structure.

In order to function, the Internet's resources, such as webservers or content delivery networks, are distributed and function in a way which largely ignores territorial state boundaries through the BGP protocol (Roberts et al., 2011). From a technical standpoint, the distribution of these resources resembles a “world society” spatiality of power model. These acts treat and see the Internet as globally contiguous, ignoring borders and with certain spatialities configured in ways more suited towards cyberwar while others are less infrastructurally conducive.

Cyberwar can only occur between ICANN/IANA recognized states.

Technical resources allowing global connectivity are allocated by two organizations: the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA). Both of these international organizations assign the technical resources which allow IP addresses and domain names to work worldwide, facilitating global connectivity. These organizations, therefore, have assumed some level of state sovereign powers (Agnew, 2009a) by having the power to allocate resources to sovereign states. Although cyber-resources exist and function along a spatiality of power model, formal cyberwar can only occur between states recognized by ICANN and IANA due to the way in which these organizations allocate resources to states. The *prosecution* of cyberwar and the *existence* of resources function along lines of a world society model, but the *allocation* of resources exists within a strictly territorial sense.

Cyberwar includes actions which are purposely intended to alter information, or disrupt computer systems, computer networks, or devices/information controlled or hosted by a computer. It can occur in lieu of, in concert with, or apart from kinetic conflict.

This final definition seeks to address claims by skeptics and alarmists on the nature of targets as a means to define cyberwar. The emphasis is on the intention of states to disrupt computer network functioning through disruptive acts or through acts which alter information. At core is less the idea of disruption rather than destruction as the digital translation of kinetic violence (Stone, 2013) – repurposing the notion of violence in cyberspace and seeing disruption as its end result. This definition avoids conflict over defining physical violence and separating sabotage, subversion, or espionage from cyber-actions by emphasizing the intentionality of the act and its disruptive potential and reality.

Limitations

This definition attempts to offer a compromise between the three perspectives. Despite this effort, it nevertheless has limitations and makes assumptions about cyberwar and cyberspace, and is thus subject to contention. Any definition, by its nature, represents compromises. In order to acknowledge this contention and the compromises made, the following section will address the following assumptions on cyberwar. Note that these are in no way all-inclusive or exhaustive, and represent an initial foray into critique of the definition offered in this dissertation:

1. War, violence, and other hostile acts can be re-classified and defined based on cyberspace's limitations and allowances.

2. A “state” can exist and act in cyberspace.

3. States engage in hostile acts against each other in cyberspace.

Efforts to define or categorize human activity or philosophies of technology involves bias, perspective, and judgment. Definitions are therefore rarely neutral, representing a limitation of language to accurately describe the world. Thus, any definition is inherently incomplete yet represents a possible method of understanding complex phenomena. To that end the definition offered in this dissertation makes assumptions and is itself limited. This definition must be seen as reflecting a geographical vision of cyberspace rather than a perspective emphasizing policy or military studies. While more than the above definitional assumptions exist, these assumptions highlighted represent high-level assumptions which must be addressed.

1. War, violence, and other hostile acts can be re-classified and defined based on cyberspace's limitations and allowances.

Cyberspace is a “man-made domain” (Gates, 2010) which exists as a function of various technical protocols and physical infrastructure. The Internet's early engineers coded and developed protocols which would allow for electronic communications to be organized, transported, and decoded in line with a certain vision of how information functions and flows. These protocols allow for information to be segmented and transported, facilitating Internet filtering but at the same time facilitating encryption technologies to break that filtering. At the same time the development of information segmentation facilitated sophisticated cyberattacks such as “man-in-the-middle” and DDoS.

No consensus international definition of war exists. The UN charter only articulates when self-defense is warranted while international law emphasizes the conditions which precede war (*jus ad bellum*) and limits behavior during a state of war (*jus in bello)*. International organizations and academics have attempted to define war based on varying criteria, but have been unable to, demonstrating the contentious nature of understanding war and violence. This ambiguity implies a lack of clarity surrounding what constitutes war and violence conditioned upon external conditions or broader context (Stone, 2013) and allowing for cyberspace to be seen as a domain in which forms of warfare and violence (Schmitt, 2013) can take place, given appropriate contextual conditions. War and violence, contentious topics outside the scope of this dissertation, are situated within broader contexts which makes their prosecution and existence problematic from a definitional standpoint. The lack of clarity shows these as concepts rather than rigid, clearly demarcated definitions, facilitating their translation and adaptation to cyberspace. This ambiguity, therefore, lends itself to being able to redefine war and violence within the structural and technical limitations of cyberspace.

2. A "state" can exist and act in cyberspace.

The notion of what constitutes a state and its role in cyberspace has been contentious since the development of the Internet. The Internet's early development was fueled by a desire to maintain and protect the United States as a state-entity (Aksoy & DeNardis, 2007) by allowing certain functions of the state to continue after a nuclear attack. However, as the Internet's development and growth moved beyond academia and government institutions its ability to easily transcend boundaries and connect disparate peoples facilitated ideas surrounding the "death of the state" and the "end of geography". The Internet became perceived as so large and complex that it was something which humans could no longer understand, allowing for virtual worlds to be posited as legitimate alternatives to the physical world. These are places where individuals could assert new identities and safely challenge existing power structures (Manjikian, 2010), transcending physical and geographical limitations.

Political geographers, political scientists, and other academics have wrestled with how best to define a state, and how much of that definition is rooted in conventional territory. Despite this difficulty, legal scholars and international law itself demonstrate that the state can exist as an entity in cyberspace through its jurisdictional and technical authorities. Its jurisdictional authority allows the state to access a form of “digital territory” in cyberspace where activities occuring on its portion of the Internet are subject to its laws. At the same time, ICANN/IANA assign technical resources to states and recognizes their configuration of autonomous systems (Roberts, Larochelle, Faris, & Palfrey, 2011) which allows states to have significant power over the Internet, including the power to complete disconnect from global cyberspace within their physical territory, articulating some form of state territory in cyberspace.

3. States engage in hostile acts against each other in cyberspace.

States generally do not disclose their hostile actions or Internet filtering in cyberspace (Deibert, Palfrey, Rohozinski, & Zittrain, 2008), and the plausible deniability afforded by the Internet and various encryption or anonymity tools facilitates this. When hostile acts are detected or occur, states have claimed that these are the actions of patriotic/private citizens and cannot be the responsibility of the state. Despite the lack of clear and unambiguous statements implicating states in hostile acts, some countries, like Iran or China, boast of their cyberwar prowess and ability to launch devastating attacks should the need arise.

This represents a limitation as the existence of cyberwar between states must be inferred from existing data, academic and security research, and public-facing statements or documents. Regardless of the lack of clear and decisive attribution, the body of cyberwar literature and empirical research is in agreement that states are active agents in cyberspace and often engage in hostile acts against one another.

These assumptions highlight the limitations of efforts at defining cyberwar. Significant questions and concerns surround the nature of the state, violence, and attribution in cyberspace. These are augmented by difficulty in the definition of cyberwar offered in this dissertation in the blurring of kinetic and non-kinetic conflict as well as its general high level of inclusiveness.

Conclusion

Cyberwar is an ambiguous concept subject to competing definitions and claims spanning academia, government, international law, and policy circles. As a result, no clear definition of cyberwar exists which is broadly agreed upon. Any effort to research or understand cyberwar must therefore engage with the definitional ambiguity of the field and offer a definition which frames and limits what can or cannot be discussed. This is due, in part, to alternative claims ranging from cyberwar as an immediate and urgent existential threat to claims that it does not exist at all.

This chapter first highlighted the efforts to establish a definition of cyberwar through briefly examining international law and key scholars. The claims made also offered contentious examples conflating cybercrime, cyberterrorism, and cyberespionage with cyberwar itself. These concepts were discussed and outlined for their practical differences from cyberwar and their existence as separate concepts articulated.

Three broad positions in the cyberwar literature were identified: alarmist, skeptic, and realist. The alarmist position is the oldest and was strongly articulated at the dawn of awareness about cyberwar in the 1980s, and argues that Western states are under immediate existential threat from cyberwar due to the widespread availability of technologies and lax security standards. Skeptics, on the other hand, assert that the threat presented by new technologies in cyberspace has been overblown, and that what exists are a select, few acts which emphasize disruption over destruction. The final group, realists, are less concerned with strict definitional attributes and more about situating cyberwar within existing international and practical frameworks.

Finally, this section sought to develop a definition for cyberwar to be used in the dissertation through a survey of key themes in the literature of cyberwar. The definition asserts that cyberwar is actions undertaken by states to alter information, disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. This definition was supported through the analysis of the three perspectives. Instead of proposing a radically new understanding of cyberwar, it borrowed elements from each group to represent a composite or spectrum vision of cyberwar.

The definition to be used situates cyberwar as involving expensive, complicated actions which can only be financially supported and developed by states. The emphasis of these actions is on information and communicative disruption rather than outright physical destruction, and these actions occur in a cyberspace which is separate yet intersects with physical space. The targets of cyberwar are not restricted to government computer networks, physical infrastructure, or key individuals. Rather, the targets are encompassed within the idea of national cyberpower whereby the sum of a nation's potential cyber-assets become vital to its ability to project power abroad and protect itself domestically, and at the same time function as targets for contemporary cyberwar.

Limitations and assumptions of the definition restrict its ability to understand or explain the entirety of cyberwar. These assumptions and limitations are largely epistemological, questioning the nature of the state, violence, and attribution in cyberspace. While these limitations and assumptions are important, and are the focus of much research, they can limit the effectiveness of analysis or research on the present and ongoing phenomena of cyberwar.

Cyberwar is a contentious topic, demonstrated through the body of literature and competing perspectives. This dissertation sees cyberwar is actions undertaken by states to alter information, disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. This definition incorporates elements from the dominant perspectives of cyberwar literature, building on decades of previous research and critical while allowing for structured analysis on the competing geographies of cyberwar and Internet control in the rest of this dissertation.

The definition offered in this chapter serves as the foundation for chapters 5 and 6, both of which situate cyberwar within the spatiality of power model rather than the explicit territorial model of chapter 3. It has accomplished this by offering a composite, compromise model which incorporates aspects of the three models within existing literature. These models each offer something valuable to the perspective of cyberwar – each model has significant influence within academic, policy, and practical circles. Thus, chapters 5 and 6 are able to build upon these models through the compromise definition offered in this chapter as the spatiality of power model is explored and contrasted with the territorial model.

Chapter 5

The Methods of Cyberwar: Attack and Defense

Introduction

Chapter 4 defined cyberwar as actions undertaken by states to alter information, disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. This implies a specific construction of the state in cyberspace, such that a "state" can be understood to exist and act in cyberspace. The state finds its strongest territorial analogue in cyberspace through Internet filtering and control, an approach through which "informational sovereignty" is asserted. At the same time, the state constructs itself in cyberspace along a traditional, territorial model firmly anchored in the idea of Westphalian borders, territory, and sovereignty. Indeed, states such as Russia, China, and Iran strongly articulate the need to defend their sovereign cyberspace from foreign incursion and control, while states such as Saudi Arabia, Australia, the United Kingdom, and Egypt argue for strengthening borders in cyberspace to protect public morality by censoring objectionable content. The territorial ideal has found strong resonance in cyberspace, through its technical structure and the illusion that provides of significant control over information flows.

However, state conflict in cyberspace, known as cyberwar, is prosecuted along lines which ignore these territorial analogies. Further, the components which states leverage to prosecute cyberwar are likewise arrayed globally in ways which betray the very territorial ideals which states seek to uphold through Internet information controls. This reveals itself as a cyber-geographical gap between the ad-hoc way the international state system has attempted to assert its territorial logic in cyberspace and how those states attempt to defend their portion of that system, their sovereign territory or project power through cyberwar. The result is an illusion of sovereign control over cyberspace masked by the ways in which cyberwar and cyberpower are at odds with state territorial logic. Cyberwar and cyberpower exist less along strictly bounded territorial lines and more along a spatiality of power model which sees that power is not only vested in only the territorial state. Power is decoupled from the territorial state, shifting and changing alongside technologies and political-economic structures (Agnew, 2003)**.**

To that end, previous chapters have addressed the territorial structure of the state in cyberspace, represented by Internet filtering and control. This chapter is the first of two chapters to address the issues related to cyberwar. The purpose of this chapter is to outline the spatiality of power and discuss the methods of cyberwar attack and defense, providing the background information for chapter 6 to demonstrate how cyberwar fits within the spatiality of power model. This chapter will begin by providing a brief overview of the spatiality of power, followed by explanations of the various methods of attack and defense in cyberwar. The following chapter, chapter 6 will ground the methods of attack and defense in three case studies which demonstrate different ways in which cyberwar has manifested itself, and the means through which it is prosecuted.

The Spatiality of Power: A Brief Overview

The territorial state is seen as a bounded entity where power is pooled and used (Giddens, 1987) with this model being projected backwards into history as part of various nation-building projects . Power is portrayed as intimately tied to a specific political-geographical construct: the territorial state. However, Agnew (2003) argues that power is more fluid and dynamic, rather than explicitly linear and bounded and a spatiality of power model is can be an alternative way to understand power, space, and the confluence of the two.

Agnew believes that the contemporary geographical conditions necessitate a resurgence of geographical imagination which can be used to envision power and space apart from states and territory. In doing so the spatiality of power allows for envisioning space and power as concepts and material entities which are historically contingent upon changes in political, economic, and technological structures and logics. For example, in a more traditional, tribal society, geographically distant from other cultures, power is oriented inward towards order and the establishment or continuation of family political dynasties (Agnew, 2003). As technologies facilitate communication, contact, and engagement with other cultures at shorter time intervals, we see the emergence of a sense of "zero sum" territoriality whereby one state can only geographically expand at the expense of another.

Four separate models exist for the spatiality of power. These models (ensemble of worlds, the field of forces, a hierarchical network, and a world society) were outlined and discussed in chapter two and will be briefly re-visited below as a conceptual aid for the rest of this chapter.

Ensemble of Worlds

The ensemble of worlds approach is historically rooted in traditional or agricultural communities isolated from other societies. In this model power is spatialized through discrete spaces and directed inward towards stability and dynastic safety. Due to dominant transportation and communications technologies of the time (Scott, 2009) conceptions of space and the broader world were oriented towards a "strongly physical conception of space as distance to be overcome or circulation to be managed" (Agnew, 2003, p. 129).

Field of Forces

Technological and political development contributes to the modern notion of the territorial state. Communications, measurement, and transportation technologies enable a level of uniformity, surveillance, standardization, and control over previous conceptions of space as distance. The territorial rigidity of states is part of a world carved up and divided amongst powers vying for control of a limited territorial pie. States become seen as containers for society and the laws, traditions, and norms associated with society (Agnew, 2003). Power is thus embodied and contingent upon territorial divisions and designations.

Hierarchical Network

The general shift of human populations away from rural areas towards cities has resulted in a spatial reconfiguration of power. Cores and peripheries/hinterlands emerge as global power centers for financial and information flows, and a respatialization and integration of hinterlands into manufacturing and extraction re-aligns remote regions with global capital. The emphasis is on geographically concentrated nodes "connected by flows of people, goods, capital, and information" (Agnew, 2003, p. 131). Power, in this model, is vested in nodes which serve as centers or strong influencers in these global flows. Thus, proximity to geographical place vis-à-vis nodes establishes a hierarchy of power – with more power vested in spatial configurations and locations which embody more "flow power".

World Society

The emergence of a global information commons (Choucri, 2012) has facilitated the spread of transnational, global identities and cultural affinities. A global commons, in other words, facilitates the development of global issues such as climate change or globalization (Agnew, 2003; Choucri, 2012), further impacted by significant variance in spatiotemporal elements of human activities. The modern world, with the existence of a global "public consciousness" has much in common with a world society. In this sense power is spatialized through its ability to pool and migrate across networks and through the vector of a global commons whereby issues emerge, are debated, and subside.

Spatiality of Power – Conclusion

The spatiality of power models are ways of envisioning power as distributed in historically and materially contingent spatial configurations. As demonstrated in the brief review above, power is articulated in different ways contingent upon political and technological development. Traditional societies, limited in spatiotemporally variable technologies (communications and transportation, for instance) situate power inwardly. A world society model, on the other hand, situates power within global public opinion and a reliance upon that power to flow across political boundaries.

Its relevance to this chapter is in its structure as seeing power as arranged in an alternative model, away from strictly bounded territorial states which have dominated geopolitical discourse since the 19th century. Cyberpower, the sum total of a state's offensive and defensive capabilities in cyberspace and its ability to leverage those capabilities during cyberwar (Klimburg, 2011; Kuehl, 2009b) operates along the lines representing a spatiality of power approach. The multiplicity of actors which comprise a state's cyberpower are geographically disparate, subject to different laws and structures and arguably embody different aspects of each of the four models. Cyberwar, a manifestation of state cyberpower, likewise operates from a grounded base in the spatiality of cyberpower – resources and operations are ageographical with vital national interests being disaggregated from territorial states.

The case studies presented in this chapter illustrate the ways in which power and conflict manifest along lines which ignore conventional state boundaries and embrace alternative spatialities from each of the four models. In order to understand how cyberwar is fought, however, it is vital to understand the means and methods of attack and defense. The technical protocols (DeNardis, 2009; Golumbia, 2009) of the Internet both enable and limit action, and serve as the rules-bounded space in which state action occurs. Thus, the means and types of attacks which can occur in cyberspace, and the defenses against these attacks, are definable, offering a way in which cyberpower and cyberwar can be seen within the spatiality of power model. It is important to note that these categories are by necessity guides rather absolutes, and offer broad “bird’s eye” views on these methods. The next section begins with an overview of the types of attacks used in cyberwar.

Attack methods

As defined in chapter 4, cyberwar is a group of actions undertaken by states to alter information, disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. These actions are defined and limited by the technical protocols which underlie the Internet. As states engage in cyberwar, they utilize a variety of different attacks and techniques in order to achieve their political goals, be they outright domination, disruption, or control.

This section outlines the types of attacks which states use to engage in cyberwar. It is followed by a section on defensive techniques, and then three important case studies which demonstrate both the techniques used by states and ties in these techniques within the broader spatiality of power model.

Types of attacks

The earliest cyberattacks were perceived as physical threats to the computers and data centers which powered the early Internet and military intelligence services (Warner, 2012). Early computers were utilized and conceived of as digital "filing cabinets", embedded within logics of violence primarily oriented around physicality, space, and presence. Thus, early reports and efforts at attacks and defense revolved around a computer's physical security.

The National Security Agency (NSA) quickly identified security concerns associated with allowing contractors to utilize their computing resources in the late 1960s. As computing resources were scarce, other agencies often utilized the NSA's computers to perform a variety of computationally-intensive tasks. The high level of demand was initially addressed by allowing for remote terminal access to the NSA's computers. In 1967 the NSA's Bernard Peters, director of the RYE system for remote terminals, declared that security cannot be guaranteed when users are allowed to remotely access terminals (Warner, 2012). In 1967 Willis Ware, member of the NSA Scientific Advisory Board and researcher at the RAND institute supported Peters' assertion stating:

> "With the advent of computer systems which share the resources of the configuration among several users or several problems, there is the risk that information from one user (or computer program) will be coupled to another user (or program)." (Ware, 1967, p. 279)

In fact, just a year after Ware's statement, West German police arrested an East German spy at IBM's regional subsidiary – the first recorded act of computer espionage (Warner, 2012). Reports on computer security were commissioned by the Defense Science Board and studies undertaken in academia to discuss the merits of significant, structural computer security. These reports provided recommendations which advocated investment in what Warner (2012) "hygiene" rather than hardware. That is, secure passwords, administrator accounts, etc. which would be software bandages to gaping security problems present in the ways computer were constructed. Path dependencies were deepened at this critical moment in computing history – due in part to the commonly-held view that computers were digital card catalogues.

As computers progressed in sophistication and networking ability, new methods of attack and defense were identified, primarily by Russian defense strategists under the guise of "information warfare". Key Russian military analysts considered information warfare to be serious enough to warrant a nuclear response (Heickerö, 2010). However, this was seen as an "unintellectual" response to the "intellectualization" of war which Russia saw taking place

(FitzGerald, 1997). Military doctrines were re-evaluated and re-developed, with cyberwar becoming a force multiplier and deterrent in a conventional conflict.

In large part due to relative parity in terms of raw destructive ability of the militaries and nuclear stockpiles of both the U.S. and Russia, cyberwar became a key opportunity to break the deadlock and advance Russian strategic interests, while at the same time acting as an effective deterrent against aggressive maneuvers by the United States. In support of this, Russia began to develop information weapons in the late 1980s and 1990s (FitzGerald, 1997), in support of their broader strategy to exploit both U.S. and western technological dependence. Among their information weapons goal was a remote-controlled virus, now known as malware and bot herding/farms, to exist by the year 2000 (FitzGerald, 1997).

Soviet analysts identified four key categories of attack, which today form the foundation of cyberwar (FitzGerald, 1997): malware, logic bombs, information disruption, and data infiltration/exfiltration.

Malware

The common experience with computer programs is beneficial: they allow us to type dissertations, edit and view photographs, search the Internet, or listen to music. However, programs can also be developed which are malicious: they can steal passwords, delete all of our data, or monitor our communications. Malware is

> "Short for malicious (or malevolent) software, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware includes computer viruses, worms, trojan horses, spyware, adware, and other malicious programs." (Coppin State University, n.d.)

Once a computer has been infected, malware can redirect computer traffic and be used to hijack basic controls, enabling the creation of “botnets” vital to DDoS attacks. It can adapt or be changed remotely, delete itself, or remain for years gathering and transmitting information back to its developers.

Malware is vital in developing and establishing long-lasting connections between geographically disparate attackers and victims, and facilitating the development of international botnets designed to attack websites. Malware exploits vulnerabilities within software, making the discovery of those vulnerabilities vital to both security and cyberwar. This is the key element in the malware-industrial complex where states are aggressively seeking new vulnerabilities as a way to achieve information dominance (Moseley, 2007; Yurcik, 1997). This has created a multi-billion dollar market for vulnerabilities, facilitating greater instability in cyberspace as states amass stockpiles of malware which could be deployed with devastating results for global communications (Simonite, 2013).

Logic Bombs

Logic bombs are an important component of malware, but sufficiently different in their purpose and intent that they warrant a separate classification. A logic bomb is a type of malware which has a set of specific instructions to erase all data on its host computer or to completely disable that computer's network traffic, rendering it disconnected from its local network and the global Internet (Landwehr, Bull, McDermott, & Choi, 1994). This software is implanted for use later, either as a threat or in conjunction with kinetic or broader cyberwar. For example, a logic bomb could be implanted within computer parts shipped from one country to another for use in critical industrial systems. At a predetermined time, or during a moment of heightened political tension or war, the bombs would be remotely activated, disabling the targeted computing systems.

Information Disruption

Information disruption is linked to Soviet-era military doctrines surrounding information dominance and using information war to shape the battlefield (FitzGerald, 1997; T. L. Thomas, 2000). It is a multi-purpose category including distributed denial of service (DDoS) attacks and website defacement. The purpose of these attacks is to restrict or limit the flow of information or to project cyberpower globally or to specific states.

Distributed Denial of Service attacks involve the use of multiple computers which simultaneously request a website. The enormous numbers of requests overwhelm the web server, resulting in the site and its server being inaccessible. If sufficient numbers of computers are used it can slow down general communications within a geographic region by overwhelming regional Internet bandwidth (Shachtman, 2009). Generally, DDoS is conducted as either a participatory DDoS event or through a "botnet". A participatory DDoS event involves large groups of individuals downloading specially designed software and target specific websites, as part of a broader political protest or disruptive movement (Nazario, 2009), as with the massive participatory DDoS events against Iran in support of protestors (Carr, 2009) or against the PayPal payment service protesting its treatment of WikiLeaks (Mackey, 2010).

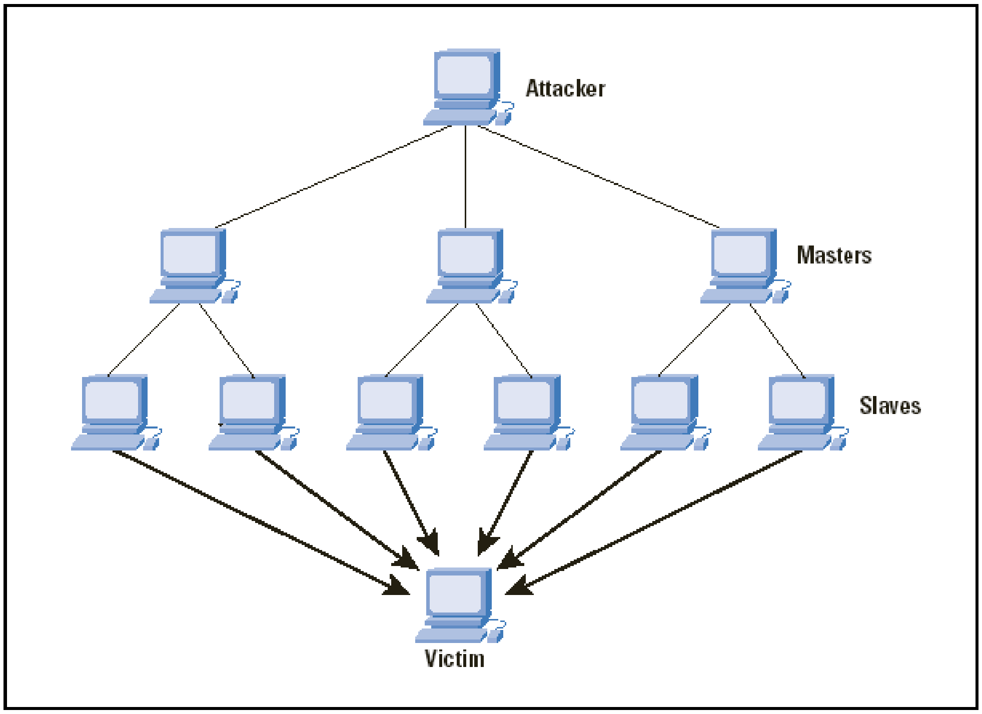
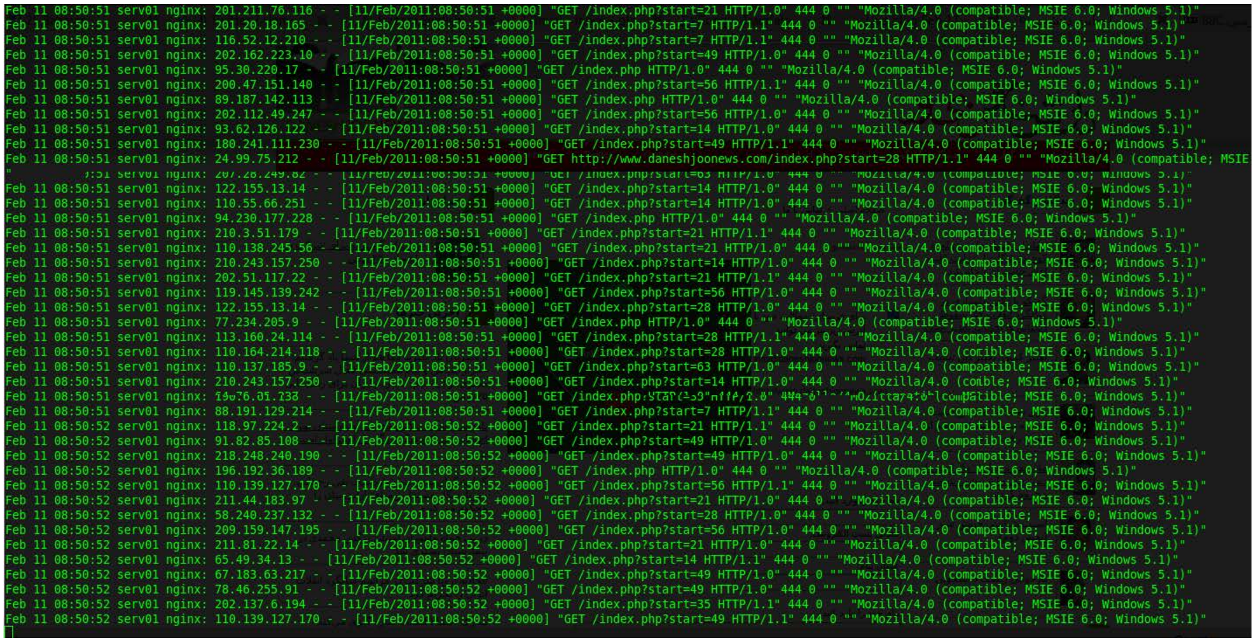


Fig. 15 –Distributed Denial of Service Attack (Patrikakis et al., 2004, p. 20)

DDoS via botnet involves infecting hundreds, thousands, or millions of computers with malware and hijacking their traffic to direct it towards attacking websites. This type of malware is often spread through malicious websites or email attachments which the user downloads and installs, erroneously thinking the file is something else (Carr, 2009). The program then turns the computer into a “zombie” for use by a “bot herder” to control at a time of his or her choosing. These botnets can exceed 1,000,000 computers and are rented out by states and non-state actors on various “dark net” black markets (Bradbury, 2014). Other states, terrorist groups, and non-state actors are customers.

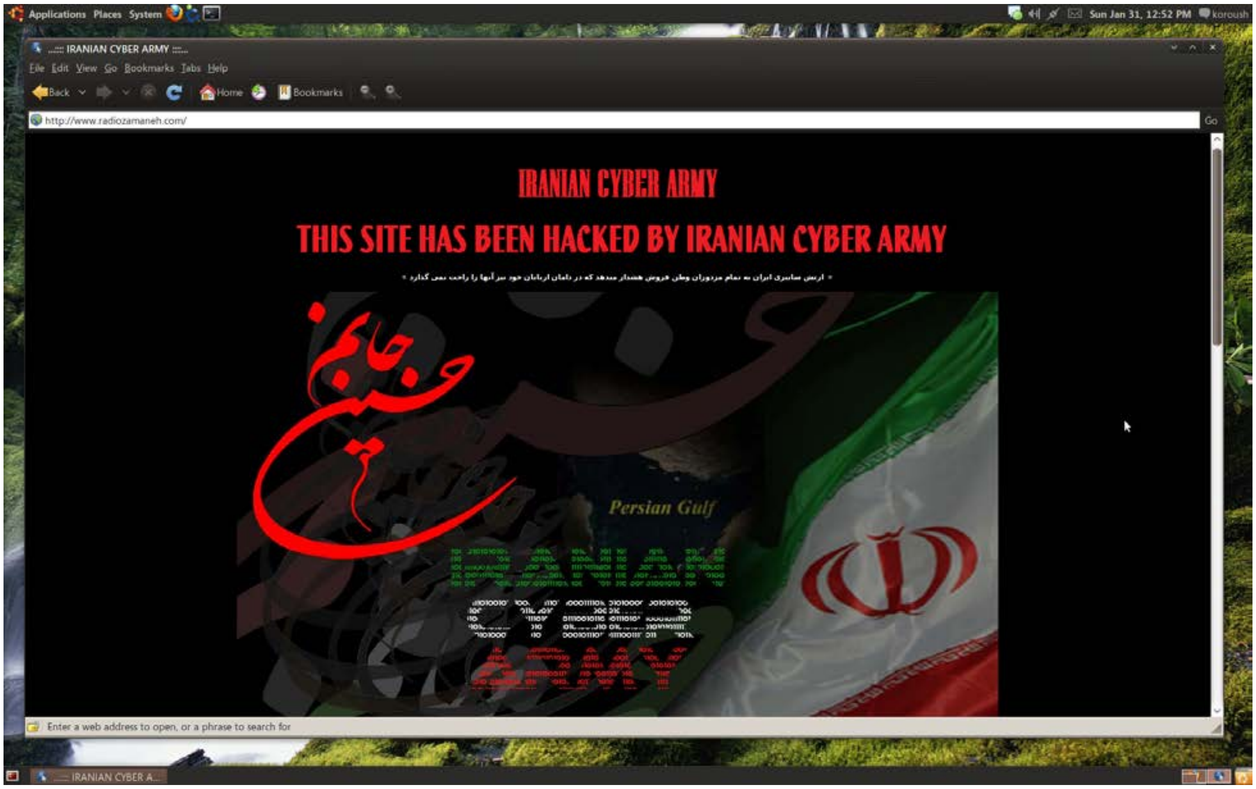


```
Feb 11 08:50:51 serv01 nginx: 201.211.76.116 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=21 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 201.20.18.165 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=7 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 116.52.12.210 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=7 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 202.162.223.10 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=49 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 95.30.220.17 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 200.47.151.140 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=56 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 89.187.142.113 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 202.112.49.247 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=56 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 93.62.126.122 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=14 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 180.241.111.230 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=49 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 24.99.75.212 - - [11/Feb/2011:08:50:51 +0000] "GET http://www.daneshjoonews.com/index.php?start=28 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE
"          9:51 serv01 nginx: 207.28.249.82 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=63 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 122.155.13.14 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=14 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 110.55.66.251 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=14 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 94.230.177.228 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 210.3.51.179 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=21 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 110.138.245.56 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=21 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 210.243.157.250 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=14 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 202.51.117.22 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=21 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 119.145.139.242 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=56 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 122.155.13.14 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=28 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 77.234.205.9 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 113.160.24.114 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=28 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 110.164.214.118 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=28 HTTP/1.0" 444 0 "" "Mozilla/4.0 (cotible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 110.137.185.9 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=63 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 210.243.157.250 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=14 HTTP/1.0" 444 0 "" "Mozilla/4.0 (coible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 14.76.01.138 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=63"HTTP/1.0" 444 0"" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:51 serv01 nginx: 88.191.129.214 - - [11/Feb/2011:08:50:51 +0000] "GET /index.php?start=7 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 118.97.224.2 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=21 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 91.82.85.108 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=49 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 218.248.240.190 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=49 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 196.192.36.189 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 110.139.127.170 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=56 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 211.44.183.97 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=21 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 58.240.237.132 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=28 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 209.159.147.195 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=56 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 211.81.22.14 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=21 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 65.49.34.13 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=14 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 67.183.63.217 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=49 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 78.46.255.91 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=49 HTTP/1.0" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 202.137.6.194 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=35 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
Feb 11 08:50:52 serv01 nginx: 110.139.127.170 - - [11/Feb/2011:08:50:52 +0000] "GET /index.php?start=49 HTTP/1.1" 444 0 "" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 5.1)"
```

Fig. 16 – DDoS attack on Iranian opposition website (Screenshot by author)

The ease of launching DDoS attacks has made them a preferred tactic for states, outraged individuals, and social movements to use in pursuit of their political goals and objectives. This has contributed to DDoS becoming widespread enough that many private firms are able to offer DDoS security and mitigation, leading to assertions that this represents a conceptual shift in DDoS. Greater security from DDoS means DDoS must now be seen as a form of non-violent protest, akin to a virtual "sit-in" rather than a hostile act within the context of cyberwar (Oliva, 2013).

Website defacement involves hacking a website to remove its content and display a message of the hacking group's choosing. It has been a prominent form of cyberattack, famous targets include the U.S. Senate's website, United Nations, and the European Union Presidency (Constantin, 2010; Deane, 1999; Keizer, 2007). Scholars increasingly see it, alongside DDoS, as a form of political protest (O’Malley, 2013; J. Thomas, 2001) rather than an outright act of cyberwar. However, the recent executive order issued by President Barack Obama for “Improving Critical Infrastructure Cybersecurity” asserts that website defacement continues to constitute a hostile act (Obama, 2013). While its effects are limited and the defacement is quickly resolved, defacement is often used as a way to expose server vulnerabilities, convey cyberpower (Carr, 2009), and gain attention for a broader political message (Carr, 2009; O’Malley, 2013; J. Thomas, 2001). Within the concept of information dominance it can be used to decrease trust in news sources, and disrupt their ability to report news at critical junctures such as during an important protest or military offensive (Deibert, Rohozinski, & Crete-Nishihata, 2012).



IRANIAN CYBER ARMY

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

« ارتش سایبری ایران به تمام مزدوران وطن فروش هشدار میدهد که در دامان اربابان خود سر آنها را راحت نمی گذارد »

Applications Places System
Sun Jan 31, 12:52 PM koroush
.::: IRANIAN CYBER ARMY :::.
File Edit View Go Bookmarks Tabs Help
Back
Home
Bookmarks
http://www.radiozamaneh.com/
Go
Persian Gulf
Enter a web address to open, or a phrase to search for
.::: IRANIAN CYBER A...

Fig. 17 – Radio Zamaneh website defaced by Iranian Cyber Army (Screenshot by author)

Infiltration and exfiltration

Infiltration and exfiltration are usually associated with cyberespionage, and in this regard are ways in which critical cyber infrastructure is compromised by external attackers. State or non-state hackers identify security vulnerabilities in vital computers and infiltrate them for the purposes of planting logic bombs or malware, website defacement, removing classified data or intellectual property, or surveillance. Infiltration, known in mass media as “hacking” is well-documented in popular culture and attracts significant amount of both popular and policy attention towards cybersecurity. However, infiltration need not be a direct relationship between an external actor and a remote computer - an attacker can compromise a remote system through using phishing or similar techniques to install malware granting remote access. Infiltration is an important element in national and international cybersecurity, and has featured prominently in popular geopolitical imaginings of cyberwar through movies such as WarGames, Sneakers, The Matrix, Die Hard 4, and others.

Exfiltration, on the other hand, leverages infiltration to remove, or exfiltrate, sensitive information or system schematics to a third party, with remote servers often located in neutral third party states in a bid towards plausible deniability. It is most commonly linked to cyber-espionage, though exfiltration can be done automatically by malware to survey a networks and systems to better plan or participate in attacks – much like the malware StuxNet did.

Attacks - conclusion

This section has outlined several categories of attack during cyberwar. These methods of attack are widely considered to be the main modes of attack in cyberwar, bound by the technical logic which underpins the Internet (Clarke & Knake, 2012; FitzGerald, 1997). These categories are malware, logic bombs, and information disruption and are broad in their conception and content. Malware is malicious software designed for a variety of purposes and to operate undetected in furtherance of a third party's goal. Malware can be used to exfiltrate information, hijack web traffic, conduct surveillance, or sabotage critical systems. Malware functions through identifying critical system vulnerabilities and exploiting them to conduct its mission. Logic bombs are a type of malware, but are designed to be implanted with a single mission and be activated later, often during times of heightened political tension or unrest.

Information disruption seeks to use DDoS, often supported by malware, to render websites and communications networks inaccessible due to tremendous traffic which overloads servers and saturates Internet bandwidth. It originated in Soviet military doctrine about the need to control information space as a means to influence both the battlefield as well as public opinion or perception.

Lastly, infiltration and exfiltration seek to gain direct access to computer systems and networks belonging to adversaries in order to exfiltrate information, plant logic bombs or malware, or for malware to determine a threat or opportunity landscape and operate successfully. Both infiltration and exfiltration can be conducted by human beings or by automated systems which automatically identify and exploit system vulnerabilities to gain access.

This section has briefly outlined four categories of attack associated with cyberwar. These categories are simplified and ignore the level of technical variability and nuance present in sophisticated cyberattacks. For example, there are multiple variations of malware each of which utilizes different technical approaches and logics to infect and spread across networks and computers. Rather than focus on technical specifications and constructions these categories offer a higher-level perspective on the types of attacks which constitute cyberwar, allowing for a broader view of how states prosecute and see cyberwar, and how defenses are constructed.

Cyber-Defense

Cyberattacks seek to exploit vulnerabilities in computer systems and technical logic in order to access systems or disrupt communications. The defender, on the other hand, must carefully observe all systems and ensure that they are secured from vulnerabilities:

> “Offensive operations dominate in cyberspace: the challenge of defense is to patch all vulnerabilities; the attacker's opportunity lies in finding only a single key vulnerability in complex systems. There are no indications that this inherent attacker advantage will change in the foreseeable future.” (Hunker, 2010, p. 4)

This creates two fundamentally different approaches and geographies to cyberwar: the attacker remains relatively footloose while the defender is increasingly static. However, recent trends have indicated that approaches to defense are changing with states emphasizing more active and automated defenses, a potentially dangerous and unstable escalation (Lotrionte, 2011).

Cyber defenses are further complicated by the multiplicity of vulnerabilities present within state territory. Government or military computer systems fall under the direct control of the state, however, critical infrastructure, financial firms, media, and millions of civilian computers are equally vulnerable yet are beyond the direct control of the state. Though advocates of robust national cyber-defense policies have emphasized enhancing the defenses of computers under the direct control of the government, the realities of a networked society mean that an infected home computer which sends an attachment to a personal work computer can result in a infection and infiltration or attack by outsiders. Thus, states must develop a conceptual model of its “defensible space”, framing the digital in geographic terms in order to understand where vulnerabilities lie and how threats will manifest.

This emphasis towards territorializing cyberspace defensively encompassed in a four-fold approach to cyberdefense: human defense, proactive measures, active defense, and national cybersecurity. Each will be briefly discussed below as a means to understand the geographies and scalar representations and metaphors which exist in contemplating defense in cyberwar.

Human

Human-scale defense rescales the concept of national cybersecurity to the individual level. This is a biopolitical approach towards cyberwar defense and security whereby the individual is deemed responsible for advanced knowledge of security protocols and for keeping all of the devices they use which are connected to the Internet updated with the latest anti-malware software. Automated email filtering systems, such as the IronPort (now Cisco) system used at major universities like UCLA, automatically filter incoming email for potential threats – removing even the option of an end recipient being able to self-determine the security of a message. This is also evidenced in university policies which automatically scan student, faculty, and staff computers which connect to the network for viruses or malware.

This approach problematizes the human and the biological in the pursuit of cybersecurity. This is grounded in case studies illustrating the ways in which advanced cyberespionage techniques such as spear-phishing (profiling and targeting users with personally-relevant malware) are used to gain access to classified information and systems. Indeed, this is believed to be the approach used for StuxNet (Gross, 2011) and remains a commonly-used approach for inserting malware in cyberwar. The mandatory use of Virtual Private Networks (VPNs), centralized organizational computing security, and organizationally mandated security refreshes and updates are representative of this trend towards centralizing security and envisioning the individual human as a security risk and problem to be solved. International deployments of corporate and government technologies likewise re-scale the concept of “national cyber homeland” (Deibert & Rohozinski, 2010a) to the individual through monitoring of emails, downloads, and web-traffic regardless of the individual's physical geographical location.

Proactive

Proactive defenses are, historically, the first conception of cyberdefense after cyberwar gained mainstream prominence. Emerging in the early 1990s, proactive defense contains a myriad of approaches towards envisioning defense and cybersecurity. Its founding philosophy is on regular, thorough testing and examination of existing security to identify vulnerabilities in order to correct them. It works against the idea of being reactive and waiting for attacks or hacks before implementing security protocols.

To that extent organizations and governments will hire or develop “red teams” whose purpose is to deliberately attack existing systems (Bendrath, 2001; White & Conklin, 2004). The origins of this specific method of cybersecurity was 1997's *Operation Eligible Receiver* where a red team created by the National Security Agency (NSA) sought to hack into vital government systems (Adams, 2001; Beidleman, 2009). The purpose of the exercise was to formally analyze the cyber security of critical computer systems in the United States, and the team of hackers was limited to only those resources which they could freely find on the Internet. The purpose of this limitation was to see how vulnerable these systems were to non-proprietary software packages or services as a proxy for a foreign state's abilities to hack domestic networks.

The results of *Eligible Receiver* were devastating. Despite over a decade of very public statements discussing the serious cybersecurity vulnerabilities the United States faces, and with significant financial and policy investments, major systems across the country were infiltrated with potentially deadly results (Adams, 2001; Beidleman, 2009):

- Power grids and 911 emergency systems for nine U.S. cities were compromised
- Complete control of the U.S. Pacific Command Center computers
- Full authorized access to 36 critical Pentagon computers, allowing for issuing orders to military units, diverting fuel deliveries, etc.

Eligible Receiver highlighted the seriousness of cyberwar to stunned U.S. military observers, who were now able to see that cyberwar could move from theory and alarm into reality. The ability to divert fuel deliveries, terminate 911 services, manipulate electricity, or issue direct military orders to units demonstrated that disruption and hacking were not the domain of curious or mischievous hackers, but rather had the potential to become major threats to the United States military with the very real potential for loss of life.

The response to *Eligible Receiver* was the implementation of defensive procedures and protocols which emphasized thorough reviews and regular testing of defensive measures. The philosophy behind proactive defenses is one of seeing systems in the same way as enemies or opponents do so as to better defend them. This approach spatializes defenses by constructing a vision of strongly bounded, territorial networks that look inward and focus on sustaining or constructing defenses against a hostile cyberspace beyond the network's boundaries. It is a highly static form of defense grounded in the specific networks which individuals use and connect to rather than, as with human security, being tied to mobile human beings.

Empirically, it manifests itself in doctrine such as the U.S. National Strategy to Secure Cyberspace (Bush, 2003) or the creation of NATO's Cooperative Cyber Defence Center of Excellence (CCDCoE) in response to the cyberwar against Estonia in 2007. These call for investments in national response teams and protocols for government agencies to ensure continuity in the event of serious cyberwar. These are conceptions of a need to monitor existing, static defenses to make them more resilient against future attack. It involves the deployment of red teams, extensive testing and patching, and in-depth knowledge of trends and patterns in contemporary cyberwar and computer security to ensure that systems defense is resilient.

Active Defense

The proactive approach to defense has recently been criticized as one whose sense of proactiveness is constructed around assumptions of *what* and *how* an enemy perceives a network infrastructure (White & Conklin, 2004). Further, despite its claim at proactiveness it is, in reality, a defensive or reactive approach which places the attacker at a distinct advantage for controlling the electronic battlefield. In other words, there is a critique against spatializing cyberspace in a way which is restrictive and closed, and which envisions a Hobbesian cyberspace outside tightly controlled and monitored boundaries.

Active defense is based on the principle that pre-emptive attack and the threat of massive cyber or kinetic retaliation represents a way to move defense out of a static and state-framed territorial mindset towards one which sees fluidity in global cyberwar and shifts the advantage to the defender:

> "You can never win a fight, whether in a boxing match or a war, by only taking defensive actions," says Dmitri Alperovitch, CrowdStrike's [an active defense cyberwar consulting firm] co-founder. "If you're just standing up taking blows, the adversary will ultimately hit you hard enough that you fall to the ground and lose the match. You need to hit back." (Gjelten, 2013b)

The principle of active defense argues that both states and private organizations must move beyond preparing only static defenses designed to stymie or slow an attacker. Instead, they must augment their static defenses with robust countermeasures which revolve around counter-attacking an adversary or disrupting their networks in such a way as to make any form of attack costly and counterproductive (Kugler, 2009). Further, in certain circumstances counterattack may require moving beyond cyberwar and towards kinetic strikes against physical targets housing infrastructure used in cyberwar, a position endorsed by the U.S. Air Force (U.S. Department of Defense, 2006).

Active defense has its philosophical roots in mutually assured destruction (MAD), a means through which an attacker would be ensured of significant and catastrophic damage in the event of a nuclear attack, an attempt to maintain a balance of power through the balance of terror. Active defense arguments are in the same vein, centered on making attacks costly or counterproductive for the attacker, the logic being that this would serve as sufficient deterrent facilitating greater security and stability in cyberspace. It has most recently manifested in cyberwar literature with the unique and original word “cyberdeterrence” generating substantial literature and debate (Harknett, 1996; Kesan & Hayes, 2011; Kugler, 2009; Libicki, 2009).

However, critical scholars have argued that active defense, instead, promotes a Cold War-esque arms race as each side will not try to have its actions restrained in cyberspace due to active defenses. Instead, these states will invest in and develop more sophisticated cyberweapons to circumvent passive and active defenses. Indeed, this is seen as one of the foundational aspects of the multi-billion dollar “malware industrial complex” whose ultimate contribution thus far has been to rapidly facilitate a more unstable and insecure cyberspace by pouring money into identifying and publishing sophisticated computer exploits (Simonite, 2013).

Regardless of critiques, active defense functions through three key elements, which Kesan and Hayes (2011) argue are detecting, tracing, attacking. Detecting attacks requires passive or static defenses to be robust enough to detect and log incoming attack packets and that these logs remain secured in some way from the attacker. Tracing requires the use of advanced digital forensics to trace the attack path back to the attacker, and can also involve inference or guess-work – a significant critique of active defense mechanisms (Caton, 2012). Finally, attacking involves launching a counterstrike against the identified or presumed attacker designed as either punishment or mitigation in the face of ongoing, sustained attack.

The traditional approach towards active defense requires a significant time lag as anonymizing technologies and traffic obfuscation can make the digital forensics discussed in Kesan and Hayes (2011) time-consuming and costly. This has contributed to a move towards rapid defense systems which can respond quickly and ensure that the cost of attack is high for the attacker known as automated active defense, which represents a new frontier in the idea of preemptive cyberwar. Automated active defense requires that the defense systems be configured in such a way to immediately respond through rudimentary, automated forensics, to a supposed attacker in an effort to immediately mitigate an incoming and ongoing attack.

Automated active defenses raise significant questions for stability and security, as massive counterattacks could be launched based on faulty algorithms used to automatically locate attackers, spreading cyberwar exponentially across multiple geographies should automated systems become widespread. Further, critics have argued that active defense migrates defense from a state-centric, deliberative format which attempts to integrate diplomacy towards a vigilante model whereby individual states prefer to attack first, and ask questions later.

Active defense does not confine itself to its physical, territorial, or political geographies but rather envisions an interconnected world through which threats can be analyzed, traced, and attacked seamlessly and without regard for consequences. The recent trend towards more automated active defenses has significantly complicated what was already seen as rapidly rising dangerous form of cyber-vigilantism (Gjelten, 2013b) by substituting immediate human judgment with automated human-developed algorithms whose sole purpose is to endlessly seek, prepare for, and launch attacks.

National cybersecurity

The final method of defending from cyberattack involves a combination of the above logics framed in an explicitly territorial way. Previous methods could be used by either individual organizations or states without any sense of cohesion or cooperation across multiple scales. However, this approach ultimately results in some sectors of a state being more secure than others, and with no clear or effective direction for future cybersecurity efforts (Clarke & Knake, 2012).

Great cyberpower states like Iran, China, and Russia have governmental structures which allow them to leverage all the cyberpower present within their territory, and to approach cyberwar from an explicitly territorial standpoint. That is, the multiple defense logics presented above are considered at a national scale and then implemented downward hierarchically. Firms have no other alternative but to comply due to either overt or covert government pressure exercised in multiple ways (Goldsmith & Wu, 2008), as means through which the state can enforce Internet control within its borders. In liberal democracies, however, a state is less able to directly require firms and citizens to undertake specific actions related to cybersecurity.

Recent evidence of widespread cyberespionage by China and organized attacks against American banks launched by Iran have prompted calls for a more overt and explicit national policy on cybersecurity (Gross, 2013; Young, 2010). The rationale behind this calls it an explicitly territorial one: creating the idea of a nation's cyber boundaries. Indeed, the American portion of the Internet has been viewed by policy scholars as a separate territorial entity requiring an explicitly territorial construction in cyberspace in order to function effectively and be able to assert power domestically and abroad. Early responses towards cyberwar in the 1980s saw the United States conceived of as a distinctly separate cyber-geographical entity with distinct boundaries which needed to be secured. The first step involved migrating all government and military computers towards a uniform policy of cybersecurity. However, the threat of cyberwar soon faded from public awareness and efforts at strengthening these “cyber boundaries” stalled.

Clarke (2012) advocates a return to the mid-1980s vision of national cyberspace, whereby private organizations would be required to enact certain minimum security protocols, which may include active cyber defenses. However, individuals within a territorial state also represent a threat to national cybersecurity, as a result of the diversity of web browsing habits and level of technical sophistication. Scholars such as Schilling (2010) have advocated for the development of national identification systems which would assign Americans IP addresses as a means towards defending the national cyberspace by being able to see which individuals represent potential security threats.

The national cybersecurity approach, therefore, represents an amalgamation of individual security and defense approaches to create a cohesive policy at the national scale. It offers an alternative scalar vision for cyber defense, one which is grounded in territory, and which dangerously ignores the elements of cyberspace which are aterritorial. For instance, a national cybersecurity policy would see critical national cyberinfrastructure as existing within the explicit political boundaries of the state. However, infrastructure firms, such as oil refineries, may have significant overseas data centers or operations, which would be excluded from any national policy but which nonetheless remain connected to the firm's headquarters, representing a continued security threat, highlighting the continued geographical problems posed by cyberwar.

Defense Conclusion

This section described several key approaches to cyber defense during cyberwar. The main categories of defense are human, proactive, active, and national. Each of these categories represents a specific way in which defense can be conducted, broadly speaking, without involvement in technical specifications. Human scaled defense argues that no over-arching cybersecurity policy can be developed without it being grounded in the most vulnerable part of any computer network: human beings. Security, therefore, is predicated upon training, monitoring, and limiting individuals in their interactions in cyberspace as a means to provide adequate defense against attack.

Proactive defenses are those defenses which situate the idea of defense at the scale of the network, and which further sees that network in a Hobbesian cyberspace whereby the network is isolated and under threat from an overtly hostile cyberspace. Defense, in this instance, occurs from establishing specific and routine protocols to "fortify" defenses while also employing outside red teams to test and attack the network so as to ascertain its robustness and trustworthiness.

Active defenses argue that the geographically static worldview associated with proactive defenses favors the attacker over the defender. Proactive defense also does not have any dis-incentive for attackers, meaning that the range of defenses needed and the static level of its conception favor a patient attacker who eventually will determine the best way to compromise the system. Instead, active defenses believe that the "best defense is a good offense" and argue that attackers should be punished for their attacks, or at least have the threat of digital or kinetic retribution be something which they must consider prior to attacking. Active defenses would allow for states or sub-national organizations to identify and attack attackers as a means to mitigate the attack or punish the attacker, making the cost of subsequent attacks prohibitive. This approach is developing rapidly, with automated active defense eliminating the need for careful human digital forensics and favoring rapid, automatic counterattacks with automatic research and investigations into attribution.

Finally, national cybersecurity seeks to unify disparate defense measures under an explicitly territorial logic. The other defensive approaches are viewed as being the purview of individual organizations and even sub-state elements of the government. No national or explicitly geographic approach exists, which is the issue the national cybersecurity approach seeks to resolve. By situating defense as mandated or required within the political-geographical extent of the state, national cyberdefenses can be successfully established and the state can be constructed through its defenses in cyberspace. However, this approach ignores the extent to which elements of the state and society transcend political boundaries such that the explicit and traditional separation of society between domestic and foreign (Agnew, 1994) has little or no technical grounding.

Conclusion

The purpose of this chapter's articulation of attack and defensive approaches is to provide contextual background for the subsequent case studies in chapter 6, used to illustrate the ways in which cyberwar exists and is prosecuted aterritorially. Both attack and defensive approaches attempt to establish a geographic bounding of computer networks, yet, as the distribution of resources across the global Internet demonstrates, the ability to isolate or confine a state or organization to a specific political-geographical extent is virtually impossible except in very rare circumstances, such as air-gapped spaces.

The methods of attack and defense in cyberwar each carry with them interpretations of space and power and thus create limitations on how these interpretations are acted upon during cyberwar. These become clear through an examination of three case studies in chapter 6, each of which demonstrate how the methods of attack and defense in cyberwar are not bound to political territory in the same way methods of kinetic warfare are. For example, launching a DDoS attack necessitates a global view of power in cyberspace, one which can completely ignore political boundaries. On the contrary, launching a drone strike necessitates negotiating political boundaries if only for the need to refuel the drone. Thus, chapter 6 will demonstrate how these methods are put into practice through three key case studies each emphasizing different ways in which cyberwar uses these aterritorial methods of attack and defense to fundamentally alter the territorially-based notions of cyberspace which states articulate through Internet censorship and control.

Chapter 6

The Spatiality of Power in Cyberwar

Introduction

Chapter 5 outlined the methods of attack and defense used in cyberwar in preparation for an examination of how these aterritorial technologies are used in cyberwar in this chapter. These case studies will be followed by analysis which will dissect and discuss the geographical and ageographical elements and how these elements fit within the broader context of the dissertation. These case studies are among the most important, groundbreaking, and highly-cited cases in cyberwar history and literature. Temporally, these case studies are important due to their being the "first" instance of a specific type of cyberwar documented, and as such act as a foundation for subsequent attacks, defense, and analysis. The innovation behind each case study also creates subsequent path dependencies which further rigidify cyberwar as refinements or enhancements of these groundbreaking and path-defining firsts. There are multiple potential models for cyberwar, including conventional DDoS-centric cyberwar, a cyberwar extending across multiple covert fronts and also a hybrid model which combining both kinetic and cyberwar. The case studies in this chapter articulate are demonstrative of these different models.

The first case study, of the 2007 cyberwar between Russia and was the first international event to be described as a cyberwar, precipitated a state of national emergency in Estonia, and invoked the potential of armed an armed response due to requirements in the NATO charter. Its importance is seen in its conceptual demonstration of the vulnerability of a highly “wired” society, and established protocols for cyberdefense and cyberwar in NATO and in NATO affiliated states. The Russia/Estonia cyberwar is an example of a traditional form of cyberwar, and best understood through popular geopolitical understandings of cyberwar.

The second example merges kinetic conflict with traditional elements of cyberwar. This approach, dubbed “hybrid warfare” by NATO (S. Jones, 2014), is seen as the future of conflict in which a state augments kinetic conflict with cyberwar in such a way that both are seen as inseparable and which both feature elements of plausible deniability and lack of attribution. This approach is influenced by the historical development of information warfare and disruption originally proposed by Russian military thinkers as part of the worldwide “revolution in military affairs” (Metz & Kievit, 1995) associated with the deployment and integration of the Internet and advanced communications technologies with military operations and units.

The third case study, of the protracted long cyberwar between Iran and the United States, highlights an alternative approach to cyberwar. In this case, international assets of states are seen as targets for infiltration and infection through sophisticated tools and technologies alongside the traditional techniques of the Russia and Estonia case study. This case features the world's first known cyberweapon, a technology designed for the explicit purpose of sabotaging physical infrastructure of a state while remaining undetected and deploying sophisticated elements to protect and delete itself. This cyberwar is novel in that it has seen spectacular attacks executed with a precision which has kept the conflict largely hidden from popular view.

These case studies illustrate the spatiality of power in practice, support the dissertation’s claim that cyberspace is articulated territorially but cyberwar is prosecuted along a spatiality of power model, and demonstrate the existence of the cyber-geographical gap between state Internet policies and state practice.

Russia/Estonia

Two elements of the Russian/Estonian cyberwar case study are critical: the technological and political contexts. Technological contexts are those contextual elements purely related to the implementation and adoption of various communications technologies, which provide a broader framework in which actions in cyberspace exist. Estonia had made significant investments in the Internet since its accession to the European Union in 2004. The Internet was a cornerstone of Estonia's internal development; in the year 2000 the Estonian Parliament declared Internet access to be a basic human right (Tăbușcă, 2010). Under the concept of “E-stonia” (Schnurer, 2015) the Estonian government decided it could leverage its comparatively small population and size and migrate most vital services to the Internet, including citizenship and voting (Mansel, 2013). Estonia therefore became the state most infrastructurally dependent upon the Internet for some elements of daily life, especially banking (Schnurer, 2015). More than 80% of Estonians used online banking and a further 97% of all financial transactions within the country, including those between individuals, companies, government agencies, and foreign firms and governments, were entirely dependent upon the Internet. A significant amount of medical communications, practice, and work was conducted remotely, and even the capital’s water supply was connected to Estonia's national high-speed Internet infrastructure (Herzog, 2011; Lesk, 2007).

Estonian citizens had an “E-ID” card to allow them to interface with banks and government online, and it was the first country in the world to host part of its local elections on the Internet in 2005 (African Network Information Center, 2009). Finally, the entirety of Estonia’s law enforcement and criminal justice systems utilized the Internet for coordination and cooperation (W. Goodman, 2010). Estonia was wired to such a degree that the BBC claimed Estonia was more technologically advanced and integrated than larger states in Europe, such as France or Italy (Lesk, 2007). It was, at the time, the most technologically integrated and dependent state in Europe (Lungescu, 2004).

This technological context allows for a nuanced understanding of the importance of cyberwar, especially as states continue to move vital services online and require various forms of online association from their citizens. A state is restricted in its actions and responses by its technological limitations (Scott, 2009), thus a technological context sets the boundaries for the possible within the political context. For example, the presence or absence of sophisticated anti-aircraft batteries may limit or expand a state's desire to intervene, demonstrated in contrasting examples between Libya and Syria. However, a technological context only illustrates a portion of the reality behind cyber war. In order to understand how cyberwar emerges, an understanding of the political context and background is necessary.

The political context of the Russia/Estonia cyberwar begins with a proposal floated by the Estonian parliament in 2007 to relocate a statute commemorating the Russian and Soviet soldiers, who died “liberating” Estonia from Nazi Germany. At the time, this proposal was seen in the context of an increasingly hostile ethnic Estonian nationalism which threatened the Russian minority, also representing a continued symbolic break with Estonia's Soviet past and increasing integration with the EU and NATO. The ethnic Russians, which comprise nearly a quarter of the total population (Greene, 2010), viewed the monument as a means through which their minority rights would be respected while ethnic Estonians saw it as a symbol of the totalitarian occupation of Estonia after the Second World War (Ehala, 2009).

The tension reached a critical tipping point in April 2007 during a series of violent protests and riots called the “Bronze Night” (Kaiser, 2015), the name given to the two days of protests and riots which erupted in response to Estonia’s decision to move the statue. Over a thousand ethnic Russians rioted for more than two days, burning cars and buildings, resulting in one death, hundreds of arrests, and more than 100 injuries (BBC, 2007). Estonian police were pelted with Molotov cocktails and responded with rubber bullets and tear gas in a bid to stop the protests from escalating. At the same time, protesters in Moscow besieged the Estonian embassy, attacking anyone who attempted to leave or enter the building, including the Estonian ambassador. The siege prompted diplomatic intervention by the European Union (Finn, 2007).

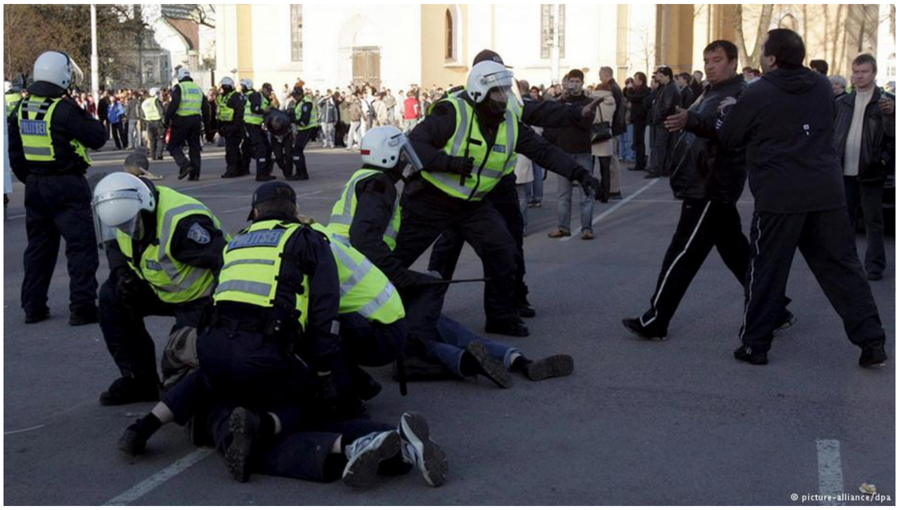


Fig. 18 – Bronze Night protests in Tallinn, Estonia (de Pommereau, 2014)

The Russian government expressed its highest level of dismay, lodging formal protests against the Estonian government and repeating its stance against the statue being moved. It went so far as to dispatch a “fact-finding” mission to examine the statue's relocation and provide a full report to interested publics (Tanner, 2007). The situation was a critical breakdown in Russian-Estonian relations, heightened by Russian fears of a shrinking sphere of influence and “encirclement” or encroachment by NATO and the EU (Fedyszyn, 2010).

These protests and political turmoil provide the political context, which, in addition to the technological context, allow for an understanding of the cyberwar. Beginning on the first night of the protests, April 27, Russian discussion forums, chat rooms, blogs, and social media were lit up by calls to action against Estonian Internet targets (A. Schmidt, 2013). These websites provided links to easy-to-download tools and a list of desirable targets for outraged Russian citizens to attack. The posts became hugely popular in Russian cyberspace, tools were designed for ease of use, allowing ordinary non-technical citizens to participate in the attacks. The initial list of websites included the Estonian parliament, presidency, and various government ministries (Traynor, 2007).

The attacks began with participatory DDoS utilizing the tools and lists of targets to attack, causing minor disruptions in the targeted websites. As the attacks produced small but demonstrable slowdowns in Estonian websites, more users and groups enrolled in the project, at one point sending over 4 million data packets per second to overwhelm Estonian websites, while Estonia’s usual national traffic is 20,000 packets per second (Davis, 2007). At the same time, more advanced hackers employed defacement tactics to deface government websites and replace images of elected officials with those resembling famous Nazis, an insinuation that the Estonians were fascists in their approach towards Russian minorities (Herzog, 2011) and demonstrating an explicitly political rationale and purpose behind the attacks. The sophistication of the attacks grew with the employment of multiple botnets to augment the cyberattacks, with the number of computer zombies arrayed against Estonia exceeding 1 million (African Network Information Center, 2009), nearly matching the population of the entire state. There were over 125 recorded instances of separate DDoS attacks, and deliberate usage of mass-emailing ("spam") systems to email the Estonian government as a means to overwhelm and shut down all email communications servers (African Network Information Center, 2009). The severity of the attacks was sufficient to cause damage to physical electronic infrastructure including routers and email mainframes (African Network Information Center, 2009). The resources and broad coordination used against Estonia were far greater than what could be reasonably achieved by motivated individuals, with NATO and other security analysts agreeing that attacks of this level could only be conducted with state resources, support, and a blind eye (Clarke & Knake, 2012; Herzog, 2011).

The initial targets, politically-connected websites, were soon augmented by expanding the list of targets to include key businesses, banks, and Internet service providers, and the email addresses of all members of Estonian parliament and government agencies (Lesk, 2007). The attacks crippled and rendered inaccessible the websites of the Estonian presidency, parliament, almost all government ministries, most political parties, the three largest news agencies in the country, most of the country's banks, the national government's Internet service provider, and most private Internet service providers (African Network Information Center, 2009). Citizens were unable to withdraw money from ATM cash machines, government systems were unable to be updated with reports or analysis, email communications between citizens, government, and business was shut down (African Network Information Center, 2009). Estonian Internet service providers were forced to disconnect their users from the Internet, and at the national level Estonia resorted to blocking all traffic originating from outside its borders, effectively isolating its communications and automated infrastructure with the rest of the world. Automated financial transactions, regulatory filings, criminal justice proceedings, transnational engineering contracts or remote work, and more were completely disabled as Estonia resorted to geographic isolation in response to the severity of the attacks (A. Schmidt, 2013).

The high level of connectivity in Estonia coupled with the severity of the attacks prompted the Estonian Minister of Defense, Jaak Aaviksoo, to consider invoking NATO’s Article 5 requirement that the Alliance come to the aid of a member under attack (Davis, 2007). He stated that:

> "All major commercial banks, telcos, media outlets, and name servers — the phone books of the Internet — felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation." (Davis, 2007)

NATO declined to intervene, citing the lack of precedence and the belief that the attack was not sufficiently dangerous (Wolff, 2014). The attacks eventually died down, allowing Estonia to regain control over its cyberspace and traffic, making banks, and public services again available to the public as well as facilitating intra-governmental communications. The importance of the attack was not lost on NATO, despite its stance on Article 5. The alliance opened the NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) in the Estonian capital of Tallinn as part of a broad-based, international expansion into cyber-defense inspired by the severity of the Estonian attacks and the realization that increased connectivity was complemented by increased insecurity. The center was established in August 2008, the year after the attacks and four months after the initial development of a cyber-defense policy by NATO at its Bucharest Summit, to be adopted by all member states (Hughes, 2009). The CCDCoE remains NATO's premier center for cyberwar, defense, and security in Europe.

Examining the Attacks

These cyberattacks were predominantly DDoS attacks, with some website defacements of prominent Estonian government websites (A. Schmidt, 2013). The use of DDoS, rather than a sustained effort to hack into vital systems to bring them down or cause damage to physical infrastructure, could be seen as a means through which the Russian Federation could test NATO cyber defenses. At the same time, the use of DDoS may have been deliberate, as the dependence of Estonia on sustained bandwidth for the operation of a significant amount of daily services would be more broadly damaged or disabled through DDoS rather than attacks on Estonian physical infrastructure.

The cyberattacks occurred in two broad waves, and lasted for nearly four weeks from April 26 – May 18th (A. Schmidt, 2013). The initial attacks were participatory DDoS encouraged on Russian blogs, forums, and websites, and Estonian officials claim that the online attacks and riots were explicitly organized and directed from the outset (A. Schmidt, 2013). These first attacks targeted government communications infrastructure through DDoS and through mass-spamming of government email accounts. The websites and online services of most government agencies were rendered unresponsive. Additionally, national newspapers and websites were brought down and communications across the country slowed substantially (A. Schmidt, 2013).

The first wave was met by a coordinated defensive response by Estonian authorities, who had been anticipating a spillover of tensions into cyberspace (A. Schmidt, 2013). These proactive defensive measures were augmented by security experts monitoring Russian cyberspace and picking up increasing levels of "chatter" indicating a level of planning or preparation for a major participatory attack (A. Schmidt, 2013). The defensive model Estonia used resembled a turn away from the ensemble of worlds model towards the field of forces, as Estonia relied on hardening its territorial boundaries in cyberspace in response to Russia's attack which embraced the world society model.

A second wave, from April 30 through May 18, was coordinated with the use of botnets and a level of technical expertise consistent with state involvement (A. Schmidt, 2013). While previous waves had been oriented towards forum participation and the mobilization of citizen volunteers, the second phase was highly focused, directed, and with specific targets and attack patterns (A. Schmidt, 2013). The primary method of attack was the use of DDoS along with website defacement to target state DNS providers, banks, government institutions, and financial institutions (A. Schmidt, 2013; Tikk, Kaska, & Vihul, 2010). This wave of the attacks was the most serious and resource-intensive, and saw most financial and government institutions become inaccessible (A. Schmidt, 2013). As a result, Estonian agencies and the government reached out to their EU and NATO counterparts in a bid to stop or mitigate the severity of the attacks.

This wave of attacks was met with countermeasures by the Estonian agencies under attack, supported by NATO as well as EU security experts from Finland, Germany, and Slovenia

(A. Schmidt, 2013). These countermeasures were augmented by a European-wide agreement through RIPE (the Résaux IP Européens Network Coordination Centre, one of five global Internet registries) allowing Estonian agencies to route specific IP addresses to RIPE for blocking at the European-wide level (A. Schmidt, 2013). Additional defensive mechanisms involved structural changes to the Estonian Internet itself to drop packets originating from Russia (W. Goodman, 2010; A. Schmidt, 2013). As the attacks escalated into the global botnet, Estonia essentially blocked all outside originating traffic from crossing Estonia's "virtual borders", disconnecting itself from the global Internet but allowing its domestic Internet to resume normal functioning essential for vital financial and infrastructural services provided by the state (W. Goodman, 2010; A. Schmidt, 2013).

The Estonian attacks were not a consistent and constant attack against targets inside Estonia. Further, these attacks were not considered large by global standards, rather they appear to have been custom-designed to suit the particularities of the Estonian Internet (A. Schmidt, 2013). These attacks occurred in geographically dispersed waves with command & control servers located around the world, ignoring conventional boundaries in their fluidity and relative ease of acquisition and decommission (Nazario, 2009).

Through digital forensics, security experts and academic researchers were able to determine that the initial attacks were started on Russian language forums (A. Schmidt, 2013). The second wave, however, utilizing botnets which spanned the globe proved to be more difficult to research and to determine geographic origin. Given the parallels between targets and attacks, security researchers assumed that the likely source behind the procurement and deployment of the botnets was Russia. This was buttressed by discoveries which implicated specific Russian and Kremlin-based IP addresses, the use of the same botnets by known Russian criminal networks in previous attacks, admissions by the state-sponsored Russian Nashi youth movement that it was behind the attacks, and the refusal of Russian authorities to investigate the claims or cooperate in any way with Estonian and EU investigations (Clarke & Knake, 2012; A. Schmidt, 2013).

What the attacks demonstrated technically was a level of citizen coordination, technical sophistication, and state-based implicit or explicit approval to allow the attacks to proceed and occur. Further, the global distribution of the Internet facilitated the devastating second phase of the attacks due to the fact that the attack vectors, the “zombies”, were located globally, necessitating a complete shutdown of the Estonian Internet to the wider world in a bid to stop the attacks. Researchers agree that the attacks were sponsored, or at least tolerated, by Russia, and the global nature of the Internet ensured that the actual accumulation of power itself in the form of zombies was centered in regions with high concentrations of computing power.

This global distribution represents an approach to power which was explicitly transcended conventional political territories, grounded in the world society spatiality of power model. While forensics research has concluded that Russia was, in varying degrees, responsible for the attacks (Blank, 2008; Grant & Association, 2007), the actual geographical distribution of the attack sources was such that there was no one entity whose political geography encompassed the actual resources used. Russia could therefore legitimately claim that even if it endeavored to shut down or restrict access within its own borders, it was powerless to prevent attackers in other jurisdictions from doing the same, which is precisely what it did (Clarke & Knake, 2012).

While Russia's claims to powerlessness are suspect they nonetheless articulate a reality in cyberwar: power is not confined to rigidly defined geographies. Motivated individuals, transnational social movements, terrorist networks, and organized cyber criminals can leverage the Internet to launch attacks and amass attack resources in such a way that the multinational or global level of cooperation needed to disrupt or stop attacks would be virtually impossible. The state that bankrolls, supports, or directs these attacks, can retain plausible deniability – or cooperate with investigations – comfortable with the knowledge that the spatiality of power model underpining cyberwar ensures that political goals can be reached regardless of geographical restrictions.

Despite this reality, states and international organizations such as the UN continue to insist on a territorial-basis for cyberwar, evidenced by the repeated claims by Estonia that Russia was solely responsible for the attacks, and the emphasis by alarmist critics that states are ultimately responsible for attacks occurring inside and outside their borders. Regardless of these claims and the seriousness with which they are received and considered, the reality of cyberwar is such that it is structurally impossible to constrain cyberwar to existing political geographies, though still targeting specific territories. Motivated attackers can launch hundreds of new servers in a matter of minutes in virtually any geographical jurisdiction on earth. At the same time, botnet herders can infect millions of computers around the world and activate them in such a way that the disconnection of entire states from the Internet would not significant damage their ability to conduct cyberwar.

Estonia Conclusion/Impact

The attacks against Estonia caught Western observers and NATO completely by surprise, despite a 1999 cyberattack using DDoS against NATO by China (Lawson, n.d.). The vulnerability of a highly-wired state to cyberwar, and the relative lack of risk or political repercussions for the attacking state was demonstrated convincingly. In response, NATO established the Coooperative Cyber Defence Centre of Excellence (CCDCoE) in Tallinn, Estonia to begin a shift in prioritization away from traditional kinetic conflict towards a hybridized future battlespace including cyberspace and incorporating a new multiplicity of cyber actors. This center would coordinate NATO-wide efforts at identifying and responding to threats, in addition to operating as central location for research and analysis on the threats in global cyberspace.

The attacks had implications outside of Estonia and Europe, prompting many other states to begin significant investments in cyberwar defenses and as a way to leverage global cyberspace in asymmetric warfare. Estonia prompted many states and corporations to develop contingency plans and defensive operational parameters should sustained or significant cyberwar occur. Estonia's contemplation of invoking Article 5, potentially initiating armed conflict against Russia, prompted fears of an unregulated “frontier” in cyberspace whose very lack of structure gave it tremendous strategic advantages and disadvantages.

Finally, the attacks began a discussion amongst global legal scholars to investigate the issues surrounding legal territoriality and cyberwar and cybercrime. While many events associated with or components of cyberwar preceded the 2007 attacks against Estonia, none was of significant mainstream profile nor were any large enough to disrupt the daily lives of millions of individuals. Thus, NATO began a long-term legal research project on developing non-binding legal guidelines for determining applicability of international law to cyberwar, known as the *Tallinn Manual.*

The cyberwar against Estonia in 2007 was a watershed moment in the history of modern communications and in post-Cold War military operations. While its duration of the cyberwar was brief, its impacts were sufficient enough to cause a long-term strategic shift in military thinking and planning by NATO, the United States, Russia, and China (Herzog, 2011). The cyberwar against Estonia constituted a "traditional" type of cyberwar, one which uses zombies and patriotic citizens as "soldiers" online. However, alternative means for cyberwar exist, including a war predicated upon a Cold War model of multiple fronts and covert action, as well as the hybrid model which fuses kinetic and cyberwar to dominate informational and physical space. The next section, on the Russian/Georgia cyberwar of 2008, focuses on this hybrid form of cyberwar.

Russia/Georgia 2008

Russian and Georgian claims over the regions of Abkhazia and South Ossetia had caused conflict between the two states since the fall of the Soviet Union (Hollis, 2011). Under the Soviet Union, the region of South Ossetia was autonomous, something which its inhabitants sought to translate into independence after the Cold War. At the same time, Abkhazia sought to gain independence as well, and Georgia fought two wars to regain control of these breakaway regions in the years immediately following the end of the Soviet experiment. In both instances Georgian troops were defeated by a mixture of local secessionists and Russian irregular troops (C. King, 2008). As a result, both regions enjoyed de facto independence and became large recipients of Russian foreign aid and human capital in the form of administrators and technical experts who guided the regions in accordance with Moscow's wishes (Kolossov & O’Loughlin, 2011).

In 2008, amidst deteriorating relations between Russia and Georgia, Georgia accused Russia of shooting down an unmanned drone it was operating in or near Abkhazia (BBC, 2008). Days later, Russian troops began to flood into Abkhazia under the pretext of defending Abkhazia and its residents from imminent Georgian aggression. Almost simultaneously in South Ossetia, separatists broke the cease-fire they had long maintained with Georgia and began to attack Georgian troops. Georgian President Mikhail Saakashvili, who had promised to regain the breakaway regions (C. King, 2004), sent Georgian troops into South Ossetia. This intervention prompted a strong Russian response, with thousands of Russian troops pouring into South Ossetia and Georgia, and Russian airstrikes hitting Georgian targets in South Ossetia (Deibert et al., 2012). Ultimately, Russia and Georgia signed a cease-fire which saw Abkhazia and South Ossetia remain as regions with de facto independence from Georgia.

At the same time, Russia's interests in Georgia lay not only in protecting Russian minorities in Abkhazia and South Ossetia, but also in Georgia's geopolitical situation as a key transit route for the Baku-Ceyhan oil pipeline. This pipeline, the second-longest in the former Soviet Union (Bilgin, 2007), represents an “end-around” route for moving oil away from Russian interference, gaining the South Caucuses and Turkey tremendous geopolitical clout and representing an economic and strategic challenge to Russian dominance of oil transit in Asia. The pipeline was a “...matter of survival for the Georgian state” (Seattle Times, 2003) while at the same time promoting further economic and political independence from Moscow for the former Soviet republics in the Caucuses.

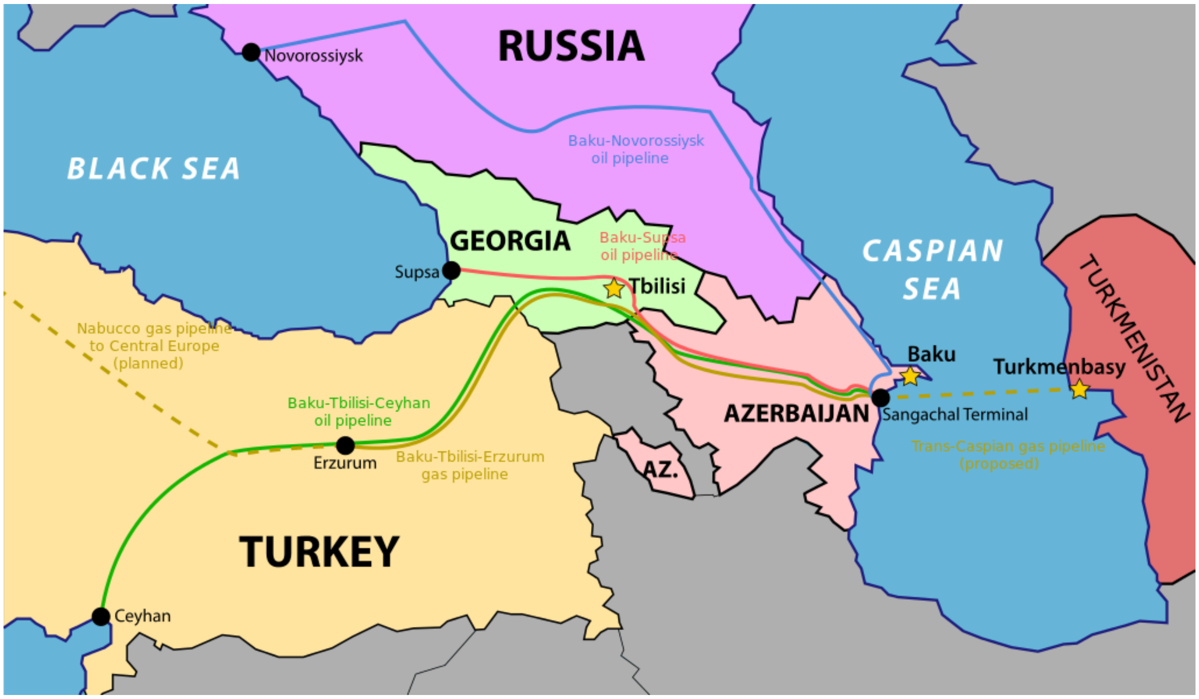


Fig. 19 – Baku-Ceyhan pipeline ("Baku–Tbilisi–Ceyhan pipeline," 2015)

The Caucasus was a potent area through which Russia could re-assert its dominance and remind "wayward" states of the geopolitical realities of greater integration with the West. It would also become an area where the lessons of the Russian cyberwar against Estonia could be refined and honed, in conjunction with a real kinetic conflict, in such a way to validate earlier Soviet military theory and doctrines on the virtue and necessity of total information dominance and total information warfare (FitzGerald, 1997; T. L. Thomas, 2000).

Indeed, in the weeks before the kinetic ground invasion of Georgia, key Georgian Internet infrastructure components were placed under attack by external agents, assumed to be Russian (Hollis, 2011). In July 2008, Russian hacker forums, blogs, and online communities were buzzing about methods and tactics for attacking Georgia targets, with an emphasis on the viability of DDoS and the virtue of website defacements – the two main types of attacks launched during the cyberwar. Arbor Networks, a prominent global security firm, had noticed a heightened amount of “noise” in July 2008 coming from Russia's hacker and cybercriminal underground, indicating that there was a high level of premeditation and strategic oversight and planning of the attacks, as opposed to motivated patriotic citizens reacting to an unexpected ground conflict.

At the same time there were multiple, low-level DDoS attacks detected against Georgian government computing systems, originating in Russia, some accompanied with the message “win+love+in+Rusia+ (Hollis, 2011). The attacks were seen as originating in Russia, but subsequent later attacks prior to the onset of cyberwar were demonstrated to have again utilized globally-distributed zombie botnets in the same way they had been utilized during the 2007 Estonian cyberwar (Keizer, 2008). These attacks were not regarded as serious at the time of their discovery, in July and August 2008, but in retrospect were seen as tests for a looming cyberwar, with the priority being on testing the functionality of the botnets and other networks procured for the purpose of attacking Georgia.

Examining the Attacks

The attacks against Georgia, primarily DDoS and website defacement (Bumgarner & Borg, 2009; Hollis, 2011), are now more commonly associated with civil resistance and non-violent demonstrations in cyberspace rather than cyberwar (Himma, 2005; Oliva, 2013; O’Malley, 2013). However, in 2008 DDoS and website defacement still represented threats to both infrastructure and public perception. What is historically significant about the Russian-Georgian cyberwar is not the methods of attack, whose novelty and significance had been demonstrated in 2007, but rather in its spatiotemporal links with the kinetic conflict – with verified attacks just hours after the formal ground invasion commenced and concluding hours after military operations had ceased (Bumgarner & Borg, 2009). The attacks leveraged a world society model in their global distribution of power, yet were articulated along the lines of the field of forces by bounding the global attacks within the very clearly delineated political territory of Georgia.

Recent research has demonstrated the possibility that cyberwar against Georgia began on August 5, 2008 a few days before the large ground incursion into South Ossetia and Georgia. Allegedly, this first attack was not against Georgian territory, but rather a sophisticated attack against a portion of the Baku-Ceyhan pipeline in Turkey. Hackers, ostensibly Russian, were able to infiltrate the pressure management systems of the pipeline to overload its pressure systems and trigger an explosion, spilling 30,000 barrels of oil and disrupting oil transit for an extended period of time (Robertson & Riley, 2014).

The first wave of verified attacks against entities located within Georgia's territory occurred just hours after the ground invasion by Russia had begun (Bumgarner & Borg, 2009) and again consisted of wide-spread DDoS against more than 50 websites, government information servers, and government communicative infrastructure (Hollis, 2011). This wave specifically targeted government and news media websites as a means to control information flow and access within the country (Bumgarner & Borg, 2009). This was supported by the use of botnets whose IP address ranges are known to be affiliated with Russian organized crime (Korns & Kastenberg, 2008; Markoff, 2008) and the unofficially state-sanctioned “Russian Business Network”, which focused the bulk of their attack power on eleven specific websites and which was connected to some of the attacks against Estonia in 2007 (Korns & Kastenberg, 2008; Stapleton-Gray & Woodcock, 2011).

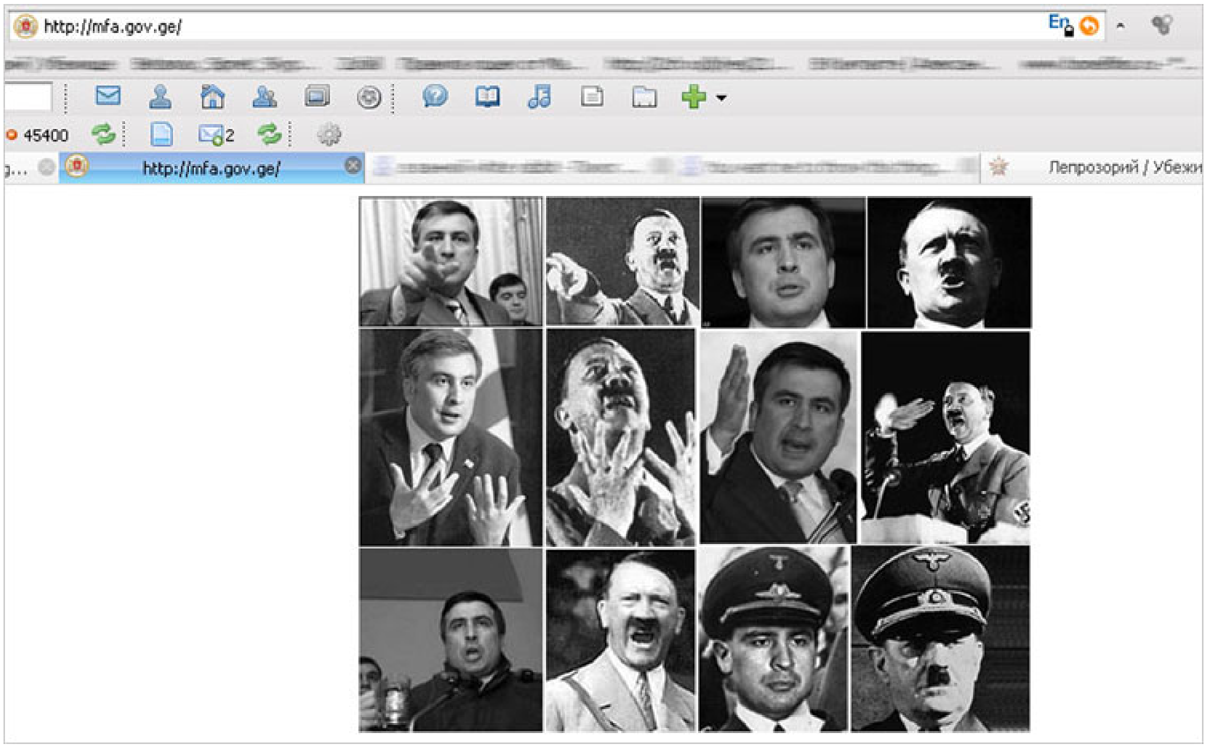
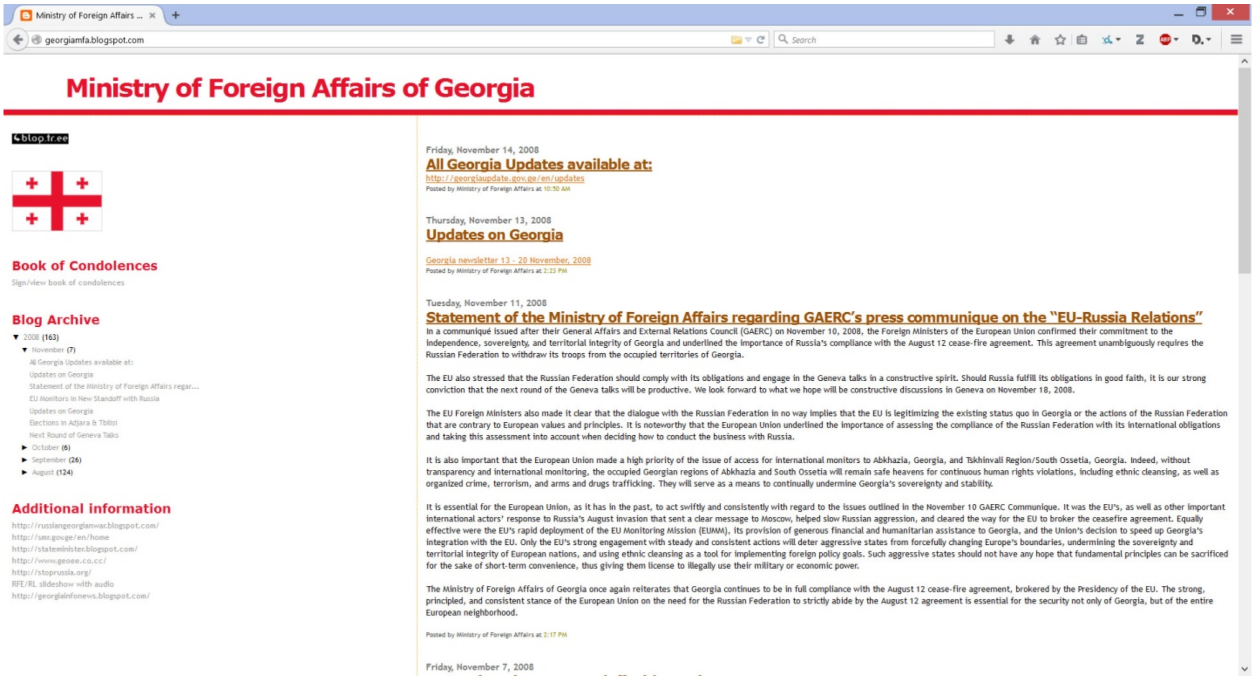


Fig. 20 – Defaced Georgian parliament website (Markoff, 2008)

A second wave of attacks emphasized participatory DDoS by providing an easy-to-use tool for Russian citizens to download and attack Georgian websites. This wave of attacks coincided with the Russian military successfully establishing a foothold in the invasion and targeted financial institutions, business associations, and educational websites (Bumgarner & Borg, 2009). The effort was to disrupt or delay the ability of Georgia to make significant financial transactions or decisions as a means of creating economic instability amongst Georgia's elite. While Internet penetration in Georgia is relatively low, the Internet is essential for commerce and trade amongst the governmental, financial, and business elite. Indeed, the attacks were so successful that the National Bank of Georgia was forced to sever all Internet connections for ten days, leaving it functionally unable to operate or process financial transactions (Bumgarner & Borg, 2009).

The participatory attacks involved a greater total number of individuals attacking Georgian targets compared to the relatively smaller number of individuals attacking Estonia. However, due to the less developed nature of the Georgian Internet fewer resources were needed to disable Georgian websites. The tools used in the participatory DDoS and in website defacement were specifically designed for the Georgian Internet and reflected technical specifications which were present in Georgia and not Estonia, again indicative of significant investment and resource-allocation towards Georgia specifically rather than as an unruly motivated patriotic mob. Indeed, forensic analysis demonstrated that some of the files used for website defacement had originally been created in 2006 – indicating that preparations for an attack on Georgia's Internet had been considered much earlier (Bumgarner & Borg, 2009).

Despite the low-level of Internet penetration in Georgia compared to Estonia, Russian hackers modified their attack plans to make continued opposition to the Russian invasion financially burdensome on elites while at the same time depriving the Georgian government of the ability to communicate or disseminate information to the general populace and world at large. These attacks rendered the majority of governmental websites inoperative, forcing the Georgian government to relocate all of its official business to Google-owned servers in the United States on the Blogspot blogging platform as well as to other U.S. based web hosts (Korns & Kastenberg, 2008). The relocation of Internet assets to a third state, the United States, which was not involved with the conflict, has generated significant controversy (Kelsey, 2008; Ryan & Ryan, 2013; Walker, 2000) about the nature of neutrality on the Internet during cyberwar.



Ministry of Foreign Affairs of Georgia

Book of Condolences

Sign/view book of condolences

Blog Archive

- 2008 (163)
  - November (7)
    - All Georgia Updates available at:
    - Updates on Georgia
    - Statement of the Ministry of Foreign Affairs regar...
    - EU Monitors in New Standoff with Russia
    - Updates on Georgia
    - Elections in Adjara & Tbilisi
    - Next Round of Geneva Talks
  - October (6)
  - September (26)
  - August (124)

Additional information

http://russiangeorgianwar.blogspot.com/
http://smr.gov.ge/en/home
http://stateminister.blogspot.com/
http://www.geoee.co.cc/
http://stoprussia.org/
RFE/RL slideshow with audio
http://georgiainfonews.blogspot.com/

Friday, November 14, 2008

All Georgia Updates available at:

http://georgiaupdate.gov.ge/en/updates

Posted by Ministry of Foreign Affairs at 10:50 AM

Thursday, November 13, 2008

Updates on Georgia

Georgia newsletter 13 - 20 November, 2008

Posted by Ministry of Foreign Affairs at 2:23 PM

Tuesday, November 11, 2008

Statement of the Ministry of Foreign Affairs regarding GAERC's press communique on the "EU-Russia Relations"

In a communiqué issued after their General Affairs and External Relations Council (GAERC) on November 10, 2008, the Foreign Ministers of the European Union confirmed their commitment to the independence, sovereignty, and territorial integrity of Georgia and underlined the importance of Russia's compliance with the August 12 cease-fire agreement. This agreement unambiguously requires the Russian Federation to withdraw its troops from the occupied territories of Georgia.

The EU also stressed that the Russian Federation should comply with its obligations and engage in the Geneva talks in a constructive spirit. Should Russia fulfill its obligations in good faith, it is our strong conviction that the next round of the Geneva talks will be productive. We look forward to what we hope will be constructive discussions in Geneva on November 18, 2008.

The EU Foreign Ministers also made it clear that the dialogue with the Russian Federation in no way implies that the EU is legitimizing the existing status quo in Georgia or the actions of the Russian Federation that are contrary to European values and principles. It is noteworthy that the European Union underlined the importance of assessing the compliance of the Russian Federation with its international obligations and taking this assessment into account when deciding how to conduct the business with Russia.

It is also important that the European Union made a high priority of the issue of access for international monitors to Abkhazia, Georgia, and Tskhinvali Region/South Ossetia, Georgia. Indeed, without transparency and international monitoring, the occupied Georgian regions of Abkhazia and South Ossetia will remain safe heavens for continuous human rights violations, including ethnic cleansing, as well as organized crime, terrorism, and arms and drugs trafficking. They will serve as a means to continually undermine Georgia's sovereignty and stability.

It is essential for the European Union, as it has in the past, to act swiftly and consistently with regard to the issues outlined in the November 10 GAERC Communique. It was the EU's, as well as other important international actors' response to Russia's August invasion that sent a clear message to Moscow, helped slow Russian aggression, and cleared the way for the EU to broker the ceasefire agreement. Equally effective were the EU's rapid deployment of the EU Monitoring Mission (EUMM), its provision of generous financial and humanitarian assistance to Georgia, and the Union's decision to speed up Georgia's integration with the EU. Only the EU's strong engagement with steady and consistent actions will deter aggressive states from forcefully changing Europe's boundaries, undermining the sovereignty and territorial integrity of European nations, and using ethnic cleansing as a tool for implementing foreign policy goals. Such aggressive states should not have any hope that fundamental principles can be sacrificed for the sake of short-term convenience, thus giving them license to illegally use their military or economic power.

The Ministry of Foreign Affairs of Georgia once again reiterates that Georgia continues to be in full compliance with the August 12 cease-fire agreement, brokered by the Presidency of the EU. The strong, principled, and consistent stance of the European Union on the need for the Russian Federation to strictly abide by the August 12 agreement is essential for the security not only of Georgia, but of the entire European neighborhood.

Posted by Ministry of Foreign Affairs at 2:17 PM

Friday, November 7, 2008

Fig. 21 – Georgian Ministry of Foreign Affairs on Google Blogspot (Screenshot by author)

The attacks which Georgia faced had already been faced by Estonia, and with rapid technological advances in under a year there were already standard best practices for Georgian IT experts to fall back on in the face of Russia's digital onslaught. The Georgian IT community did, in fact, reach out to Estonian officials who then connected them to EU and NATO experts in order to bolster Georgia's defenses through remote administrative changes in European Internet infrastructure upon which Georgia relied (Bumgarner & Borg, 2009). By both relocating vital government services to the United States and advocating a more decentralized approach to defenses, Georgia utilized the spatiality of power model through its approach to defenses – seeing the conventional idea of "territory" as more a flow of resources and power rather than something inherently associated with the physical geography of Georgia itself. The response, to seek technically-grounded assistance from the EU and NATO, echoes the hierarchical network model which sought to connect Georgia to more powerful nodes for security. At the same time, the relocation of vital official state services exists along the world society model when resources were relocated away from Georgia without concern for political boundaries.

Aside from the ways in which Georgia leveraged a spatiality of power model for cyberwar in order to bolster its defenses against a global series of attacks, what distinguishes these attacks from those in Estonia and from other instances of cyberwar before and since, was the linkage between attacks in the digital realm and offline, kinetic military action. Once Russian commanders had successfully established a foothold in Georgian territory, attacks were intensified and designed to sow confusion amongst the general populace, government functionaries, and financial/political elites (Bumgarner & Borg, 2009; Hollis, 2011). This was augmented by a remarkable geographical focus in directing attacks towards the local news and government communications services in the Georgian city of Gori at the same time as the Russian ground and air offensive began against the city. The attacks were specific enough that intelligence analysts were able to use them in order to predict or anticipate where Russian attacks were focused or were imminent (Hollis, 2011).

Military theorists postulated that these attacks were designed to informationally isolate communities in such a way that degraded their ability to utilize online communications to gather and disseminate information. Further, given the reliance of traditional communications technologies, such as the telephone or more recently mobile phones, on Internet-connected servers to switch and route calls, these attacks would be slowed or stopped the ability of individuals to place or receive phones calls or text messages, contributing to geo-informational isolation in the context of the broader conflict. As discussed in chapter 4, this is in line with long-standing Russian information war theory which advocates complete control of information space as a means to achieve both tactical and strategic objectives during kinetic conflict. In this case the conduit was cyberspace, and approaching cyberwar through a spatiality of power model which allowed for power and resources to be pooled and utilized decoupled from conventional notions of territory and political geography.

In contrast with general strategic approaches to warfare, physical attacks against news and media organizations were avoided, with analysts speculating this was done because they had been rendered functionally inoperable due to over-reliance on digital communications (Bumgarner & Borg, 2009). Conflict had shifted from a strictly physical perspective which included only land, air, sea, and space, to now become more volumetric (Elden, 2013a) by encompassing cyberspace as a domain for conflict as well as a space which could be seen as a parallel, supporting domain during times of kinetic conflict. If considered with the results of the attack against the Baku-Ceyhan pipeline, cyberwar could also be seen as a crossover domain between the virtual and kinetic as well, something which alarmists have long claimed (Arquilla & Ronfeldt, 1993; Clarke & Knake, 2012).

Finally, the attacks were also noteworthy when viewed vis-a-vis the Estonian cyberwar in terms of targets. In the case of Estonia, cyberwar had widespread effects across the country, and was something felt by a majority of the population in some way. As Bumgarner and Borg (2009) argue, however, the Russian/Georgian cyberwar was distinguished in the fact that targets for cyberwar seemed to have been chosen to specifically limit widespread disruption to the general populace. While banking and news services were disrupted, these did not have a widespread impact in the general populace when adjusted for the relative disparities in Internet infrastructure between Estonia and Georgia (Bumgarner & Borg, 2009). In the same way that combat operations are specialized for the unique physical and cultural geography of different locations, the case of the Russian/Georgian cyberwar demonstrated that cyberwar was a domain which must also adapt to the specificities of unique national Internets, despite its aterritorial and ageographical nature.

Russia/Georgia Conclusion

For the first time in modern military history a conventional ground war was paralleled by a cyberwar between two sovereign states (Markoff, 2008), a historic first in the history of cyberwar. These attacks were not generic attacks against a broad spectrum of targets, but were both conceptually and geographically focused and had significant preparation time indicating the inclusion of cyberwar within Russian military thought and practice. Cyberwar, therefore, was to be seen as an autonomous yet complementary space for state operations which worked with both intelligence and military operations in order to achieve state geopolitical objectives.

Despite its historical importance, the Russian/Georgian cyberwar was conventional in many regards. The use of DDoS, website defacement, botnets, and participatory DDoS technologies echoed the earlier cyberwar with Estonia. Likewise targeting government, news, and financial websites was also part of a well-established approach to cyberwar. However, the Russian/Georgian cyberwar is noteworthy because it represents the first recorded instance of cyberwar and kinetic conflict occurring simultaneously, with cyberwar (aside from the Baku-Ceyhan pipeline attack) in a supporting role towards information dominance.

The Russian/Georgian cyberwar is awash in geography and geographical themes. Broadly speaking there were two geographic themes to the attacks: those focused against governmental agencies broadly within Georgia, and attacks which were geographically focused in regions or areas where the Russian military was active or would soon be active (Bumgarner & Borg, 2009; Hollis, 2011). Further, the specific nature of attack and defense demonstrated one of the central themes of this chapter, namely the dissonance between the way the Internet is conceptualized at the state level, and how that conceptualization transforms once cyberwar has begun. The spatiality of power model seen here strongly embraced the world society and hierarchical network models.

As this section has discussed, there were preparatory attacks supplemented by early reconnaissance to identify appropriate or impactful targets which would complement the kinetic military offensive. Although some Georgian hackers attempted to counterattack (Hollis, 2011), by and large the official response of Georgia appears to have been to relocate vital official government online services to a third state and leverage NATO's expertise in cyberwar in an attempt to defend those assets which could not be easily relocated (Bumgarner & Borg, 2009; Hollis, 2011; Korns & Kastenberg, 2008).

This demonstrates a cyber-geographical gap between the ways in which both states envisioned the Internet and how both states practice cyberwar on the Internet. In the first instance, Russia identified and worked against targets located with the geographical territory of Georgia proper. These targets were identified not only for the geographical specificity in terms of supporting kinetic conflict locally, but also in their ability to destabilize political elites within the country in support of Russia's political aims. Servers within Georgia were compromised and hacker forums and blogs located within the country itself were also targeted for attack.

However, the cyberwar itself saw both sides reconceptualize their ideas of political territory through leveraging the global nature of the Internet in response to specific threats and attacks. For Russia, this was done through utilizing botnets with command computers located in the United States (Korns & Kastenberg, 2008) and other states. For Georgia this was accomplished through relocating strategic assets to the United States. In both instances the states in which these incidents took place were not aware of the actions taken by another sovereign state in their territory. This is noteworthy as these efforts overtly involved relocating digital assets to third party, ostensibly neutral states while leveraging the digital assets of a large, regional military alliance. International law has yet to substantively address the idea of cyberneutrality, though existing international law would make providing aid to a state a contravention of declared neutrality in a conflict, making U.S. cyber assets legitimate targets for attack by Russia, or others (Korns & Kastenberg, 2008).

The Russian/Georgian cyberwar was a watershed moment in the history of cyberwar and kinetic conflict. Like the case of Estonia, DDoS distributed globally was used to disable key assets. However, these attacks were highly geographically specific by targeting specific cities timed to coincide with a kinetic ground interventions in those cities. The response to the attacks saw Georgia relocate key state assets to the United States and to have that content further subdivided globally through Content Delivery Networks (CDN) used by companies such as Google. In doing so the Russian/Georgian cyberwar demonstrates the ways in which geography and cyberspace become entwined, confused, and juxtaposed during times of war and conflict and how the cyber-geographical gap exists and functions during kinetic war.

US and Iran – 2010 – Present

The third case study examines a series of actions which have occurred between the United States and Iran from 2010 through the present, with emphasis placed on the well-known StuxNet case. These actions have been largely covert and unattributable actions designed to halt or slow Iran's nuclear program. Iran has retaliated to demonstrate that it has sufficient cyber capabilities to make efforts to sabotage its nuclear program costly for the United States – a form of cyberdeterrence. This case study stands in contrast to the previous two in that most of the actions have occurred beneath the surface and have only emerged through accidental leaks or cryptic messages left in the code which powers the cyberweapons themselves. In many ways, the US/Iran cyberwar can be understood as the future of cyberwar (Farwell & Rohozinski, 2011) in that two states are engaged in an ongoing conflict which does not reach levels of mass disruption as with Estonia nor does it work simultaneously with a kinetic conflict as with Georgia.

The US/Iran cyberwar begins with the initial discovery in 2007 of a sophisticated piece of malware which would later be codenamed Flame. This malware was designed using the structural programming logic in a publicly demonstrated prototype codenamed Mosquito, which allowed the software to effectively change its “mission” once installed on target computers. This would allow the program to evade detection or to mask its true purpose after being discovered. Flame built upon Mosquito and was found to have originated in Europe, and then spread to the Middle East with a unique geographic concentration in Iran (Gross, 2013). It utilized over eighty servers in multiple countries across Europe, Asia, and North America while infecting computers primarily in Iran but also the Palestinian Territories, Syria, Lebanon, Egypt, Sudan, and Saudi Arabia (Zetter, 2012).

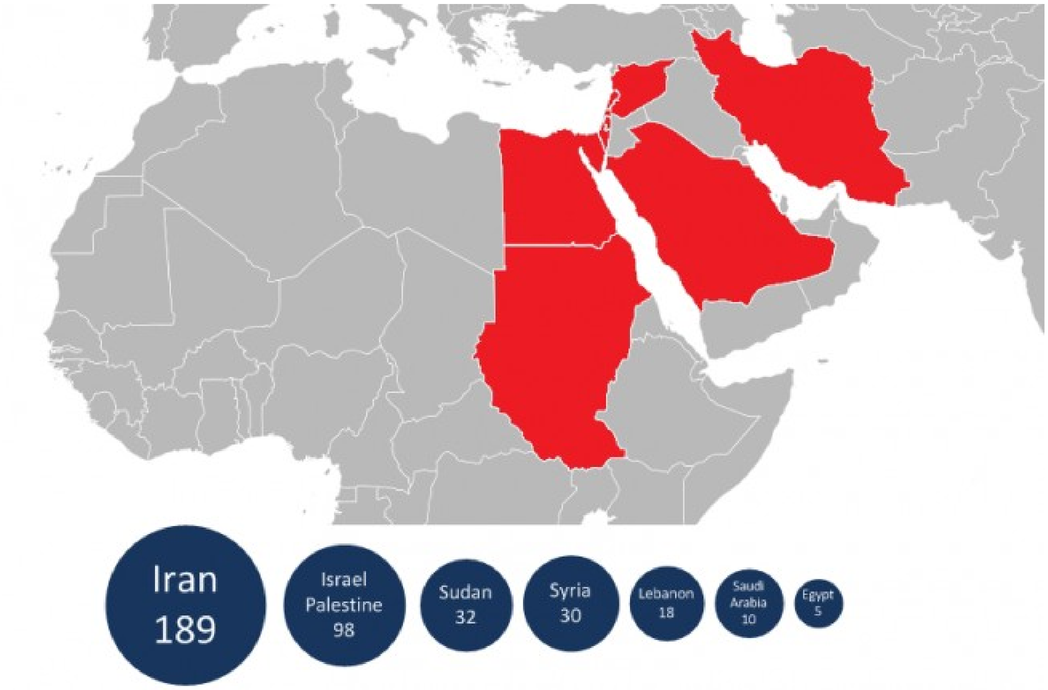


Fig. 22 – Map of Flame infections (Zetter, 2012)

Flame was unique in that it utilized aspects of Mosquito to protect itself and ensure that its creators had maximum flexibility to discover and extract the specific information they were looking for. In other words, remote operators could change its "mission" in real-time to reflect the environment and information it encountered once it infected a machine. Multiple versions of Flame were discovered, including some customized to remotely record audio or video secretly through smartphones, others to retrieve industrial schematics, and still others which simply "reproduced" through covertly enabling Bluetooth on mobile devices and then spreading to other devices within close geographic proximity (Gross, 2013). Most importantly, Flame appears to have been constructed for the purposes of general cyberespionage, primarily targeting Iran (Lee, 2012).

Flame and Mosquito provide the structural foundations for the development of the world's first cyberweapon in 2010: StuxNet. StuxNet was malware designed to destroy highly specific industrial components which were located within Iran's nuclear enrichment facilities, erase evidence of its presence, and fool computer administrators into believing that all centrifuges were functioning normally (Gross, 2011; Markoff, 2011). The discovery of StuxNet sent ripples through the world's security communities as it represented the first “cyberweapon” specifically designed to destroy or damage physical infrastructure, sophisticated enough to have accomplished its objective almost entirely undetected (Gross, 2011).

The implications of such a weapon for cyberwar was immense, with physical destruction of targets in remote countries through targeted malware moving from the realm of science fiction, academic theory, and military contingency planning into reality. Its discovery likewise had important philosophical implications for the nature of cyberwarfare and conflict more broadly: the virtually unattributable destruction of physical infrastructure would redefine the nature of conflict and violence. For legal scholars, the rules and assumptions of international, state-based conflict, which had been developed under different technological regimes and philosophies from the 19th through the mid-20th centuries, were threatened more overtly than with the cases of Estonia or Georgia.

StuxNet was designed to alter speeds on nuclear centrifuges in order to cause them to malfunction or be destroyed (Gross, 2011; Zetter, 2014). It did this by targeting specific software developed by the German company Siemens and used to power centrifuges, specifically model S7-300 (Falliere, Murchu, & Chien, 2011; Gross, 2011; Zetter, 2014). In the event that the Siemens software was not found, then StuxNet would render itself inert and delete itself from the computer. It would, however, first attempt to spread promiscuously to other computers connected to the infected computer and to continue scanning for S7-300 on those computers (Falliere et al., 2011).

If the Siemens software was found, then StuxNet would proceed to scan the system for specific disk drives used on the S7-300 system from two vendors: Vacon from Finland and Fararo Paya from Iran. The existence of these drives would confirm to StuxNet the high probability that this system was an intended target, and from there it would examine the connected centrifuges for those which spin between certain pre-defined frequencies (Falliere et al., 2011; Shakarian, 2011). If all of these elements were determined to be in place, StuxNet would then cause the centrifuges to rapidly increase and then decrease in rotational speed, stressing the centrifuge and forcing it into collision with nearby parts of the centrifuge structure, causing the machine to be destroyed (Stark, 2011). While these centrifuges were spinning wildly, StuxNet would feed information to the centrifuge operators indicating that all centrifuges were operating within normal operating parameters so as to keep its work undetected (Gross, 2011, 2011; Markoff, 2011).

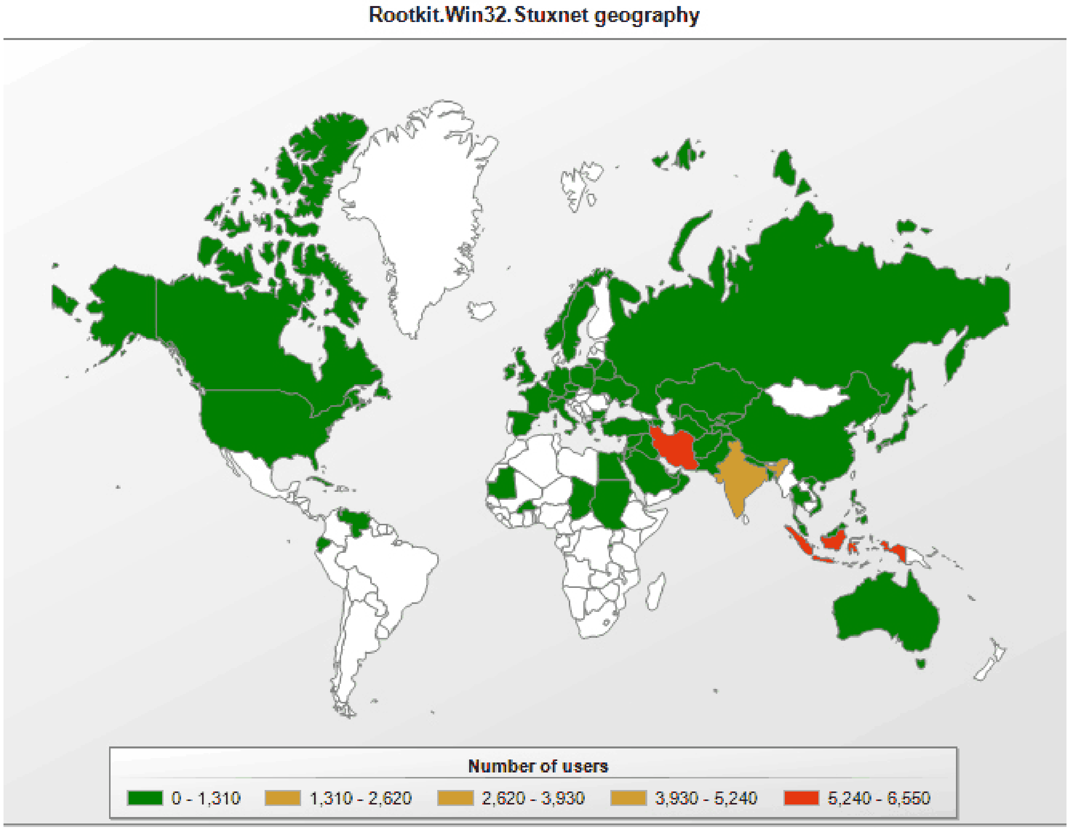


Fig. 23 – Map of StuxNet infections (Finin, 2010)

The malware faced a significant problem in reaching its target as these sensitive computers were air-gapped to secure these systems from malware attacks over the Internet. To combat this, the developers of StuxNet ensured that the malware could easily spread through infected USB drives. Again, the high level of security at the Natanz reactor center in Iran would preclude contractors or other intelligence assets from being able to easily and reliably reach the systems. Continuing the game of cat and mouse, StuxNet's developers targeted instead the internal systems of five companies that intelligence sources believed to be closely associated with Iran's nuclear program (Zetter, 2014). The hope was that someone from one of these closely connected companies would unwittingly take an infected drive into Natanz, thus allowing the malware to spread promiscuously through the facility (Zetter, 2014). This approach appears to have been successful, as various employees of companies associated with nuclear centrifuges in Iran apparently posted questions to anti-virus forums asking for help with unusual problems associated with Siemens software (Zetter, 2014) in advance of the infection of Natanz.

Ultimately, StuxNet was able to infect Natanz and impact the centrifuges located there. According to Zetter (2014):

> "But by August that year, only 4,592 centrifuges were enriching at the plant, a decrease of 328 centrifuges since June. By November, that number had dropped even further to 3,936, a difference of 984 in five months. What's more, although new machines were still being installed, none of them were being fed gas." (Zetter, 2014)

StuxNet was a precision weapon designed to target very specific elements of industrial control systems associated with Iran's nuclear program at Natanz. It was able to cross the air-gap and successfully infect computers in its target location, and then identify the correct target and destroy almost 1,000 centrifuges. Researchers vary in their estimates of StuxNet's impact on Iran's nuclear program. Some believe that it set Iran back by two years (D. Sanger, 2012), while others contend that the impact was minimal and that Iran was able to replace the damaged centrifuges rapidly (Warrick, 2011). While StuxNet's impact on Iran's nuclear enrichment program is subject to debate, its psychological effect on Iran was tremendous: the country announced it was increasing investment in cyberwar capabilities significantly, and issued veiled threats that it would retaliate (Gross, 2013). Indeed, Iranian president Mahmoud Ahmadinejad issued a public statement acknowledging that an infection had taken place and had impacted Iranian centrifuges – a first for the Islamic Republic.

StuxNet was discovered accidentally in July 2010 by security firm VirusBlokAda, based in Minsk, Belarus, when clients in Iran reported issues with their computers (Gross, 2011). From there it was analyzed, and reverse-engineered by the world's leading computer security firms where its complexity and sophistication was quickly discovered. All analysis pointed towards significant state sponsorship of its development specifically by the United States and Israel (D. Sanger, 2012), as the sophistication of the code indicated access to resources far beyond what would be available to non-state actors. From the spatiality of power perspective, the precise targeting of the malware to an explicit territorial state connects this case to the state-based territorial sense of power in the field of forces model – power was believed to be located purely within Iran's political boundaries and StuxNet's code reflects that. Further, the development of StuxNet occurred in the air-gapped environment of Israel's secret Dimona complex in the Negev desert (Broad, Markoff, & Sanger, 2011; Zetter, 2011a) which targeted an air-gapped environment, the Natanz facility. In other words, the ancient ensemble of worlds model becomes resurrected through these inward-looking, clearly demarcated and separate spaces of development.

StuxNet's command and control servers appeared to be located in Denmark and Malaysia, part of a geographic effort to distance the malware from its developers (Falliere et al., 2011; Gross, 2011) and a way in which the world society model was embraced by the United States in this case. Within StuxNet's source code were references to the Bible involving Persia and speeches and comments by Iranian president Mahmoud Ahmadinejad (Gross, 2011). Researchers claimed that StuxNet was the most sophisticated and advanced malware that had yet been discovered, and reinforced a belief that only a state with significant resources could have developed and deployed such sophisticated software (Gross, 2011).

Indeed, in 2012 the New York Times reported that officials in the Obama administration had confirmed that StuxNet had been part of a broader, long-term project codenamed “Olympic Games” initiated by president George W. Bush in 2006 as an effort to destroy or significantly degrade Iran’s nuclear program (D. Sanger, 2012). Obama had decided to extend and enhance this program through the development of StuxNet while remaining aware of the important precedent which StuxNet would set for the future of cyberwar:

> “Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.” (D. Sanger, 2012)

The very public discovery and dissection of StuxNet did not deter or slow down the broader cyberwar against Iran. Shortly after the discovery of Stuxnet, security researchers discovered another malware, this time codenamed Duqu, operating in two specific countries: Sudan and Iran. According to researchers, Duqu was constructed for the explicit purpose of exfiltrating information on industrial command and control systems back to command and control servers located in “Vietnam, India, Germany, Singapore, Switzerland, the UK, the Netherlands, Belgium, South Korea”, and other states (Kamluk, 2011).

Duqu was designed to capture information through recording keystrokes and screenshots and transmit that information back to the command and control servers located globally. Pieces of the code appeared to be based on StuxNet leading some researchers to dub it the “Son of StuxNet” (Zetter, 2011c). The malicious intent of the software and geographic specificity led many researchers to conclude that Duqu was a follow-up to StuxNet designed to survey the post-StuxNet landscape in Iran in anticipation and preparation for future attacks. Indeed, leading security firm Symantec issued the following statement about Duqu:

> “The threat was written by the same authors (or those that have access to the Stuxnet source code) and appears to have been created since the last Stuxnet file was recovered. Duqu's purpose is to gather intelligence data and assets from entities, such as industrial control system manufacturers, in order to more easily conduct a future attack against another third party. The attackers are looking for information such as design documents that could help them mount a future attack on an industrial control facility.” (Symantec Security Response, 2011)

StuxNet opened the doors for researchers to begin to examine similar structural programmatic logics in other malware and attempt to construct a matrix of threats which may have the same source. This led to the discovery of alternative malware, including “StuxNet’s Secret Twin” which had earlier attempted to sabotage the centrifuges creating seemingly random incidents which altered the pressure of gas present in the centrifuge systems (Langer, 2013) as well as the later discovery of the Mahdi malware, again designed to exfiltrate sensitive industrial control information out of Iran (Gross, 2013). Iran’s proxies in Lebanon were the target of the Gauss malware (Gross, 2013) which again sought to exfiltrate information in support of a broader perspective of Iranian state power regionally. It is generally believed that there are other, active programs against Iranian infrastructure or political power currently deployed or in development by the United States and Israel, and that Operation Olympic Games represented a proof of concept – or "Sputnik moment" to demonstrate the superiority of the United States cyberwar capabilities.

The sheer scale of Operation Olympic Games and the relatively unambiguous source and targets did not go unnoticed by the Iranian government. Iran promptly declared that it would be significantly increasing its cyberwar potential, including expanding its cyber-army to identify threats and project power abroad (Gross, 2013). In March 2012 Iran's Supreme Leader Ayatollah Ali Khamenei established the High Council of Cyberspace with a reported $1 billion in funding (I. Berman, 2012), in contrast with the U.S. cyberwar budget of approximately $5 billion (Michaels, 2013).   As analysts had warned, the emergence of StuxNet prompted an escalation of investment and action in state cyberwar, setting a new precedent technologically, militarily, and politically.

Fig. 24 – Iran's "Twitter Revolution" (Bhattacharya, 2009)

Iran had long claimed that the United States was using the Internet as a tool to destabilize and overthrow the regime (Fars News, 2009). Indeed, during the protests which followed the contested 2009 Iranian presidential elections, the Internet was explicitly politicized by the U.S. State Department which intervened to stop Twitter from undergoing scheduled maintenance at a time when it believed Iranian protestors were actively using the site (Grossman, 2009). This event, and statements by Secretary of State Hillary Clinton and the broader news media about the world's first "Twitter Revolution" in Iran and mass-participatory DDoS against Iranian government servers (A. Berman, 2009; Keller, 2010; Evgeny Morozov, 2009b) were taken to indicate an Internet-wide threat to a regime which was already subject to crippling international sanctions and diplomatic isolation. Initial responses had the Iranian Cyber Army hack prominent U.S. and opposition websites, including main opposition sites Kaleme, Rahesabz, and Tahavolesabz as well as Twitter and the Voice of America (Sheikholeslami, 2010). This attack was conventional website defacement, and displayed a message which threatened and taunted the United States' perceived superiority on the Internet.

After StuxNet, another series of attacks against American interests ensued, all of which were connected back to Iran or to Iranian proxies by dedicated security researchers. The first attack in July 2011 targeted DigiNotar, a Dutch firm which issues encryption certificates used by web browsers to encrypt communications between users and their banking, social media, or email accounts (Galperin, Schoen, & Eckersley, 2011; Gross, 2013). The attacker was able to issue compromised certificates and thus intercept the email communications of over 300,000 Gmail users in Iran while threatening the encrypted communications of all of the world's Internet users (Arnbak & Van Eijk, 2012; Galperin et al., 2011; Gross, 2013).

The attack was considered to be one which not only would allow the Iranian government to target and intercept dissident and opposition communications, but also would serve as a tremendous threat and display of power to the world and United States. By undercutting the core of the Internet's encryption protocols, Iran demonstrated that it had the technical sophistication and wherewithal which would serve as a deterrent to future cyberwar from the United States, as well as demonstrating how vulnerable the United States was to cyberwar. Iran's success in the DigiNotar hack prompted the world's Internet browsers to immediately and unilaterally stop accepting DigiNotar certificates, an unprecedented move (Zetter, 2011b). The security risk was significant enough for the Dutch government to take ownership of the firm, which was declared bankrupt shortly thereafter (Arnbak & Van Eijk, 2012; Zetter, 2011b) and prompted a major restructuring of Dutch encryption certificate-issuing authorities (van der Meulen, 2013). Iran's DigiNotar hack was an important proof of concept which bolstered Iran's credibility in cyberwar and encouraged a more advanced attack against the U.S. corporate oil interests of Saudi ARAMCO in August 2012.

The attack against ARAMCO was the largest and most significant attack on a corporation in the history of networked computing, and was the first recorded attack whose sole purpose was the destruction of data rather than exfiltration or surveillance (Gross, 2013). Codenamed Shamoon, the Arab version of the name Simon, it occurred on August 15, 2012 on the night of an important Islamic holiday, Lailat al Qadr (Gross, 2013). Shamoon infected tens of thousands of computers, with over 30,000 computers having their entire hard drives and data erased, and the screen replaced only with an image of a burning American flag (Gross, 2013). Digital forensics indicates that an insider who had physical access to the machines was able to use an infected USB drive to plant the virus on a networked computer, after which the malware's code enabled it to automatically replicate and spread through more than 75% of Saudi Aramco's internal communications network. It wiped out vital data key to refining and exploration, while infecting computers belonging to the company around the world, including the Netherlands and the United States (Bronk & Tikk-Ringas, 2013).

Saudi Aramco, Saudi Arabia's national oil company, flew in executives and security researchers from the world's leading firms, including IBM, Red Had Linux, McAfee, and Microsoft (Gross, 2013), to discuss and examine the attack which had crippled the company's internal communications network. U.S. intelligence officials and computer security researchers believe the attack was retaliation for a smaller attack against one of the main Iranian oil processing plants located on the island of Kharg, codenamed Wiper, believed to be conducted by the United States, which forced Iran to shut down all oil production on the island for two days in 2012 (Gross, 2013). Documents leaked by NSA whistleblower Edward Snowden confirm this fear while also claiming that Iran had learned from Wiper, and to a lesser degree StuxNet, Duqu, and Flame, critical elements needed to ensure launch sophisticated cyberwar attacks against U.S. strategic interests (Zetter, 2015). As several researchers had claimed immediately after the attacks, the United States was teaching the Iranians and other geopolitical adversaries about the U.S.' cyber-capabilities.

Shamoon was relatively simplistic compared to StuxNet, Mosquito, Flame, and Duqu – it contained numerous errors (Osborne, 2012) and its internal code was apparently written to include clues implicating hackers located in Arab states, not Iran. Researchers and intelligence officials believe these clues were deliberately placed in such a way as to distract from the likely originator of the attack, Iran (Perlroth, 2012). Despite not reaching a high level of technical sophistication, Shamoon was nonetheless advanced, focused, and most importantly, successful. Wiping out massive amounts of data disrupted Aramco's business operations and put Iranian cyberwar capabilities firmly on the map.

Iran's retaliation continued in the month following the Shamoon attack. In September 2012 U.S. based banks and financial firms encountered the most sophisticated DDoS attacks ever detected. The attacks targeted "Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T and HSBC" (Peterson, 2013) and other financial firms by launching a global DDoS attack located in datacenters around the world which eclipsed the enormous bandwidth these banks had purchased for security (Perlroth & Hardy, 2013). Indeed, the traffic used in the attack was reported to be significantly larger than the sum total of the traffic used in the Russian cyberwar against Estonia, with some researchers claiming that the attacks were more than 10 times larger than any participatory DDoS ever recorded (Gross, 2013; Perlroth & Hardy, 2013).

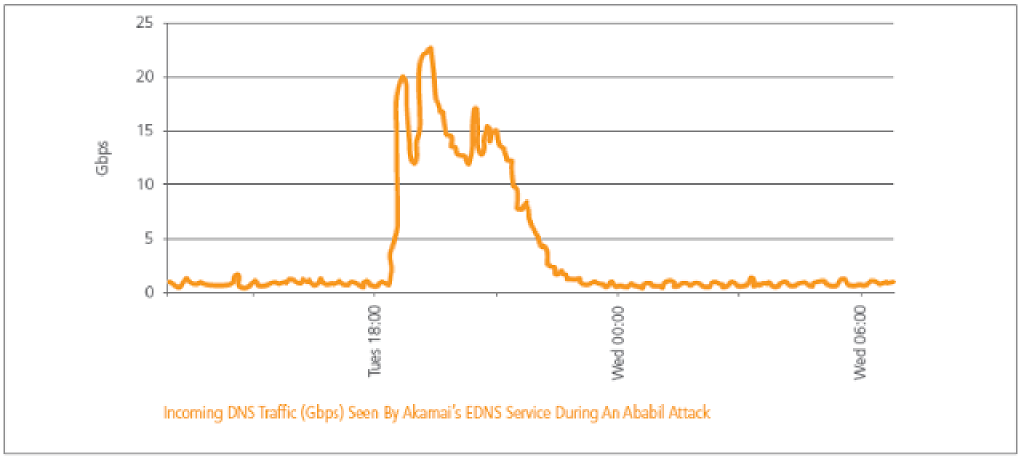


Fig. 25 – Spike in DNS traffic during an Operation Ababil attack (Goh, 2013)

These attacks were novel in two regards: their technical sophistication and their geography. Technically, these attacks were the first “encrypted DDoS” attack which leveraged the encryption technologies that banks and financial firms use to encrypt customer data, not only overload to the traffic to the websites, but also to dramatically increase the load on the actual servers through forcing them to process CPU-intensive encrypted traffic. This was possible because servers must encrypt each packet rather than just transmit data, effectively doubling the workload per packet of information. Thus, an encrypted DDoS would disable webservers utilizing fewer resources and more rapidly than a conventional unencrypted DDoS attack.

While the technical sophistication was significant, it is the geography of the attacks which was tremendously novel, exploiting a uniquely spatial perspective on power in cyberspace. In the previous two case studies, attacking states leveraged global malware infections of random computers which had their control orders centralized at “command and control” servers which were distributed globally, including within western states. At the time of these attacks, the idea of “cloud computing”, which leverages the geographical concentration of computing power at datacenters to bring down storage costs and allow for seamless data storage, was non-existent. Cloud computing has only become a significant force in data storage and processing within the past 4 years, evidenced through the rise of services as Google Drive and Dropbox. These DDoS attacks, dubbed Operation Ababil, had chosen to eschew what had been the orthodoxy to date – infecting millions of computers of ordinary Internet users. Instead, they embraced cloud storage and chose to infect servers located in datacenters. In this case, Iran operated within the model of the hierarchical network, identifying leading network centers globally and infecting them for the purposes of leveraging political power in cyberspace.

The attackers infected cloud servers worldwide with a piece of malware known as “itsoknoproblembro”, which evaded anti-virus software detection, and spread like wildfire through these geographically concentrated locations with thousands of servers to bring unparalleled global attacking power. Security researchers and DDoS experts state that the attacks on individual bank and financial firm websites exceeded 70 gigabits (Perlroth & Hardy, 2013). This number must be seen within the context of average Internet traffic: mid-size businesses routinely have less than 1 gigabit of traffic while a large international bank – such as Bank of America – may barely reach 40 gigabits of traffic during peak intense usage (Perlroth & Hardy, 2013). The costs of the attacks were large as well – with some banks reporting costs of more than $10 million for emergency security to defend against their unprecedented scale (Gross, 2013).

Security and intelligence officials are nearly unanimous in their claim that Iran is behind the attacks. Forensics research discovered various hackers from Tehran bragging online about the development of a new DDoS tool in the weeks preceding the attack, while elements of the attack bore a strong resemblance to earlier actions conducted by Iran (Gross, 2013). In response to evidence that the responsibility for these attacks ultimately resides with Iran, private organizations believe that the responsibility to protect their firms from attack resides with governments (Gross, 2013). Indeed, the Obama administration responded by encouraging greater bilateral communications between private industry and government on cybersecurity (Zezima, 2015).

US/Iran – Conclusion

In contrast to the previous examples of cyberwar, the cyberwar between the United States and Iran is conducted almost entirely in secret, with the exception of Operation Ababil. To many researchers in the field, this represents the future of cyberwar: conducted in secret with potentially devastating results and no oversight from the international community. The relatively secretive nature of this new form of cyberwar has the potential to create greater and more mysterious global insecurity while at the same time with the potential that attacks could be easily mis-attributed to a neutral state.

StuxNet was groundbreaking in that it represented the first ever cyber superweapon developed to target specific industrial control systems and deployed against a focused geographical target. It looked for key fingerprints of specific industrial control systems and, remotely, caused them to spin out of control while masking this and convincing local supervisors that all systems were operating as usual. The attack disabled over 1,000 nuclear centrifuges (Zetter, 2014) and by some accounts slowed Iran's nuclear program by almost two years (D. Sanger, 2012).

StuxNet confirmed the viability of this type of cyberwar while at the same time opening the door for a new type of cyberwar focused less on mass DDoS, as in the previous cases, and more towards the development of specific cyberweapons – a cyber-arms race reminiscent of the Cold War. This was confirmed through the discovery of other malware, Flame, Duqu, and Wiper, which were again focused on information exfiltration or eradication targeting Iran's nuclear, industrial, and oil industries and programs (Gross, 2013).

Experts believed the StuxNet attack opened the door for a focus on the development of more sophisticated cyberattacks, largely focused on specific weapons. Iran's response was to compromise global Internet security prompting a worldwide response by Internet web browsers, such as Internet Explorer, Firefox, and Google Chrome, to update their browsers to defend against the DigiNotar attack. Subsequent attacks saw a near-perfect replication of the Wiper attack in assaulting the servers of Saudi Aramco and erasing data from over 30,000 computers in the largest attack in corporate history (Gross, 2013). Operation Ababil and "iknownoproblembro" extended this by combining DDoS and the development of a superweapon to infect global datacenters, concentrate unprecedented cyber power, and launch spectacular attacks which brought global banks to their digital knees.

The U.S. and Iran cyberwar likely continues apace, despite no prominent attacks being exposed or discussed by Iranian or U.S. officials since Shamoon and Operation Ababil. This case eschewed the conventional cyberwar and hybrid cyberwar approaches towards one which emphasized technical sophistication and geographic abstraction. Previous cyberwars, such as Estonia and Georgia, emphasized overt brute force while the case of the U.S. and Iran emphasized technical sophistication operating largely in the shadows and behind closed doors, but with devastating results.

Case Studies - Conclusion

These case studies provide three important and highly-cited examples of how cyberwar has evolved and developed from 2007 through to the present. They likewise demonstrate the ways in which power in cyberspace is practiced and realized through geographic abstraction and through a spatiality of power model rather than through rigid geographic boundaries, although targets often have a high level of geographic specificity.

Early cyberwar, in the case of Estonia, is seen as something which attempts widespread disruption and overwhelming brute force to accomplish its political aims. It leverages the global connectivity of cyberspace and lax security standards to commandeer millions of computers around the world to attack specific targets located within Estonia's sovereign territory. It is also seen as something which can be defended through embracing the spatiality of power and connecting with regional Internet power brokers in order to shield a state or region from global attack. At the same time, states may choose to turn inward, disconnecting entirely from global commerce, communications, and financial networks as Estonia ultimately was forced to. Finally, as states become more wired and dependent upon cyberspace, large scale attacks become more devastating resulting in potentially serious situations where day-to-day life is significantly affected for citizens, specifically in terms of financial transactions. The severity of these attacks and the potential for disruption of basic daily life may prompt states to seek military intervention, as Estonia attempted by considering invoking Article 5 of the NATO charter.

Later, in the case of Georgia and Russia, cyberwar was employed in support of kinetic ground conflict and seen as a force multiplier rather than something operating exclusively in cyberspace. It was seen as a means through which specific geographies could be targeted in advance or during a kinetic offensive in order to sow confusion and misinformation while exerting pressure on national political and financial elites to come to favorable terms with an invader. On the other hand, these attacks and their geographical concentrations in specific cities, for instance, can be powerful intelligence events and allow states to prepare or anticipate attacks.

A defending state such as Georgia can appeal to the global Internet to decentralize and de-territorialize its vital online services and locate them in an ostensibly neutral third country and on more resilient globally-distributed platforms. In effect, the global DDoS attacks encounter resistance and defense from global datacenters in a cyberwar waged for a specific geographically-focused area. Cyberwar is simultaneously local and global.

Finally, the United States and Iran moved cyberwar away from a very public and disruptive eye towards covert actions and the development of superweapons. The United States targeted Iran through development of the most sophisticated malware known: StuxNet. This malware was designed to identify specific industrial controllers used to power centrifuges in Iran’s Natanz nuclear facility, causing centrifuges to spin wildly and be destroyed. Additional malware, Duqu, Flame, and Wiper, were later discovered and which attempted to exfiltrate information about Iran’s nuclear program or destroy data associated with Iran’s oil industry.

In both instances, these actions again leveraged the ways in which power is spatially rather than politically-territorially distributed in cyberspace to facilitate plausible deniability while allowing for highly-focused attacks against industrial systems and compromising global Internet security in pursuit of state territorial political aims. Globally distributed command and control servers allowed for geographic obfuscation of attacks while facilitating greater insecurity through the potential for mis-attribution. Finally, the attacks took advantage of the nature of cloud computing and utilized a spatiality of power concept through focused and concentrated collections of servers and computing power to launch the largest DDoS attacks recorded.

This section discussed three of the most important and highly-cited cases of cyberwar which are notable not only for their temporal position in the history of cyberwar, but also for their novelty and how they established international precedents. These case studies sought to provide a background for the ways in which states pursue cyberwar not in the way in which they articulate their national cyberspace territorially through Internet control, but through a spatiality of power model in which power is globally distributed with shifting concentrations structured at the global level. As the spatiality of power is the dominant theme of this chapter, the geographic themes which underpin this in the case studies presented will be the subject of the final section of this chapter.

The Spatiality of Cyberwar

Background

The spatiality of power sees power as not distributed along traditional geopolitical lines whereby state boundaries are seen as rigid limits and container of power. Agnew (2003) argues that power has largely been conceived of as associated with territorial states. However, he argues that as political, economic, and technological conditions have changed throughout human history, so too have the ways in which power and space interact. Four models have been presented outlining this evolution: ensemble of worlds, field of forces, hierarchical network, and world society (Agnew, 2003). These models are equi-present, though with varying influence, with the latter two remaining the dominant ways in which the spatiality of power manifests in the present world (Agnew, 2003). This section will discuss how the spatiality of power was evidenced in each of the case studies presented.

As a note, Agnew (2003) considers the ensemble of worlds model to have less relevance in the modern world than other aspects of the spatiality of power. Likewise, this is reflected in its limited relevance in the interconnected nature of cyberwar, save for the case of Iran. Thus, discussion of the ensemble of worlds will be limited.

Russia/Estonia

The Russia and Estonia cyberwar in 2007 was primarily focused on the use of global DDoS to target the territorial Internet infrastructure of Estonia as a means to project Russian power in cyberspace. By itself, Russia would be unable to utilize computers exclusively within its territorial boundaries to launch an attack against Estonia, as there would be a clear case in which geographic attribution was certain along state-territorial lines. In order to effectively achieve its political aims in cyberspace, Russia was therefore compelled to articulate a territorial foe and use the global spatiality of power to attack that foe. The global DDoS used a large number of computers distributed around the world which were infected with malware and which were controlled through centralized command and control servers. It also relied upon “patriotic citizens” to attack Estonian targets through the use of various rudimentary scripts and programs which automated the process, making it easier for novice users.

In the ensemble of worlds model, power is articulated through profound and structural separation of human groupings, in such a way that power is concentrated and directed internally rather than externally. Human societies exist with limited communicative connectivity, something which no longer remains prevalent in the world. We can see in the Estonian case that the ensemble of worlds case is largely irrelevant and Agnew (2003) notes its general decline globally.

The field of forces model, on the other hand, seeks to locate power within territorially bound states and as such the spatiality of power is encountered with the container of the territorial state. The Estonian case demonstrates a way in which this can be untenable in cyberwar: locating power exclusively within a territorial state results in that state being identified as the attacker in cyberwar, effectively eliminating the plausible deniability which allows cyberwar to be so effective, and which specifically allowed Russia to continue its operations against Estonia. While the field of forces model argues that states form alliances in order to project power, the way power was projected by Russia in this case required the use of cyberpower resources located in states without their explicit or formal approval, as malware infects computers without permission form the user or authorities in the states in which the infections occur.

Defending states relying on power exclusively directed inward see those defenses fail when faced with the global, borderless nature of cyberwar: a solitary state must leverage the global nature of cyberspace to face global attacks, or it will disconnect and focus power inward instead. Thus, within the Estonian case we can see how this model is of limited relevance because Estonia lacked the resources and preparation to effectively counter or slow the attacks without completely disconnecting itself from the Internet. However, leveraging the technical and infrastructural expertise and cyberpower of states which are sympathetic to the defending state's cause, as demonstrated by NATO and neighboring states response to attempt to assist in Estonia's defense, does emphasize the way in which the field of forces model remains relevant within limited cases. Estonia embraced the aspect of the field of forces which necessitates that states form power blocs. Indeed, this policy continued in the aftermath of the Estonian cyberwar whereby NATO proceeded to generate rules and defensive procedures for member states.

The hierarchical model's emphasis is on specific nodes identified with cities and city-regions: “Political power is a function of where in the hierarchy of sites from global centers to rural peripheries a place is located” (Agnew, 2007b, p. 6) With regards to the Internet, then, power is akin to a flow, and congeals or spreads around various nodes and their surrounding hinterlands. Global DDoS (pre-Ababil) requires intense concentrations of humans with computing resources, thus typically situating this aspect of cyberpower within dominant global and technologically-sophisticated cities. Further, routing patterns for Internet traffic prioritize geographic proximity to major data sharing and transit hubs, evidenced in intense international competition for exporting or importing Internet connectivity (Cowie, 2011).

Thus, the hierarchical network was a spatiality of power model which Russia utilized through the subsidiary botnets it leveraged to attack Estonia. A botnet composed of rural computing power with poor connectivity would not enable Russia to mount a serious and effective attack – it must locate and situate power within existing power nodes, leveraging the connectivity between these nodes worldwide. Traditional DDoS emphasizes hierarchical networks by specifically seeing cyberspace in a way which is without territorial boundaries, and a connection of nodes of power potential to be identified, targeted, and then infected. States which have high concentrations of these resources, consequently, are not necessarily more powerful: they also have higher levels of insecurity due to the larger “cyber frontlines” in unregulated computers which may become attack vectors.

Finally, the world society model postulates a confluence of real and virtual spaces, the emergence of a global public opinion and awareness, as well as spontaneous and reciprocal time and space in global human affairs (Agnew, 2003). Indeed, the Estonian cyberwar saw the real and virtual conflated in the idea moving a bronze memorial statue prompted a retaliatory cyberwar which paralyzed real financial interactions and exchanges. The physical migrated to cyberspace which fed back into physical space; this was at once enabled through global connectivity and defended by the very global connectivity which raised awareness in distant security centers which rushed to defend Estonia**.** The simultaneity of time and space this model requires is evidenced in the globe-spanning nature of the attacks, which could occur around the clock largely without regard for geographic distance from the target, which therefore necessitated defense measures in Estonia which coincided not with Estonian spatiotemporality, but rather with the globe as a whole, at the same time. In this sense Estonia's spatiotemporality was not defined by its actual spatiotemporal location, but rather in a global sense defined by the sum total of time and space for the globe itself.

This model also postulates that actors are largely equal and unhierarchical. While the distribution of computing resources and data transfer *are* hierarchical, the actors themselves (computers) once situated within their respective hierarchical nodes are effectively unhierarchical – even a very old computer can launch a DDoS attack. This is a function of the technical simplicity of DDoS attacks in sending small requests to servers repeatedly, something which can even be effectively accomplished through mobile phones (Kumar, n.d.). Likewise, the defending actors, the targeted webservers, are comparable to regular desktop computers and laptops, thus ensuring that the conflict is between technical equal non-human actors. Further, the protocols also ensure that, at least from a foundational aspect, all actors are playing by the same rules and limits.

Russia/Georgia

The Russian/Georgian cyberwar was an example of a hybrid cyberwar, which has become an increasingly common way in which Russia has chosen to project power – evidenced most recently in Ukraine (S. Jones, 2014). This cyberwar occurred alongside a conventional kinetic conflict, and was as a force multiplier in support of ground operations to ensure information dominance. Similar to the Estonian case, this case relied upon mass global DDoS to attack targets located within Georgia, yet those targets were specified down to precise geographic coordinates in order to support Russian ground forces. As with the case of Estonia, the ensemble of worlds model is largely not applicable to the Georgian example.

The field of forces model, however, is highly relevant to this case. Similar to the case of Estonia, Russia conceived of Georgia as an explicitly state-territorial entity such that the entirety of its cyberpower was located within its territorial boundaries. It expressed state power through violating Georgia’s territorial sovereignty with a kinetic ground, naval, and air assault as well as through the domain of cyberspace. To that end, the DDoS attacks against Georgian targets were located exclusively within Georgia itself, and further territorialized through two broad emphases: state political/financial elites and local targeted attacks. Russia’s approach in cyberspace, therefore, was predicated upon an assumption that the entirety of Georgia’s cyber-assets were located within the state itself.

Defensively, the field of forces model had some relevance as Georgia conceived of other states as offering more robust protections from cyberattacks, or for being more politically sympathetic to its cause. Thus, Georgia chose to relocate services to the United States and other western liberal democracies as opposed to China, Iran, or other states with robust Internet infrastructure yet were perceived of territorially as being not politically supportive of Georgia. Despite this, the field of forces model was less relevant to the Georgian case than the other two elements of the spatiality of power.

The hierarchical network model as applicable to Georgia echoes the same ways it was applicable to Estonia, due to the fact that both relied on global DDoS as a critical component of their cyberwar. However, Russian attacks envisioned Georgia as a series of specific kinetic/cyber nodes which would be targeted for a mixture of attacks. Indeed, the attacks against Georgia were highly specific and focused on these nodes. This was compounded by Georgia's geographical location with regards to Internet infrastructure such that the resources which were infrastructurally easily available to the Estonian capital were not easily available to Georgian cities as a function of Tblisi and Gori's location within the hierarchical Internet network. Thus, Georgia was forced to relocate services closer to those locations which were more associated with political power vis-a-vis the broader global network.

In doing so, states can conceive of their geographic location as having a strong bearing on their relative power in cyberspace, despite the comparative parity of non-human actors. In other words, cyberpower is also a function of "...where in the hierarchy of sites from global centers to rural peripheries a place is located" (Agnew, 2007b, p. 6). Thus, Georgia would relocate to countries whose nodes were nearer to global centers and which would therefore have more potential bandwidth and other resources to be allocated towards defending itself from attack. Indeed, in the contemporary world of threats to human rights activists from authoritarian regimes it is recommended for activists to leverage this idea and relocate their sites to services offered by major technology companies whose resources are located closer to global centers (Zuckerman, Roberts, McGrady, York, & Palfrey, 2010).

The Georgian case is most strongly associated with the world society model, due to the first ever combination of kinetic and cyber warfare and the associated relocation of territorial cyber-assets to other states. Physical and virtual space were conflated with the case of Estonia, but this was a function of the inter-connectivity of society – specific geographies were not necessarily targeted through the virtual by virtue of their physical location. However, in the case of Georgia we can see clearly that specific cities were targeted by Russian hackers in conjunction with imminent or ongoing kinetic assaults. Further, Russian hackers conceived of both the global and the local simultaneously: using globally distributed botnets to attack cities in support of limited kinetic assault on those cities. Indeed, these attacks were found to increase in the hours before an attack, maintain a plateau during the assault, and dwindle in intensity in the hours after the assault had concluded (Bumgarner & Borg, 2009).

The implication of these attacks was to firmly locate the physical and the virtual within the same conceptual and practical categories, with no distinction being made for the idea of cyberspace as separate from physical space. They further considered the nature of global communications and sought to address this by creating information dominance within Georgia such that news about what was occurring within the country could not be reported to the world at large, shifting global perceptions of the physical conflict itself.

In response to the attacks, Georgia relocated many of its state cyber-assets to other countries, primarily the United States, by migrating hosts and moving to globally-distributed blog platforms. Prior to this, Georgian state Internet resources were located within Georgia itself, and hosted by government servers maintained by government employees. In other words, Georgian state Internet assets were associated with the territory of Georgia itself. During the attacks, however, the Georgian state was no longer able to adequately defend these sites, and was forced to relocate and reconceptualize its territory in cyberspace. As Agnew (2003) argues, the world society model articulates the idea of global public opinion and connectivity. While Russia approached the cyberwar from an approach which embodied the spatiality of power in a way unique to its regional projection of power and interests, Georgia did so defensively. The state utilized the comparatively unhierarchical structure of the Internet to relocate key assets to other states closer to key hierarchical nodes – in essence fusing these two concepts.

U.S./Iran

The previous cases emphasized global DDoS, something which had been perceived as a major threat from the earliest days of networked computing, only declining in relative importance over the past few years. As the ways in which DDoS manifested itself was understood, security firms were able to develop services to mitigate DDoS to an extent whereby DDoS is now considered something akin to civil disobedience rather than cyberwar (Himma, 2005; Oliva, 2013; O’Malley, 2013). However, this is predicated on the idea of participatory or malware-induced DDoS – as the case of Iran demonstrates new innovations in the realm of DDoS emphasize the rapidly shifting nature of cyberwar. The case of Iran is a harbinger of the future for cyberwar, as it moves from a DDoS-centric approach towards covert action, physical infrastructure destruction, and the development of cyber superweapons. To that end, the case of Iran merits greater attention than the previous cases. Cyberwar and technological development is iterative – each conflict or development informs future developments emphasized by the structural programmatic logic underpinning cyberspace.

Notably, for this dissertation, the U.S. - Iran cyberwar also demonstrates the future of geography in cyberspace, with states utilizing the cyber-geographical gap in cyberspace towards their explicit political and strategic advantage. The early attack by StuxNet, for example, utilized global command and control servers in states which were not connected to StuxNet and many which were allied to the United States, while leveraging the relative anonymity of the Internet to obfuscate its state territorial origins and facilitate plausible deniability by all states involved. The potential existed, therefore, for Iranian digital forensics to inadvertently believe that another state, such as Denmark which housed some command and control servers, was providing material support to an attack which threatened nuclear physical infrastructure or was attempting to steal state secrets. Iran would therefore be reasonably justified in retaliation, embroiling an uninvolved state in a cyberwar it neither sought nor was aware it was participating in. Indeed, Flame, Duqu, and Wiper leveraged this as well in such a way as to facilitate a state of national psychological insecurity with regards to threats in cyberspace, a nameless and stateless foe which utilized the global reach of the Internet to hide its geography yet which had a clearly articulated geographical foe.

The response by Iran likewise leveraged the spatiality of power in cyberspace to project power in cyberspace and to achieve strategic objectives through asymmetric warfare and cyberwar. The DigiNotar attack compromised global Internet security by threatening to undercut the essence of Internet security through exposing encrypted data. Indeed, Iran utilized a global approach to tap into the emails of Internet activists around the world by targeting the decentralized global nature of security certificates and web browsers. Further, if the currency of the Internet is information, then the assault on Saudi Aramco represented a new global frontier on state relationship to information: no longer considered to have value in its exfiltration, data has value in its destruction. Further, data becomes increasingly disaggregated from its territorial origins and destinations, residing on countless servers worldwide.

In contrast with the previous cases, the ensemble of worlds model has unique relevance with the case of Iran. StuxNet was developed in comparative isolation, in a secured sub-state space so that accidental leakage or inadvertent infection was impossible, allegedly at Israel's secret and unacknowledged Dimona complex in the Negev Desert (Broad et al., 2011; Zetter, 2011a). This air-gapped space, functionally disconnected from global communications was the epicenter for the development of a cyber-superweapon to target a similarly disconnected space at Iran's Natanz nuclear enrichment facility. The question of the continued relevance of the ensemble of worlds, therefore, is less a question of a broad view of human societies as Agnew (2003) argues, and instead a question of how the concept of separation and communicative isolation varies dependent on scale and purpose of human institutions.

Iran and Israel had longstanding ties and strong historical connections, in contrast to the central thesis of the ensemble of worlds. However, within these connected and networked societies there exist spaces of disconnection and isolation, which involve high levels of hierarchy and order so as to maintain their special isolation. In the post-StuxNet cyberwar interconnected environment, these ensemble spaces become increasingly valuable and due to their heightened value demonstrate the ways in which the epochs within the spatiality of power are present, albeit in limited or altered forms. Sites of immense political and military power are increasingly separated, through security protocols including air-gapped Internet communications; they represent new interpretations of the idea of ensemble of worlds.

The field of forces appears in the ways in which StuxNet was developed and targeted. As Takhteyev (2012) and Golumbia (2009) have argued software code and programming practices are embedded with the social and cultural practices of the places in which they originate. That is, the structure and logics of technologies must reflect varying political, social, and cultural assumptions and understandings (Winner, 1989). This is evidenced in the various ways in which states have constructed their national Internets, down to the local level configuration of networks (Roberts et al., 2011; Wright, 2012).

Thus, the programmers under direction from state authorities encoded specific conceptions of the geopolitical extent of Iran. Kaspersky Lab and others confirm this as the clear majority of infections of StuxNet, Flame, and Duque occurred within Iran's territorial borders (Gross, 2013). Thus, "…political boundaries provide the containers for the majority of social, economic and political activities." (Agnew, 2003, p. 130) and this is demonstrated in the precise geo-targeting of these superweapons by the United States. The political and military power the United States was targeting through StuxNet, other malware, and the attack on Kharg Island were confined purely to Iran's territory, including technologically. Malware, in other words, was encoded with geographic perceptions of the spatial extent of Iran's political power. Despite the high level of Internet interconnectivity which Iran has due to its geographical location (Cowie, 2011), nevertheless its power was conceived of as strictly and literally bounded within the conventional territorial state.

For the hierarchical network, Iran's counterattack involved attacking Saudi Aramco and launching a tightly controlled DDoS against vital U.S. financial firms. First, the attack against Saudi Aramco focused on launching a specific attack against a node in the global oil production network which was comparatively highly placed – Saudi Arabia is a major global oil producer, and Aramco is the national oil company. However, targeting Saudi Aramco was akin to targeting a periphery in the way Iran conceptualized U.S. power in terms of cores and peripheries – by striking and disabling Aramco's production through wiping out all of its data, Iran would disable a vital periphery while harming the U.S. core which was the ultimate target. Iran demonstrated a global conception of hierarchical networks, evaluating targets for comparative vulnerability and understanding that vulnerability was concentrated in peripheries – something which alarmist cyberwar scholars have long argued.

The unique nature of the retaliatory DDoS by Iran, however, emphasized aspects of both the hierarchical network and world society. Again, Iran understood that the nature of global datacenters and the “cloud” is one of a hierarchical network which sits as an infrastructural communicative underpinning for the world society model. Thus, for Iran to successfully impact the United States and its most powerful and well-secured and financed firms, it needed to embrace this vision. This was accomplished by regarding certain nodes in Internet connectivity and infrastructure as fundamentally more important and of greater value and with greater global linkages. These were targeted, infected, and used to attack the high value financial targets regardless of geographical boundaries so as to project power globally vis-a-vis the United States in cyberspace. Indeed, the geography of datacenters is often at tremendous odds with the conventional geography of computers: most of them are located in relatively remote, obscure areas housed in nondescript warehouses (Gilder, 2006; Jaeger, Lin, Grimes, & Simmons, 2009), with tens of thousands of largely homogenous computers which could be infected. A large city, on the other hand, is home to a tremendous number of computers but each computer varies significantly from the next one as no two users have identical security expertise or practices. Scale is a powerful variable in terms of cyberwar.

Throughout this cyberwar, the United States has been approaching cyberspace from an explicitly traditional geopolitical sense, practicing cyberwar within the field of forces model. It is Iran whose approach has been more thoroughly modern in its geography despite the technical advantage which the United States has in its cyber superweapons. The world society model is represented through Iran's conception of how best to impact the United States, especially envisioned through the attack on DigiNotar. It did so through utilizing computers worldwide en masse to attack the overwhelmingly powerful nodes of the United States. This attack targeted the backbone of global encrypted Internet security, prompting a worldwide response from all Internet browsers and operating systems in use in order to mitigate the damage and ensure that individuals could trust that their passwords and financial information as well as and other private information transmitted online with banks, medical institutions, social media, and ecommerce platforms was secure. Global connectivity and communications, therefore, were compromised precisely because of their global nature – the fact that the certificate authority attacked was located in the Netherlands was structurally irrelevant. Rather than situate power in cyberspace solely within the United States, Iran understood that undermining the backbone of Internet security for the globe would be far more effective than an attack just on one country. Iran's attack demonstrated that power was pooled and distributed globally, and a form of power was concentrated within certificate authorities.

The case of the U.S.-Iran cyberwar can be seen as the most complex example of cyberwar out of the three case studies, and it is acknowledged as the most important moment in the history of cyberwar (Gross, 2011). It is complex not only from a technical aspect, but from the ways in which it fully embraces a full spectrum of the spatiality of power. Each aspect is present and an important factor in offense and defense, from the hyperlocal to the global. If, as Farwell and Rohozinski (2011), argues this case is the future of cyberwar, then the future of cyberwar is one which has moved resolutely away from the explicitly territorial approach embodied in global Internet control and one in which cyberwar is practiced between states along a spatiality of power model.

The following table summarizes the case studies through the spatiality of power framework, while also providing for the similarities and differences of the cases. In doing so, the table will allow for future research to build a more geopolitical theory of cyberwar centered around the similarities and differences of the cases. This will allow for structure and process to be seen more clearly, disaggregating the geographical from the technopolitical contexts.

	Explanation	Russia/Estonia	Russia/Georgia	U.S./Iran	Differences	Similarities
Ensemble of Worlds	Power is articulated through structural separation	N/A	N/A	Stuxnet developed in and deployed against separate air-gapped spaces;	DDoS - based cyberwar relies upon connectivity rather than isolation.	Utilizing the digital to penetrate separate spaces to achieve political goals.
Field of Forces	Power located in territorial entities	Russia: N/A Estonia: Leveraged international technical alliances to stop cyberattacks	Russia: Attacks explicitly territorial Georgian cyberpower Georgia: International technical alliances to stop attacks; relocates cyber-assets to other territorial states based on alliances	Olympic Games malware (including StuxNet) deliberately targets Iran's territory; Iran's power conceived of in territorial terms	Attacks must be territorially defined; defense seeks to leverage the state monopoly over international geographical connectivity.	Cyberpower's structure is on territorial lines: alliances, targets, and infrastructure. Cyberpower must be located somewhere. Territory as "framing principle" for attack and defense.
Hierarchical Network	Emphasis on cities, nodes of power, and hinterlands	Russia: Embraces model, seeks out nodes with high connectivity to power botnet used in attacks Estonia: N/A	Russia: Envisioned cyberpower as hierarchical nodes within Georgia. Georgia: Relocated cyber-assets to other territorial states located near nodes associated with state cyberpower.	Iran's counterattacks targeted hierarchical nodes of oil and finance using hierarchical nodes of computing power (data centers)	Physical nodes of power harder to relocate than nodes associated with cyberpower.	Nodes of power become nodes of vulnerability for both attack (via botnets) and defense.
World Society	Power in social groupings, confluence of real and virtual spaces, global public opinion, as well as spontaneous and reciprocal time and space	Synchronized protests and cyberattacks; global attacks operated at a global spatiotemporality rather than a local Estonian spatiotemporality; equal and unhierarchical global actors.	Physical/virtual spaces conflated due to simultaneous cyber and kinetic attack on specific locations; using global botnets to attack specific cities prior to kinetic ground offensives; Georgian state relocates vital state cyber-assets to other states and nodes globally	Iran's DigiNotar counterattack targeted and compromised global Internet security and connectivity; conceived of and projected power globally through networks	Purely digital and hybrid conceive of global battlespace to different ends: one for disruption/attack, the other as pool of potential resources.	Envisioning global cyberspace as pool of resources or vulnerability – a global battlespace; understanding that connectivity is vulnerability; leveraging physical and virtual convergence.

Table 5: Case Studies and the Spatiality of Power

Spatiality of power - Conclusion

The purpose of this chapter has been to demonstrate how the practice of cyberwar falls along the lines of a spatiality of power model, rather than the strict territorial model of Internet control discussed in previous chapters. To accomplish this, this chapter provided an overview of the spatiality of power, discussed the means of attack and defense in cyberwar, demonstrated the spatiality of power in three key case studies, and analyzed these case studies from the spatiality of power model. In doing so, this chapter demonstrated that cyberwar as practiced by territorial states embraces a spatiality of power worldview and model, standing in strong contrast to the ways in which states actually articulate and construct their Internet through Internet control. The gap between state territorial practices in cyberspace and the ways in which states wage war in cyberspace is the cyber-geographical gap, one which contributes to greater global instability and insecurity through mis-attribution and automated defenses.

The spatiality of power argues that power is not a function of territory, but rather something which can be seen as historically and materially contingent. To that end, he proposes four models: ensemble of worlds, field of forces, hierarchical network, and the world society. Each of these models roughly corresponds with varying eras in human sociopolitical and technological development, such that the earliest eras of recorded history roughly correspond with the ensemble of worlds model of comparative isolation while modern societies echo the world society model of interconnection and global consciousness. However, human societies are largely iterative in their development, learning from past mistakes and adapting to changing conditions by repurposing the past to invent the future. Thus, each of the models exists in the world, albeit with varying degrees of influence and presence. The dominant spatiality of power at present is the world society, but hierarchical networks and the field of forces retain a strong level of influence in global affairs.

Underpinning the prevalence of the world society model is globally-integrated communications, powered by the Internet. The clear majority of world communications, finance, and media is powered by the Internet at either an overt level or through reliance on the Internet to transmit and connect globally. The communicative infrastructure of global society is the Internet: nearly 3 billion people use the Internet, and over 77% of users in the developed world use the Internet regularly (International Telecommunication Union, 2013). Globally, approximately 40% of humans use the Internet regularly, with users from the developing world doubling to almost 2 billion in just five years (International Telecommunication Union, 2013).

This high level of global interconnectivity relies on certain technical protocols and logics which facilitate that connectivity, yet which also provide the foundation for structural insecurity. The TCP/IP protocol which powers computer networking, for instance, also allows for certain exploits, such as DDoS, to exist which can overload a network and disable a server. The very nature of software code which powers the computers themselves allows for the development of both beneficial and harmful software. With global connectivity and the fungibility of software comes the potential for the development and deployment of malware. While slow to realize the potential of this level of technological malleability, states have embraced it and sought to project and access power through cyberspace.

They have done so by exploiting elements of the programmatic logic of the Internet so as to launch attacks against opponents worldwide. These attacks come in a variety of forms, including logic bombs, DDoS, and malware, with each having varying abilities to harm or disrupt normal communications across societies. States also recognized that with the ability to attack comes the ability to be attacked, and have developed a variety of means to defend their digital assets and national cyberspaces even as the project power and attack in an increasingly ageographic way.

Three case studies highlighted this, ranging from the Estonian cyberwar of 2007 to the ongoing U.S.-Iran cyberwar at present. These case studies also demonstrated how cyberwar has evolved since 2007: from DDoS, to hybrid/kinetic support, and finally to superweapons and destroying physical infrastructure remotely. The interconnected nature of the global Internet allowed states to utilize power-based resources globally so as to reach their specific political goals. In the case of Estonia, for instance, Russia leveraged global botnets of infected computers to seriously compromise Estonia's ability to process financial transactions through the entire country. Despite the fact that the conflict between Estonia and Russia was firmly grounded in traditional territorial politics, when conflict by kinetic means was deemed unsuitable, cyberwar was waged along the lines resembling the spatiality of power concept.

Each of these cases showed the contrast between state practice of cyberwar and their territorial approaches to cyberspace outlined in previous chapters. While botnets, DDoS, and malware can be limited to strict territory, especially in the case of silencing domestic opposition, they gain considerable strength and flexibility when their power is conceived of and structured globally rather than territorially. Thus, a state would see cyberspace as a potential global battlespace where threats, power, and opportunities are distributed globally and without borders with only specific concentrations occurring in different locations. The nature of global connectivity is such that even if a state seeks to target a specific territorial entity, as in the case of the U.S./Iran, to do so it must digitally traverse and thereby expose to risk all of the states which lie between the two adversaries.

This chapter has demonstrated how the spatiality of power model manifests during cyberwar between states, and the ways in which states embrace various aspects of the model depending on national objectives and political goals. While power may be conventionally and broadly conceived of territorially, its practice and distribution in the modern world is increasingly along the lines of a spatiality of power model. Nowhere is this more evident than in cyberspace, where the nature of the Internet lends itself to be seen and utilized as a global network whole rather than a set of distinct and separate national Internets.

The territorial mindset, however, has not abandoned this dream and has sought to embrace the Internet territorially through Internet control. This territorial model becomes largely nonsensical during times of cyberwar, where states must reconceptualize traditional territorial power and see power in terms of the technological limitations and global expanse of cyberspace. As evidenced in the case studies and analysis in this chapter, the idea of the territorial state and territorialized power becomes increasingly unstable in cyberspace, to the extent that other states easily infect and utilize resources located within third party states to pursue their own extra-territorial political goals through cyberwar. Thus, this chapter has identified the spatiality of power embedded within the ways in which cyberwar is conducted. In doing so, it creates juxtaposition with both traditional state territoriality as well as state attempts to reassert territory through Internet control, demonstrating the existence of the cyber-geographical gap.

Chapter 7

Conclusion

Introduction

The development of the Internet profoundly altered the geopolitical foundations of information and conflict. The ease with which information could be sent, stored, and retrieved prompted a reconfiguration in how states relate to information and to conceptions of territory in the new informational space. States perceived the Internet as an extension of sovereign territory, akin to air or sea rights, and proceeded to develop laws, policies, and technical protocols to territorialize the portions of cyberspace which they regarded as belonging to them. This has occurred through overt Internet censorship and control in states like China, Iran, Russia, France, the United Kingdom, and Germany. At the same time, states have also territorialized the Internet through the implementation of sophisticated surveillance systems and information storage, much like the United States.

Power, on the other hand, has an explicitly spatial component to it. One manifestation of the spatial extent of state power comes during war. The spatial dimension of state power has expanded beyond the physical earth to include enroll subterranean, naval, aerial, and space into the domains in which state power can be asserted through violence. This has continued in cyberspace through the advent of cyberwar, and state efforts to militarize cyberspace while projecting power across the global Internet.

At the nexus of territory and war in cyberspace exists a cyber-geographical gap: states have different spatial standards depending on the context and situation. One standard is a rigid territorial approach through Internet censorship and control which provides an equally rigid container for the state in cyberspace. For cyberwar, on the other hand, the world is a stage and states articulate power in a way which sees power as a global cyber resource rather than strictly bounded to territory. Thus, there is a fundamental disconnect between the geographies of cyberspace and the geographies of cyberwar.

The literature in academic geography and cyberwar/Internet studies has largely ignored the spatiality of cyberspace and state territory. This dissertation sought to examine the existence of this cyber-geographical gap, and to demonstrate specifically how this gap exists. The cyber-geographical gap is significant because it 1) represents the first critical geopolitical engagement with Internet filtering and cyberwar in academic geography; 2) as such, it provides a theoretical foundation for examining the nature of attribution in cyberwar; 3) it reveals a theoretical geographical instability at the nexus of traditional sovereignty and alternative spatialities of power.

Research Questions and Themes

This dissertation brought conceptual and theoretical geopolitical analysis to cyberspace and cyberwar, a first within the discipline. Beyond its academic significance, the dissertation posed two key research questions which it sought to answer: **1) Does geopolitics manifest in cyberspace? If so, how?; 2) What are the geographies of cyberwar?** These questions were answered through a series of chapters which first sought to define geopolitics and cyberwar, understand and demonstrate the territorialization of cyberspace, and finally to see the spatiality of power within cyberwar.

The Geopolitics of Cyberspace

Broadly speaking, this dissertation engaged with two themes each reflecting the research questions: Internet control and cyberwar. The first theme is articulated through the geopolitics of cyberspace, evidenced by Internet censorship and control. Geopolitics is a way humans see and construct their world through specific geographical practices and representations. Historically, these practices and representations have involved the physical world and its domains: land, sea, air, and space. Flows across these domains were subsumed and incorporated within blocks of space demarcated by borders which formed the territory over which states exerted their sovereignty. Flows of humans and capital, for example, become subsumed under the state in which they are immediately located and subject to its rules and laws.

The development of the Internet as a means to ensure the informational survival of the United States in the event of catastrophic nuclear war (Aksoy & DeNardis, 2007) created a domain in which information was spatialized. In many ways it built upon the earlier development of international postal systems, the telegraph, and the telephone where the idea of a separate domain of information and exchange had already existed in the Republic of Letters during the 17th and 18th centuries (Dalton, 2004; D. Goodman, 1994).

Mass, networked computing with near-instantaneous connectivity ensured that vast informational networks could be created across the United States and the world. These global networks became analogous to the physical terrain where flows of humans, capital, and goods had long been subjected to the territorialization and geopolitics of physical space. As these information flows gained in greater importance, states sought methods to apply a geopolitical lens to information flows. The development and implementation of Internet infrastructure and resource allocation provided a first order of territorialization by allocating technical development, domain names, IP address ranges, and autonomous systems deployment to individual states. Sub-national groups were not allowed to participate or have control over the deployment of the Internet's technical and physical resources.

In the same way that flows of nature, such as mountain ranges, plains, air, or sea, become subject to geopolitical representation and practice so as to become geopolitical, so too did the flows of information on the physical and technical infrastructure of the Internet become subject to geopolitics. Once the infrastructure, or "natural environment" of cyberspace was deployed and information began flowing, states began to assemble the practices and rhetoric needed to territorialize information and develop the geopolitics of cyberspace through Internet filtering and control.

At first, the state constructs the activity regulations, demonstrated by Goldsmith and Wu (2008) which create the social, cultural, legal, and political means through which the flow of information through its block of space can be territorialized to that state. These include outright bans on certain content in cyberspace as well as more mundane rules requiring Internet service providers to register before providing service. This is supported and reified through the technical regulations (Goldsmith & Wu, 2008) which ban specific information within certain geographies through leveraging the technical logic of the Internet to restrict or allow information. When activity and technical regulations are combined, you have an explicit territorialization of cyberspace along the lines which the state has determined.

Large bodies of research have shown the quantifiable existence of multiple Internets based on individual state attitudes towards sovereignty (Deibert et al., 2008, 2011, 2010; Deibert & Rohozinski, 2010a; Faris & Villeneuve, 2008; Murdoch & Anderson, 2008; Warf, 2011; Wright, 2012; Zittrain & Edelman, 2003). Thus, the Internet itself becomes measurably territorialized and contingent upon the geographical location from which it is accessed (Ashraf, 2011b; Burkhart, 2011), including nationally (Deibert et al., 2008, 2011, 2010) and subnationally (Wright, 2012).

Internet censorship and control create a clear geopolitics to cyberspace centered on the multiplicity of “national Internets” around the world: one for each state. States have thus replicated the existing global geopolitical order in cyberspace through the development of Internet controls which reconfigure information flows around their territorial boundaries. In the same way that other flows are influenced by the geopolitical territories they cross, information likewise embodies this longstanding trend towards territorialization, despite significant cyber-libertarian rhetoric about the Internet disrupting borders.

However, during cyberwar states articulate a different geographical logic, one which is at odds with the explicitly territorial structure which they themselves have articulated through Internet controls. Thus, the explicit geographical framing of cyberspace which states advocate for is reversed during cyberwar, the second theme of the dissertation.

The Spatiality of Cyberwar

The second theme of this dissertation focused on the ways in which cyberwar up-ends the explicitly territorial geography of cyberspace which states have created. The gap between cyberwar and Internet controls highlights a cyber-geographical gap in state behavior, with implications for security and stability in cyberspace.

As outlined in chapter 3, and with a specific focus on the philosophy of artifactual politics associated with Langdon Winner (Winner, 1980, 1989), technologies can embody and create politics and political geographies. The Internet's technical logic is political, biased towards segmentation and control of information demonstrated in the early split of ARPANET and MILNET (Roberts et al., 2011). This technological logic also enables and limits the forms of behaviors states will have in cyberspace, such as Internet control as well as cyberwar.

As defined in chapter 4, cyberwar is actions undertaken by states to alter information disrupt computer systems, networks, or Internet-connected devices belonging to or deemed critical to another target state. These actions include a large variety of methods for attack and defense. DDoS attacks, for instance, necessitate that a state see computing resources as global in scope and scale rather than restricted to any one state or region. This allows the state to both have sufficient resources to wage cyberwar, as well as to obfuscate its involvement so as to leverage the anonymity offered by the Internet. Defensive measures, for instance, can include the relocation of assets to other states, or active defenses which automatically launch counter-attacks based on automatic analysis of attack patterns and origins.

The means through which cyberwar is waged operate along geographical lines which differ substantially from the state territoriality of the conventional Internet. Methods of defense likewise embrace specific spatialities which largely see the conventional territorial state vanish. The cyberpower needed to successfully bring down American financial institutions, for example required datacenters distributed around the world in order to muster sufficient power to disrupt these organizations (Gross, 2013; Perlroth & Hardy, 2013).

The case studies cited, those of Estonia/Russia, Georgia/Russia, and the U.S./Iran show that when cyberwar erupts, states abandon conventional territory and instead embrace a model which sees the very territory they argue they are defending disappear. For example, the Russian DDoS attacks against Estonia used computers from computers located all over the world, hijacking their Internet traffic and directing it towards specific targets within Estonia itself.

It is this disappearance of the territorial state which alters the sense of power away from one where it is pooled in states and into a model which resembles the spatiality of power model outlined in chapter 2. Power in cyberspace during cyberwar is not bound to the territorial state, but instead is distributed globally in varying ways and accessed without regard for any sense of conventional political geography. This is the spatiality of power model, a model whose origins lie with Durand and Lévy (Durand et al., 1993; Lévy, 2007) and which was embraced by Agnew (2003) as a basis for this dissertation.

The spatiality of power model argues that power is fluid and ignores political boundaries, rather than something bounded by the territorial state. This model can be an alternative way to understand power, space, and the confluence of the two. It allows an envisioning of space and power as material concepts which are contingent historically on changes in human politics, economic principles, and technologies. In other words, power is arrayed differently globally than the way it is in the traditional territorial model of Internet control articulated by states.

The multiple case studies examined in this dissertation demonstrated how cyberwar is conducted, and how that conduct is at odds with the traditional territorial state because cyberwar relies upon states envisioning power in cyberspace along the lines of the spatiality of power model rather than the conventional approach to which they have attempted to subject the Internet.

Thus, Internet control and cyberwar represent two methods in which states act in cyberspace. The first, Internet control, sees states extend their existing territorial imaginings into the realm of information, similar to the ways in which it was extended into the air, sea, space, and subterranean domains. When states attempt to resolve differences through conflict in cyberspace, however, this method is completely abandoned and states embrace a model which obviates the very territorial state they seek to defend. What are the implications of this for cyberspace?

The Cyber-Geographical Gap: Implications, Discussion, & Research Questions

The cyber-geographical gap manifests itself as the conceptual space between state territorializing of cyberspace through Internet control and the aterritorial, spatiality of power model through which states approach cyberspace during cyberwar. On the one hand, states conceive of power as territorially bounded, while on the other hand states see power as not connected to territory.

At present, states around the world are actively controlling and monitoring their portion of the Internet in a way which corresponds to a territorial logic. They are extending the idea of terrestrial territory into the flow of information by constructing elaborate systems which monitor and exclude informational flows. This is supported by state laws, practice, and the increase in state intervention at the Internet policy and governance level worldwide. The territorialization of the Internet has led scholars and activists to worry that the Internet is becoming “balkanized” threatening the idea of a global Internet which fosters cross-cultural communications, as well as international trade, commerce, and finance.

On the other hand, as demonstrated in this dissertation, state perceptions of power in cyberspace do not wholly conform to the territorial state model, despite significant rhetoric and investment. During times of cyberwar, states see the Internet in its globally-distributed nature, and instead conceive of power as something distributed globally without boundaries. They seek to leverage this spatiality of power so as to pursue their own territorially-based objectives, demonstrated in the case studies of previous chapters.

As outlined in the case studies, when states appropriate the computing resources of other states for their purposes, they may inadvertently place those states at risk of retaliation or attack, especially with the growth of automated active defenses. The territorialization of cyberspace in the event of such a counter-attack then leads to the potential for an escalation to kinetic conflict or one in which significant parts of society are disrupted without recourse or acknowledgment. While states seek to ground cyberspace in territory, their actions during cyberwar betray this perspective and contribute to greater instability. An image of stability, through Internet control or heightened oversight, does nothing to change the reality associated with the ways state behave in cyberspace during cyberwar. The danger lies in the gap between these two practices within the state itself.

Indeed, although cyberwar is trumped in its lethality by nuclear and kinetic conflict it nonetheless has real-world repercussions which can include widespread destruction, financial or commercial crisis, as well as potentially fatal results for military logistics. The results in Estonia demonstrate that individuals may become unable to conduct routine financial transactions or that emergency services may be unable to function during a cyberwar. In the event of a response to another state implicated in cyberwar, the results may be similar or greater, given the increased sophistication of cyberwar weaponry after StuxNet.

This is no alarmist claim for re-creating the international state system as a means to govern the Internet. There may be no easy or quick solution, but as yet there has likewise been no acknowledgment of the dichotomy between these two state practices and their implications for the future of the state and power in cyberspace. Instability in cyberspace exists through an articulation of two competing visions of power by states. There is likewise an uncertainty in the role or existence of the state in cyberspace as well: the territorial state exists and doesn't exist in cyberspace at the same time. It exists in times of relative peace, and during times of cyberwar it appears to vanish – a state of simultaneous (non)existence is the cyber-geographical gap.

To that end, this dissertation has sought to demonstrate the existence of the gap through two research questions: **1) Does geopolitics manifest in cyberspace? If so, how?; 2) What are the geographies of cyberwar?**

The first research question, **does geopolitics manifest in cyberspace? If so, how?** was addressed through linking the state practice of Internet control to the geopolitical practices of the past. This is accomplished by understanding the ways in which the state's geographical conception has always been technologically-mediated. Whether that technology be surveying tools, the written word, human language, the state and its geopolitical foundation in borders, territory, and sovereignty has relied upon technological development to exist as an entity whose existence itself can be communicated outward. Thus, the development of surveying gives polities their first boundaries which appeal beyond the natural world to an "abstract" entity of geographical coordinates.

This is extended with the Internet, through censorship and control. Internet control was selected as the means to demonstrate territorialization in cyberspace precisely because it exists at a greater level of disconnection and abstraction from the physical state than Internet infrastructure itself. States create, maintain, and establish informational territory, borders, and sovereignty in cyberspace through the myriad technologies and legal structures which create Internet control.

Geopolitics, is a way of seeing and constructing the world through geographical representations and practices. These practices and representations exist in cyberspace as well, and most clearly demonstrate their existence in the world and realm of cyberspace through the ways in which the purely informational aspects of the Internet are territorialized through Internet control.

The second research question, **what are the geographies of cyberwar?** attempted to understand how cyberwar's geographies manifest through understanding the methods and means of attack and defense, as well as through three important case studies. During times of cyberwar, the state no longer relies on its territorial power structure as a means to wage cyberwar. In other words, those resources contained within a state's cyber boundaries are no longer the only power which a state has. In a conventional kinetic conflict, for instance, a state is largely dependent upon its domestic resources and perhaps those of sympathetic allies or other elements within states in which it is in conflict. It cannot rely on the rest of the world as a pool of power which can be drawn upon to further its political aims.

Cyberwar operates from a state perspective in a completely different way. The entire world becomes a pool of power from which the state can draw upon. Indeed, using resources located within its own territory or cyber-territory becomes problematic as it allows that state to be easily identified and targeted, essentially negating the advantages which a spatiality of power model offers. Thus, states will draw upon global connections and connectivity in furtherance of their own political goals, highlighted through the case studies in this dissertation.

For example, to cripple Estonia, Russia leveraged globally distributed botnets to attack selected targets within Estonia. This allowed for the territorial state of Russia to use computers located around the world and in other states to attack another state. The United States located command and control servers for malware to attack Iran in India, Vietnam, Belgium, the United Kingdom, the Netherlands, South Korea, Switzerland, Hong Kong, Turkey, and other states. On defense, the state of Georgia was able to relocate domestic cyber-resources to the United States and other states in a bid to stay online when it was under attack from a globally-distributed botnet. Both attacker and defender can see the Internet as a means to wage cyberwar, rendering the state in cyberspace as a transnational entity with attack and defense vectors located globally largely without political geography.

Implications and importance

This dissertation has answered the above research questions, but what are the implications of the cyber-geographical gap, and why is it important? At first, this research highlights the existence of the cyber-geographical gap between state territorial practices during times of peace and the spatiality of power, or comparatively aterritorial, practices during times of conflict. At first, these may seem like a pair of opposites, and indeed they are presented as such in this dissertation and in large bodies of academic literature which seek to pit aterritoriality vs territoriality. The presence of a pair of opposites in all aspects of life, however, often obfuscates more than it reveals. The existence of a gap between a pair of opposites is rarely seen as the answer itself, and instead policy recommendations or impact assessments, indeed even our own minds, will tend towards this binarized view rather than the conceptually difficult ambiguity which may lie before us but which is itself a possible solution and direction.

Territoriality versus spatiality of power seems to create a conflict, or an either/or proposition between different geographies of power. This conditions elements of expectations and reality, especially with comparatively solid concepts such as attribution and accountability which are foundational elements of the international state system. Indeed, much has been written and said in academic literature about the attribution problem and the role of geography in cyberspace, but perhaps it is worth considering that new and less momentarily clear notions of attribution and geography may, in fact, be the way these aspects of the international state system manifest themselves in cyberspace.

However, in the digital realm, the existence of ambiguity is the norm, and the pair of opposites reveals this. Rogers (2010) argues for the Internet to be researched on its own terms, rather than trying to subsume yet another domain of inquiry under traditional 19th century methodologies which may no longer be relevant. That is, the Internet may have methodological insights and research methods which are uniquely suited for it, that as a human-constructed domain it is worth seeing if new avenues for research present themselves. Extending this for cyberwar, Stone (2013) argues that cyberwar does exist not because it is physically violent per se, but rather that the digital changes notions of violence within the domain itself. Whereas a finger pulling a trigger constitutes the foundation of much state violence in the modern world, a finger hitting a keyboard may be the way this similar violent energy manifests itself in the human-constructed domain of cyberspace.

The implication for state behavior of the existence of the cyber-geographical gap demonstrated in this dissertation would not be an overhaul of any existing system, but perhaps an acceptance of the ambiguity inherent in cyberspace, and the recognition that this ambiguity has real-world implications - demonstrated in the case studies. Attempting to bottle cyberspace into a system of state territoriality during times of conflict can lead to misattribution and unintentional spread of cyberwar, as seen by how StuxNet was able to spread beyond Iran's borders (Gross, 2013) where it may have encountered other systems with unforeseen consequences for human life. Indeed, the spread of automated active defenses discussed in chapter 5 could lead to automatic spread of cyberwar with potentially serious consequences. Therefore, this is the importance of this dissertation: that it has demonstrated that geographical ambiguity and lack of clarity for cyberspace exists, and it need not be problematic unless it is unacknowledged.

Further, the implication that ambiguity or uncertainty may be the norm does not turn cyberspace into a libertarian free-for-all. The ambiguity of cyberspace’s geographical elements – territoriality and the spatiality of power – actually necessitates increased coordination and cooperation amongst states and a recognition of cyberspace’s unique geographical nature. Treaties about outer space, the moon, the seas, and Antarctica demonstrate that humans can recognize uniqueness and exceptions to monolithic systems and viewpoints and engage, at the minimum, in dialogue about the topic. If there is to be a clear policy recommendation from this dissertation in light of the cyber-geographical gap it has demonstrated, it would be for states to develop treaties for the conduct of war in cyberspace which do not try to reduce it to territoriality or a free-for-all. Indeed, any treaty which attempts to do so will likely create the opposite of the stability it seeks to guarantee.

In this case, what is the relationship of cyberspace to geopolitics after this dissertation? The answer to this question is an extension of the previous answer: does it make sense to see cyberspace within a sense of geopolitics at all? Can a system whose fundamental scale is global be seen within geopolitics? This dissertation has demonstrated that there is a geopolitics to cyberspace, through Internet control. But this geopolitics is a tenuous one, subject to the whims of states who embrace and discard it with ease and lack of consequences. Again, a pair of opposites emerges, and thus the answer to this question is that this dissertation has demonstrated that a single geopolitical approach to cyberspace is fundamentally misguided.

The Internet is, as any technology is, a site where ideas of the past and future collide in the present. Geopolitics as a discipline and way of seeing the world is not obsolete in the least, but as a human-vision of the world must see beyond binaries and closer to the way cyberspace works, which in this case may be instability and uncertainty without international investment in governance and multi-stakeholderism. The Internet is that site where older notions of geopolitics encounter alternative modes, seen in the existence of the cyber-geographical gap. However, the cyber-geographical gap is not a paradox or geopolitical inconsistency, but a feature of geopolitics in cyberspace and how geopolitics manifests in the digital realm. Undoubtedly much more research must be done on this aspect, incorporating Internet governance, physical infrastructure, data transit agreements, etc. before a clearer picture can be determined.

Finally, the spatiality of power model is well-suited to understanding the ways in which power manifests in cyberspace specifically, in large part because power within the model is unstable. Indeed, each of the four models present within it articulate different eras of human political, technological, and social standing. Within it are state territorial senses of power as the field of forces and more broad-based methods such as the world society model. This model represents a fruitful avenue for a preliminary demonstration of how a geopolitics of cyberspace could be constructed, one which embraces the uncertainty and fluidity which the cyber-geographical gap embraces. Indeed, even older models within the spatiality of power, such as the ensemble of worlds, are present in cyberspace as demonstrated in the case studies of chapter 6.

This dissertation does not extend or challenge the spatiality of power, but rather sees it as a means through which cyberspace could be seen with a geopolitical lens, and a model which states can embrace, allowing them to channel traditional state authority in new avenues for cyberspace so as to avoid the instability inherent in binary systems. The existence of a pair of opposites on either side of the gap is because states do not want to address the fundamental instability and insecurity of the cyber-geographical gap. The spatiality of power model is itself an unstable model, with different spatialities of power equally present, and yet this model most closely encapsulates and captures contemporary cyberspace and international affairs. Indeed, if this dissertation has demonstrated anything about the spatiality of power, it would be an embrace of this model as a potential vision for the academic geopolitics of cyberspace.

Future Research

This dissertation and its demonstration of the cyber-geographical gap is significant because: 1) it represents the first critical geopolitical engagement with Internet filtering and cyberwar in academic geography; 2) it provides a theoretical background for the problem of attribution in cyberwar; 3) it reveals a theoretical geographical instability at the nexus of traditional sovereignty and alternative spatialities of power. Below are brief notes on some potential future research avenues.

Academic geography has largely ignored cyberwar, despite billions of dollars being poured into cyberwar across the globe. The longstanding “revolution in military affairs” has led to an interconnected battlespace, one in which cyberwar can cripple military offensive operations. Indeed, the Internet is the communicative infrastructure for modern kinetic conflict as well as cyberwar. By ignoring or not engaging with this topic, academic geography has ceded significant intellectual ground to other disciplines. As this dissertation has demonstrated, there are significant geographic elements to be discussed and analyzed in cyberwar, and the importance of these elements will only increase as the Internet continues to become part of the vital communicative infrastructure of modern conflict. To that end, this dissertation represents the first significant treatment of cyberwar in academic geography.

Noticeably absent in this dissertation was an engagement with the infrastructure of cyberspace itself: the routers, datacenters, transit exchange centers, cables etc. which allow the Internet to function. The Internet's infrastructure is grounded in a clearly articulated geography, and while some early research has been conducted on this in geography, it remains an avenue which has a significant geopolitical element (Cowie, 2011). States, such as Iran, seek to build Internet infrastructure and develop comprehensive transit agreements which allow them to leverage power in Internet transit (Cowie, 2011). This avenue of research remains virtually untouched in academic geography.

This dissertation has provided two frameworks for envisioning cyberspace: the conventional territorial model of Internet censorship and control, and the spatiality of power model associated with cyberwar. These two models can be expanded and used to stimulate research which seeks to examine the ways in which Internet infrastructure intersects with the territorialization of cyberspace through Internet control, demonstrated in preliminary research by Roberts et al. (2011). Examining the geographic distribution and spatial configuration of networks within states allows for a more complete and thorough picture of how states territorialize information and cyberspace.

At the same time, this lends itself towards seeing an additional element to the geopolitical nature of cyberwar: international transit agreements and the geopolitics of Internet infrastructure. Thus, the geographical position of a state in the global configuration of Internet infrastructure can allow for an attacker to route attacks over the most efficient path to the targets, possibly opening new dimensions in cyberwar.

Future research would seek to integrate the infrastructure of the Internet into a geopolitical framework which sees both the physical and informational aspects of the Internet. This would allow for a clearer picture of the ways in which states engage with cyberspace, rather than from a purely informational approach offered in this dissertation.

Additionally, chapter 3 must be significantly extended through additional case studies in order to build a more robust theory of the territorialization of cyberspace through Internet censorship and control. I believe this to be a very fruitful avenue for future research, and indeed a topic which is virtually unstudied in academic geography and whose conceptual foundations are nowhere to be found in Internet research literature. Thus, this avenue of future research will embrace the interdisciplinary nature of the topic to bring geographical ideas outside the discipline in relation to the Internet.

Elsewhere, this dissertation also offers an elementary engagement with the geographies of attribution in cyberwar, something which has likewise been ignored in academic geography. The problem of attribution is a well-known one in cyberwar literature, and one which has continued relevance especially after the development of StuxNet. Conventional geopolitics of conflict take attribution as a feature of conflict, even in the present “hybrid conflict” between Russia and Ukraine. However, as geopolitics and the international state system has significant technological contingencies, is the idea of geopolitical attribution likewise technologically contingent?

As Stone (2013) and Rogers (2010) have argued, evaluating the digital in terms of the non-digital can lead to epistemological problems for research. Notably for this dissertation, arguing that violence on the Internet should be the same as violence off the Internet can lead to a reductive understanding of the varieties of violence. Thus, evaluating the digital in terms of the digital can lead to new insights and further allow for a critical appraisal of the merit of attribution in cyberwar. In other words, the existence of the problem of attribution in cyberwar may not be a problem, it may be an aspect or feature of cyberwar and cyberspace itself. By seeing the ways in which states are undecided on geographies of cyberspace and cyberwar in this dissertation, it provides a direction forward in moving beyond the attribution problem towards a philosophical and geographical engagement with the existence of attribution as a problem in cyberspace.

The inevitability and rapid nature of technological change may seem to bound this dissertation's relevance within the present (2015) situation of global technopolitics. Among these concerns may be the development of multiple Internets, or other measures which may render the idea of a "global Internet" dated and irrelevant. However, this dissertation points towards multiple Internets emerging, specifically in chapter 3 on the geopolitics of Internet control. Already evident is the fact that the informational environments of the world differ as a result of Internet filtering, and what Internet a user encounters varies radically dependent upon geography.

The technical protocols in place now and in the foreseeable future will largely have the same technical and protocol logics at play, limiting any sense of a radically new Internet. This has been briefly touched on by DeNardis (2009) in literature on technical "protocol politics". The capability for multiple Internets already exists, and in some spaces has already emerged –

mesh networks, for example, in addition to “national Internets” such as in Iran and air-gapped Internet spaces discussed in the dissertation. Thus, the present system and any future systems are strongly limited and bound by technological logics and infrastructures. The seeds of future Internets exist at present and are capable of being realized in the present. Thus, while the specific details of future technological developments may change, the fundamental logics and overarching view of state behavior in cyberspace and the constraints and freedoms affordable by technologies on state behavior will remain.

The existence of the cyber-geographical gap demonstrates a theoretical geographical instability at the nexus of traditional sovereignty and the spatiality of power. The binary nature of the commonly-repeated phrase “deterritorialization” is laid bare in the existence of this geographical instability. As Agnew (2009a) has argued, the existence or non-existence of sovereignty and other geopolitical elements is not a binary, but rather varies spatially even across an internationally recognized sovereign space. Thus, the existence of the cyber-geographical gap offers an avenue to examine the nature of sovereignty, borders, and territory in the 21st century through an examination of how states enact these concepts in cyberspace. As a conceptual, technological, and social frontier cyberspace offers an ability to determine the ways in which states see themselves and their relationships to other states, as they seek to form themselves anew in the digital domain.

This dissertation offered a conventional assumption of political geography by translating territorializing processes, such as borders, territory, and sovereignty into cyberspace. However, building upon Rogers’ (2010, 2013) important research on the nature of the digital and digital methods, in what ways do borders, territory, and sovereignty manifest in state practice on the

Internet apart from Internet control and cyberwar? What do these tell methods tell us about geopolitics as practiced and as enacted?

This theoretical avenue of research has been undertaken loosely by Elden (2013a) and others with volumetric geopolitics, but it stops short of advancing into cyberspace, the next great frontier for the geographic state. It is precisely the absence of critical geopolitical engagement with cyberspace in academic geography which indicates that this is a promising and fruitful domain for research. An avenue which challenges the binary understandings of territory and deterritorialization, and will offer significant insights into the nature of geopolitics in a world in which the majority of human communications, trade, finance, entertainment, culture, knowledge generation, and innovation will occur in cyberspace.

Finally, information has become highly politicized, and to such a degree that this dissertation may seem to espouse certain political or ideological perspectives. To remedy this, in future research, the history of borders would be expanded to include the ways in which certain forms of information have been historically conceived of and restricted to certain spaces (Curry, 1999). This is seen, for example, in sacred caves in which specific words can only be spoken (Sponsel, 2015). What is conceived of as speech or information has thus long been subject to varying degrees of spatialization, both conceptually and literally, and the modern Internet (and the issues in the dissertation) are in many ways a continuation of a long-standing practice in human societies.

Situating informational geographies within a larger historical and spatial context would allow the Internet to stand apart as a specific technology (or bundle of technologies) and the ways in which it enables or constricts political behavior by states in cyberspace.

This avenue implies that perhaps there is not a political or ideological perspective and rather the cyber-geographical gap represents simply how the modern Internet and state behavior in cyberspace functions. The gap becomes less a problem and more an empirical reality, as in the way technologies generally develop new sociotechnical contexts through which states navigate. This approach allows the dissertation to move from hints of being more political or ideological towards an approach which allows further research on how the Internet and its associated technologies and state behavior function rather than a statement on how it should function.

Conclusion

The territorial state embraces the Internet in two disconnected and disconcerting ways: territorially and through the spatiality of power. In cyberspace, the state exists in the cyber-geographical gap between these two approaches, being neither here nor there. The dissertation has demonstrated the existence of this gap, and it is hoped that the research and analysis presented here offer a fruitful foundation for critical geographic engagement with territory, borders, and sovereignty in cyberspace.

BIBLIOGRAPHY

Abelson, R., & Goldstein, M. (2015). Anthem Hacking Points to Security Vulnerability of Health Care Industry. *The New York Times*. Retrieved from http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Rand Corporation.

Adams, J. (2001). Virtual defense. *Foreign Affairs*, 98–112.

African Network Information Center. (2009). *Estonia Cyber Attacks 2007*. Presented at the Afrinic-11. Retrieved from http://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf

Agnew, J. (1994). The territorial trap: the geographical assumptions of international relations theory. *Review of International Political Economy*, *1*(1), 53–80.

Agnew, J. (1999). Mapping political power beyond state boundaries: territory, identity, and movement in world politics. *Millennium-Journal of International Studies*, *28*(3), 499–521.

Agnew, J. (2003). *Geopolitics: Re-visioning World Politics* (2 edition). London ; New York: Routledge.

Agnew, J. (2005). *Hegemony: The New Shape Of Global Power* (1 edition). Philadelphia: Temple University Press.

Agnew, J. (2006). Religion and geopolitics. *Geopolitics*, *11*(2), 183–191.

Agnew, J. (2007a). No borders, no nations: making Greece in Macedonia. *Annals of the Association of American Geographers*, *97*(2), 398–422.

Agnew, J. (2007b). Spatiality and territoriality in contemporary social science. *Piazzini, C. Y Montoya, V.(eds) Geopolíticas: Espacios de Poder*.

Agnew, J. (2009a). *Globalization and Sovereignty*. Lanham: Rowman & Littlefield Publishers.

Agnew, J. (2009b). Making the strange familiar: geographical analogy in global geopolitics*. *Geographical Review*, *99*(3), 426–443.

Agnew, J. (2010). Still trapped in territory? *Geopolitics*, *15*(4), 779–784.

Agnew, J., & Corbridge, S. (1995). *Mastering Space: Hegemony, Territory and International Political Economy*. London ; New York: Routledge.

Aksoy, P., & DeNardis, L. (2007). *Information Technology in Theory* (1st ed.). Course Technology.

Aldrich, R. W. (1996). *The International Legal Implications of Information Warfare*. DTIC Document.

Alexander, H. G. (Ed.). (1998). *The Leibniz-Clarke Correspondence: Together wiith Extracts from Newton's Principia and Opticks*. Manchester University Press.

Allen, P. D., & Demchak, C. C. (2003). The Palestinian-Israeli Cyberwar. *Military Review*, *83*(2), 52.

Alonso, A., & Oiarzabal, P. J. (2010). *Diasporas in the New Media Age: Identity, Politics, and Community*. University of Nevada Press.

Anderson, B. (2006). *Imagined Communities: Reflections on the Origin and Spread of Nationalism, Revised Edition* (Revised edition). London ; New York: Verso.

Ardrey, R. (1971). *The Territorial Imperative* (1st edition). Dell.

Arnbak, A., & Van Eijk, N. (2012). Certificate Authority collapse: regulating systemic vulnerabilities in the HTTPS value chain.

Arquilla, J. (2012). Cyberwar is already upon us. *Foreign Policy, 192*.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141–165.

Arthur, C. (2011). DigiNotar SSL certificate hack amounts to cyberwar, says expert. Retrieved March 10, 2015, from http://www.theguardian.com/technology/2011/sep/05/diginotar-certificate-hack-cyberwar

Aryan, S., Aryan, H., & Halderman, J. A. (2013). Internet censorship in Iran: A first look. *Free and Open Communications on the Internet, Washington, DC, USA.*

Ashraf, C. (2009). *#iranelection: The Digital Media Response to the 2009 Iranian Election*. Berkman Center for Internet & Society - Harvard University. Retrieved from https://cyber.law.harvard.edu/interactive/events/luncheons/2009/11/iranelection

Ashraf, C. (2011a). Understanding Iran's Cyberpolitical Context. Retrieved from http://advocacy.globalvoicesonline.org/2011/03/31/understanding-irans-cyberpolitical-context/

Ashraf, C. (2011b). *World Wide Web? Visualizing Spaces of Internet Censorship*. Presented at the Association of American Geographers Annual Meeting.

Austen, I. (2013, January 14). 3 Former Top Nortel Executives Are Acquitted of Fraud. *The New York Times*. Retrieved from http://www.nytimes.com/2013/01/15/technology/former-nortel-executives-acquitted.html

Baku–Tbilisi–Ceyhan pipeline. (2015, March 8). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Baku%E2%80%93Tbilisi%E2%80%93Ceyhan_pipeline&oldid=650443029

Barkham, J. (2001). Information Warfare and International Law on the Use of Force. *NYUJ Int'l L. & Pol.*, *34*, 57.

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Retrieved February 10, 2010, from https://homes.eff.org/~barlow/Declaration-Final.html

Barnes, T. J., & Farish, M. (2006). Between regions: science, militarism, and American geography from World War to Cold War. *Annals of the Association of American Geographers*, *96*(4), 807–826.

BBC. (2007, April 28). Tallinn tense after deadly riots. *BBC*. Retrieved from http://news.bbc.co.uk/2/hi/europe/6602171.stm

BBC. (2008, April 21). Russia “shot down Georgia drone.” *BBC*. Retrieved from http://news.bbc.co.uk/2/hi/7358761.stm

Beidleman, S. W. (2009). *Defining and deterring cyber war*. DTIC Document.

Beilin, J., Blake, M., Cowell, M., Fisher, D., Gilbert, S., Hanson, R., … Leavitt, A. (2009). The Iranian election on Twitter: The first eighteen days. *The Web Ecology Project*, *1*(26.06).

Beiser, V. (2010, November 1). Digital Weapons Help Dissidents Punch Holes in China’s Great Firewall. Retrieved March 14, 2015, from http://www.wired.com/2010/11/ff_firewallfighters/

Bender, B. (2012). World More Dangerous, Top General Tells Harvard. Retrieved March 16, 2015, from https://www.bostonglobe.com/news/nation/2012/04/12/world-more-dangerous-top-general-tells-harvard-world-more-dangerous-top-general-tells-harvard/XrSM8cTzyZ0YstKv36JhJN/story.html

Bendrath, R. (2001). The cyberwar debate: Perception and politics in US critical infrastructure protection. *Information & Security: An International Journal*, *7*, 80–103.

Bendrath, R., Eriksson, J., & Giacomello, G. (2007). From’cyberterrorism’to’cyberwar’, back and forth. *International Relations and Security in the Digital Age. Hrsg. von Johan Eriksson Und Giampiero Giacomello. Abingdon: Routledge*, 57–82.

Bendrath, R., & Mueller, M. (2011). The end of the net as we know it? Deep packet inspection and internet governance. *New Media & Society*, *13*(7), 1142–1160.

Bennett, W. L., Breunig, C., & Givens, T. (2008). Communication and political mobilization: Digital media and the organization of anti-Iraq war demonstrations in the US. *Political Communication*, *25*(3), 269–289.

Berkowitz, B. D. (2003). *The New Face of War: How War Will Be Fought in the 21st Century* (First Edition edition). New York: Free Press.

Berman, A. (2009). Iran's Twitter revolution'. *The Nation*, *15*.

Berman, I. (2012). The Iranian Cyber Threat to the US Homeland. *Statement before the US House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and Subcommittee on Counterterrorism and Intelligence*.

Betz, D. (2012). Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *Journal of Strategic Studies*, *35*(5), 689–711.

Beyer, J. L. (2014). The emergence of a freedom of information movement: Anonymous, WikiLeaks, the Pirate party, and Iceland. *Journal of Computer-Mediated Communication*, *19*(2), 141–154.

Bhathal, R. (2006). Astronomy in Aboriginal culture. *Astronomy & Geophysics*, *47*(5), 5.27–5.30.

Bhattacharya, U. (2009). Found in Translation » Blog Archive » Revolutionary Twitter. Retrieved April 7, 2015, from http://foundintranslation.berkeley.edu/?p=4638

Bijker, W. E., Hughes, T. P., & Pinch, T. (Eds.). (2012). *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (anniversary edition). The MIT Press.

Bilgin, M. (2007). New prospects in the political economy of inner-Caspian hydrocarbons and western energy corridor through Turkey. *Energy Policy*, *35*(12), 6383–6394.

Bin Laden, O. (2005). *Messages to the World: The Statements of Osama Bin Laden*. (B. Lawrence, Ed., J. Howarth, Trans.) (annotated edition edition). London ; New York: Verso.

Bishop, R. (2011). Project “Transparent Earth”and the Autoscopy of Aerial Targeting The Visual Geopolitics of the Underground. *Theory, Culture & Society*, *28*(7-8), 270–286.

Blank, S. (2008). Web War I: is Europe’s first information war a new kind of war? *Comparative Strategy*, *27*(3), 227–247.

Blij, H. de. (2010). *The Power of Place: Geography, Destiny, and Globalization’s Rough Landscape* (Reprint edition). Oxford; New York: Oxford University Press.

Boas, T. C. (2006). Weaving the authoritarian web: The control of Internet use in nondemocratic regimes. *How Revolutionary Was the Digital Revolution*, 361–378.

Bolt Beranek and Newman Inc. (1981). *A History of the ARPANET: The First Decade*. DARPA.

Bradbury, D. (2011). In plain view: open source intelligence. *Computer Fraud & Security*, *2011*(4), 5–9.

Bradbury, D. (2014). Unveiling the dark web. *Network Security*, *2014*(4), 14–17.

Branch, J. (2014). *The Cartographic State: Maps, Territory, and the Origins of Sovereignty*. Place of publication not identified: Cambridge University Press.

Brito, J., & Watkins, T. (2011). Loving the Cyber Bomb-The Dangers of Threat Inflation in Cybersecurity Policy.

Broad, W., Markoff, J., & Sanger, D. (2011, January 15). Stuxnet Worm Used Against Iran Was Tested in Israel. *The New York Times*. Retrieved from http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Bronk, C., & Tikk-Ringas, E. (2013). Hack or attack? Shamoon and the evolution of cyber conflict. *Shamoon and the Evolution of Cyber Conflict (Feb 01, 2013).*

Brown, D. (2006). A proposal for an international convention to regulate the use of information systems in armed conflict. *Harvard International Law Journal, 47*(1), 179–221.

Brown, N. (1990). Planetary geopolitics. *Millennium-Journal of International Studies, 19*(3), 447–460.

Bryan, J. (2010). Force multipliers: Geography, militarism, and the Bowman Expeditions. *Political Geography*, *29*(8), 414–416.

Buchan, R. (2012). Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law*, *17*(2), 212–227. http://doi.org/10.1093/jcsl/krs014

Bumgarner, J., & Borg, S. (2009). Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008. *US-CCU Special Report*.

Burkhart, N. (2011). *Visualizing Worldwide Internet Censorship and Filtered Network Access*. Presented at the Association of American Geographers Annual Meeting.

Bush, G. W. (2003). *The National Strategy to Secure Cyberspace*. Morgan James Pub.

Butler, D. L. (2001). Technogeopolitics and the struggle for control of world air routes, 1910–1928. *Political Geography, 20*(5), 635–658.

Callanan, C., Dries-Ziekenheiner, H., Escudero-Pascual, A., & Guerra, R. (2010). *Leaping over the firewall: A review of censorship circumvention tools*. Freedom House.

Campen, A. D., Dearth, D. H., & Goodden, R. T. (1996). *Cyberwar: Security, Strategy, and Conflict in the Information Age*. AFCEA International Press Fairfax, VA.

Carr, J. (2009). *Inside Cyber Warfare: Mapping the Cyber Underworld* (1st ed.). O’Reilly Media.

Caton, J. L. (2012). Beyond domains, beyond commons: context and theory of conflict in cyberspace. In *Cyber Conflict (CYCON), 2012 4th International Conference on* (pp. 1–11). IEEE.

Cha, A. E., & Nakashima, E. (2010, January 14). Google China cyberattack part of vast espionage campaign, experts say. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

Chairman of the Joint Chiefs of Staff. (2013). *Joint Publication JP 3-27 Homeland Defense 29 July 2013*. CreateSpace Independent Publishing Platform.

Chandler, A. (1993). *The visible hand*. Harvard University Press.

Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from stuxnet. *Computer*, *44*(4), 91–93.

Chien, E. (n.d.). Stuxnet: A Breakthrough. Retrieved January 24, 2015, from http://www.symantec.com/connect/blogs/stuxnet-breakthrough

Choucri, N. (2012). *Cyberpolitics in International Relations*. Cambridge, Mass: The MIT Press.

Clarke, R. A., & Knake, R. (2012). *Cyber War: The Next Threat to National Security and What to Do About It* (Reprint edition). New York: Ecco.

Clash of Civilizations. (2015, February 28). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Clash_of_Civilizations&oldid=649192807

Clayton, M. (2010, September 21). Stuxnet malware is “weapon” out to destroy ... Iran’s Bushehr nuclear plant? *Christian Science Monitor*. Retrieved from http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant

Clinton, W. J. (1996). Executive order 13010-critical infrastructure protection. *Federal Register, 61*(138), 37347–37350.

Clough, J. (2012). The Council of Europe Convention on Cybercrime: DefiningCrime'in a Digital World. In *Criminal Law Forum* (Vol. 23, pp. 363–391). Springer.

Cohen, T. (1997). *Censorship and the Regulation of Speech on the Internet*. Centre for Applied Legal Studies.

Cold War (1979–85). (2015, February 26). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Cold_War_(1979%E2%80%9385)&oldid=648987014

Constantin, L. (2010). EU Presidency Website Defaced. Retrieved January 20, 2015, from http://archive.news.softpedia.com/news/EU-Presidency-Website-Defaced-131187.shtml

Cooke, E., Jahanian, F., & McPherson, D. (2005). The zombie roundup: Understanding, detecting, and disrupting botnets. In *Proceedings of the USENIX SRUTI Workshop* (Vol. 39, p. 44).

Coppin State University. (n.d.). Common Terminology. Retrieved January 20, 2015, from http://www.coppin.edu/its/terminology

Cosgrove, D. (2003). *Apollo's Eye: A Cartographic Genealogy of the Earth in the Western Imagination*. Baltimore, Md.; London: Johns Hopkins University Press.

Cowie, J. (2011). *The Geopolitics of Internet Infrastructure*. Harvard University. Retrieved from http://cyber.law.harvard.edu/interactive/events/luncheon/2011/11/cowie

Cullum, B. (2010). Spotlighting digital activism in Vietnam. *Online Article, Http://www. Movements. Org/blog/entry/spolighting-Digital-Activism-in-vietnam/Accessed*, *21*, 2010–02.

Curry, M. R. (1999a). New technologies and the ontology of places. *Red Rock Eater Digest. URL: Http://commons. Somewhere. com/rre/1999/RRE. New. Technologies. Acnd. Html [date Visited: 4/29/03]*.

Curry, M. R. (1999b). On the possibility of democracy in a geocoded world. *Social Science Computer Review*, *17*(1), 10–15.

Curry, M. R. (2005). Toward a geography of a world without maps: lessons from Ptolemy and postal codes. *Annals of the Association of American Geographers*, *95*(3), 680–691.

Czernich, N., Falck, O., Kretschmer, T., & Woessmann, L. (2011). Broadband infrastructure and economic growth*. *The Economic Journal*, *121*(552), 505–532.

Dalton, S. (2004). *Engendering the Republic of Letters*. Montreal: Mcgill Queens Univ Pr.

Davis, J. (2007). Hackers Take Down the Most Wired Country in Europe. Retrieved January 23, 2015, from http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

Day, A. P. R. E. (2008). *The Modern Invention of Information: Discourse, History, and Power* (1st edition). Carbondale: Southern Illinois University Press.

Deane, J. (1999). Hackers deface Senate, challenge FBI. Retrieved January 20, 2015, from http://www.zdnet.com/article/hackers-deface-senate-challenge-fbi/

Deibert, R. (2003). Black code: Censorship, surveillance, and the militarisation of cyberspace. *Millennium-Journal of International Studies, 32*(3), 501–530.

Deibert, R. (2009). The geopolitics of internet control: censorship, sovereignty, and cyberspace. *The Routledge Handbook of Internet Politics,* 323–336.

Deibert, R. (2011). Towards a cyber security strategy for global civil society. *Global Information Society Watch*.

Deibert, R. (2013). *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Toronto: Signal.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2008). *Access denied: The practice and policy of global internet filtering*. Mit Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2011). *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Cambridge, MA: The MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Haraszti, M. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Mit Press.

Deibert, R., & Rohozinski, R. (2010a). Control and subversion in Russian cyberspace. In *Access controlled: The shaping of power, rights, and rule in cyberspace* (pp. 15–34).

Deibert, R., & Rohozinski, R. (2010b). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, *21*(4), 43–57.

Deibert, R., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue*, *43*(1), 3–24. http://doi.org/10.1177/0967010611431079

Deibert, R., & Villeneuve, N. (2004). Firewalls and power: An overview of global state censorship of the Internet. *Human Rights in the Digital Age. London: GlassHouse*.

Delibasis, D. (2002). The right of states to use force in cyberspace: Defining the rules of engagement. *Information & Communications Technology Law*, *11*(3), 255–268.

Delibasis, D. (2007). *The Right to National Self-Defense: In Information Warfare Operations*. Arena Books Limited.

DeLuca, C. D. (2013). Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors, The. *Pace Int'l L. Rev. Online Companion*, ii.

Demir, H. (Ed.). (2012). *Luciano Floridi's Philosophy of Technology: Critical Reflections* (2012 edition). New York: Springer.

DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance (Information Revolution and Global Politics)*. The MIT Press.

Denning, D. (2007). A View of Cyberterrorism 5 Years Later. *Internet Security: Hacking, Counterhacking, and Society*, 123.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and Netwars: The Future of Terror, Crime, and Militancy*, *239*, 288.

De Pommereau, I. (2014). Driven by fear of Russia, Estonians flock to national guard. Retrieved April 7, 2015, from http://www.dw.de/driven-by-fear-of-russia-estonians-flock-to-national-guard/a-18084627

Diamond, L. (2010). Liberation technology. *Journal of Democracy*, *21*(3), 69–83.

Diamond, L., & Plattner, M. F. (2012). *Liberation Technology: Social Media and the Struggle for Democracy*. Johns Hopkins University Press.

Diener, A. C., & Hagen, J. (2009). Theorizing borders in a “borderless world”: globalization, territory and identity. *Geography Compass, 3*(3), 1196–1216.

Diener, A. C., & Hagen, J. (2012). *Borders: A Very Short Introduction*. New York: Oxford University Press.

Diez, T. (2004). Europe’s others and the return of geopolitics. *Cambridge Review of International Affairs*, *17*(2), 319–335.

Dolman, E. C. (2002). *Astropolitik: classical geopolitics in the space age*. Psychology Press.

Dowler, L., & Sharp, J. (2001). A feminist geopolitics? *Space and Polity*, *5*(3), 165–176.

Doswald-Beck, L. (2002). Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. *Computer Network Attack and International Law*.

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, *44*(5), 643–666.

Durand, M.-F., Lévy, J., & Retaillé, D. (1993). Le monde. Espaces et systèmes.

Efrati, A., & Gorman, S. (2011). Google mail hack blamed on China. *The Wall Street Journal*.

Ehala, M. (2009). The Bronze Soldier: identity threat and maintenance in Estonia. *Journal of Baltic Studies*, *40*(1), 139–158.

Elden, S. (2007). Governmentality, calculation, territory. *Environment and Planning D*, *25*(3), 562.

Elden, S. (2009). *Terror and Territory: The Spatial Extent of Sovereignty*. Minneapolis: Univ Of Minnesota Press.

Elden, S. (2010). Land, terrain, territory. *Progress in Human Geography*, *34*(6), 799–817.

Elden, S. (2013a). Secure the volume: vertical geopolitics and the depth of power. *Political Geography*, *34*, 35–51.

Elden, S. (2013b). *The Birth of Territory*. Chicago ; London: University Of Chicago Press.

Ellul, J., & Merton, R. K. (1967). *The Technological Society*. (J. Wilkinson, Trans.). New York: Vintage Books.

Embar-Seddon, A. (2002). Cyberterrorism Are We Under Siege? *American Behavioral Scientist*, *45*(6), 1033–1043.

Embassy of the United States, London. (2013). White House Fact Sheet on US Support for Civil Society.

Engels, F. (1978). On authority. *The Marx-Engels Reader*.

Esfandiari, G. (2010, June 11). The Myths And Realities Of New Media In Iran’s Green Movement. *RadioFreeEurope/RadioLiberty*. Washington. Retrieved from http://www.rferl.org/content/Irans_Green_Movement_And_New_Media/2068714.html

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. *White Paper, Symantec Corp., Security Response*, *5*.

Farish, M. (2010). *The contours of America's cold war*. Minneapolis: University of Minnesota Press.

Faris, R., & Villeneuve, N. (2008). Measuring global Internet filtering. *Access Denied: The Practice and Policy of Global Internet Filtering*, 5–28.

Fars News. (2009). 35 million US dollars to help cyber activists against Iran. *Fars News*. Retrieved from http://www.farsnews.com/newstext.php?nn=8812120222

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555586

Faughnder, R., & Hamedy, S. (2014). Sony insider -- not North Korea -- likely involved in hack, experts say. *Los Angeles Times*. Retrieved from http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hack-inside-job-not-north-korea-20141231-story.html

Fedyszyn, T. (2010). Saving NATO: Renunciation of the Article 5 Guarantee. *Orbis*, *54*(3), 374–386.

Fidler, D. P. (2011). Was Stuxnet an act of war? Decoding a cyberattack. *Security & Privacy, IEEE*, *9*(4), 56–59.

Finin, T. (2010). Is Stuxnet a cyber weapon aimed at an Iranian nuclear site? Retrieved April 7, 2015, from http://ebiquity.umbc.edu/blogger/2010/09/23/is-stuxnet-a-cyber-weapon-aimed-at-an-iranian-nuclear-site/

Finn, P. (2007, May 3). Protesters in Moscow Harass Estonian Envoy Over Statue. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/05/02/AR2007050202547.html

Fisher, M. (2013, April 23). Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism? *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

FitzGerald, M. C. (1997). Russian views on electronic and information warfare. In *Proceedings of the third international command and control research and technology symposium: partners for the 21st Century, National Defense University* (Vol. 126).

Florida, R. L. (2002). *The rise of the creative class: and how it's transforming work, leisure, community and everyday life*. Basic books.

Foltz, A. C. (2012). Stuxnet, Schmitt Analysis, and the Cyber" Use-of-Force" Debate. *Joint Force Quarterly*, (67), 40.

Foltz, C. B. (2004). Cyberterrorism, computer crime, and reality. *Information Management & Computer Security*, *12*(2), 154–166.

Ford, P. (2001). Europe cringes at Bush "crusade"against terrorists. *Christian Science Monitor*, *19*, 2001.

Forman, S., & Barnes, J. E. (2011). Cyber-Combat: Act of War—Pentagon Sets Stage for US to Respond to Computer Sabotage with Military Force. *Wall Street Journal*, *30*.

Foster, P. (2013). "Bogus" AP tweet about explosion at the White House wipes billions off US markets. *Telegraph.co.uk*. Retrieved from http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html

Foucault, M., & Sheridan, A. (2012). *Discipline & Punish: The Birth of the Prison* (2nd edition). Vintage.

Freedom House. (2013). *Freedom on the Net 2013*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2013

Freeze, C. (2012). Canada needs to take threat of Chinese cyberespionage more seriously: former top spy. Retrieved March 6, 2014, from http://www.theglobeandmail.com/news/politics/canada-needs-to-take-threat-of-chinese-cyberespionage-more-seriously-former-top-spy/article4598561/

Friedman, T. L. (2007). *The World Is Flat 3.0: A Brief History of the Twenty-first Century* (Third Edition edition). New York, NY: Picador.

Frydman, B., & Rorive, I. (2012). Fighting Nazi and Anti-Semitic Material on the Internet: The Yahoo! Case and It's Global Implications. *Case and It's Global Implications (January 5, 2012)*.

Fukuyama, F. (2006). *The end of history and the last man*. Simon and Schuster.

Gable, K. (2009). Cyber Apocalypse now: securing the Internet against cyberterrorism and using universal jurisdiction as a deterrent.

Galperin, E., Schoen, S., & Eckersley, P. (2011). *A Post Mortem on the Iranian DigiNotar Attack*. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack

Gates, R. (2010). *Quadrennial Defense Review*. United States Department of Defense. Retrieved from http://www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.pdf

Geer Jr, D. E. (2011). Eisenhower revisited. *IEEE Security & Privacy*, (4), 88.

Gelvin, J. L. (2011). *The Modern Middle East: A History* (3 edition). New York: Oxford University Press.

Gheytanchi, E., & Kamalipour, Y. (2010). Symbols, signs, and slogans of the demonstrations in Iran. *Media, Power, and Politics in the Digital Age: The 2009 Presidential Election Uprising in Iran*, 251.

Giddens, A. (1987). *A Contemporary Critique of Historical Materialism: The nation-state and violence* (Vol. 2). Univ of California Press.

Gilder, G. (2006). The information factories. *Wired Magazine*, *14*(10), 1–5.

Gjelten, T. (2013a). Is All The Talk About Cyberwarfare Just Hype? Retrieved March 19, 2014, from http://www.npr.org/2013/03/15/174352914/is-all-the-talk-about-cyberwarfare-just-hype

Gjelten, T. (2013b). Victims Of Cyberattacks Get Proactive Against Intruders. Retrieved January 20, 2015, from http://www.npr.org/2013/02/13/171843046/victims-of-cyberattacks-now-going-on-offense-against-intruders

Glanz, J., & Markoff, J. (2011). US underwrites internet detour around censors. *The New York Times*, *1*.

Goh, G. (2013). DNS hijacking: Government needs to step in. Retrieved April 7, 2015, from https://www.digitalnewsasia.com/security/dns-hijacking-government-needs-to-step-in

Goldsmith, J. (2011). Cybersecurity treaties: a skeptical view. *Future Challenges in National Security and Law*.

Goldsmith, J., & Wu, T. (2008). *Who Controls the Internet?: Illusions of a Borderless World*. New York: Oxford University Press.

Golumbia, D. (2009). *The cultural logic of computation*. Harvard University Press.

Goodman, D. (1994). *The Republic of Letters: A Cultural History of the French Enlightenment*. Ithaca: Cornell Univ Pr.

Goodman, W. (2010). *Cyber Deterrence: Tougher in Theory than in Practice?*. DTIC Document.

Gorman, S. (2012). Chinese hackers suspected in long-term Nortel breach. *The Wall Street Journal*.

Gottmann, J. (1973). *The significance of territory*. Univ of Virginia Pr.

Gottmann, J. (1975). The evolution of the concept of territory. *Social Science Information*, *14*(3), 29–47.

Graham, S. (2004). Vertical geopolitics: Baghdad and after. *Antipode*, *36*(1), 12–23.

Grant, R., & Association, A. F. (2007). *Victory in Cyberspace*. Air Force Association.

Greenberg, L. T., Goodman, S. E., & Soo Hoo, K. J. (1998). *Information warfare and international law*. DTIC Document.

Greene, D. (2010). Russian Minority Struggles In Post-Soviet Estonia. Retrieved March 20, 2015, from http://www.npr.org/templates/story/story.php?storyId=129333023

Greenhouse, L. (1987). Computer Security Shift is Approved by Senate. *New York Times*, *24*.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Metropolitan Books.

Gregory, D. (2011). The everywhere war. *The Geographical Journal*, *177*(3), 238–250.

Grossman, L. (2009, June 17). Iran Protests: Twitter, the Medium of the Movement. *Time*. Retrieved from http://www.time.com/time/world/article/0,8599,1905125,00.html

Gross, M. J. (2011). A declaration of cyber-war. *Vanity Fair*, *53*.

Gross, M. J. (2013). Silent War. *Vanity Fair*.

Hachigian, N. (2002). The internet and power in one-party East Asian states. *Washington Quarterly*, *25*(3), 41–58.

Harknett, R. J. (1996). *Information warfare and deterrence*. US ARMY WAR COLLEGE.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2011). The Law Of Cyber Attack. *California Law Review*, *2012*, 76.

Haughney, C., & Perlroth, N. (2013, August 27). Times Site Is Disrupted in Attack by Hackers. *The New York Times*. Retrieved from http://www.nytimes.com/2013/08/28/business/media/hacking-attack-is-suspected-on-times-web-site.html

Healey, J., & Grindal, K. (Eds.). (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association.

Hearn, K., Mahncke, R. J., & Williams, P. A. (2009). Culture jamming: from activism to hactivism. In *Australian Information Warfare and Security Conference* (p. 3).

Heickerö, R. (2010). *Emerging cyber threats and Russian views on Information warfare and Information operations*.

Heidegger, M. (2003). The question concerning technology. In R. Scharff & V. Dusek (Eds.), *Philosophy of Technology: The Technological Condition - An Anthology* (pp. 252–264). Wiley-Blackwell.

Helleiner, E. (1996). *States and the reemergence of global finance: from Bretton Woods to the 1990s*. Cornell University Press.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, *4*(2).

Himma, K. E. (2005). Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified? *Available at SSRN 799545*.

Hiro, D. (1989). *The longest war: the Iran-Iraq military conflict*. Psychology Press.

Hollis, D. M. (2011). Cyberwar case study: Georgia 2008. *Journal Article| January*, *6*(11), 20am.

Horkheimer, M., & Adorno, T. W. (2007). *Dialectic of Enlightenment*. (G. S. Noerr, Ed., E. Jephcott, Trans.) (1 edition). Stanford, Calif: Stanford University Press.

Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011). When do states disconnect their digital networks? Regime responses to the political uses of social media. *The Communication Review*, *14*(3), 216–232.

Hughes, R. (2009). NATO and Cyber Defence.

Hunker, J. (2010). Cyber war and cyber power. *Issues for NATO Doctrine. Research Paper No*, 2.

Huntington, S. P. (1993). The clash of civilizations? *Foreign Affairs*, 22–49.

Hwang, T. (2007). Herdict: a distributed model for threats online. *Network Security, 2007*(8), 15–18.

Ihde, D. (1975). The experience of technology: human-machine relations. *Philosophy & Social Criticism, 2*(3), 267–279.

Ihde, D. (1978). *Technics and Praxis: A Philosophy of Technology* (1st ed.). Springer.

Ihde, D. (2003). A Phenomenology of Technics. In R. Scharff & V. Dusek (Eds.), *Philosophy of technology: the technological condition: an anthology* (pp. 507–529). Wiley-Blackwell.

International Telecommunication Union. (2012). *Russia, UAE, China, Saudia Arabia, Algeria, Sudan, and Egypt: Proposals for the Work of the Conference* (No. DT-X). World Conference on International Telecommunications (WCIT-12): International Telecommunication Union. Retrieved from http://files.wcitleaks.org/public/Merged%20UAE%20081212.pdf

International Telecommunication Union. (2013). *The World in 2013: ICT Facts and Figures*. ITU.

Jaeger, P. T., Lin, J., Grimes, J. M., & Simmons, S. N. (2009). Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. *First Monday, 14*(5).

Jakobi, A. P. (2013). Non-State Actors All Around: The Governance of Cybercrime. *The Transnational Governance of Violence and Crime: Non-State Actors in Security*, 129.

Jensen, E. T. (2002). Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense. *Stanford Journal of International Law, 38,* 207.

Johnson, P. A. (1999). *An Assessment of International Legal Issues in Information Operations*. DTIC Document.

Jones, S. (2014). Ukraine: Russia's new art of war. *Financial Times, 28*. Retrieved from http://www.ft.com/cms/s/2/ea5e82fa-2e0c-11e4-b760-00144feabdc0.html#axzz3UyH2IPIf

Jones, L., & Sage, D. (2010). New directions in critical geopolitics: an introduction. *GeoJournal, 75*(4), 315–325.

Joyner, C. C., & Lotrionte, C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, *12*(5), 825–865.

Junio, T. J. (2013). How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. *Journal of Strategic Studies*, *36*(1), 125–133.

Juris, J. S. (2005). The new digital media and activist networking within anti–corporate globalization movements. *The Annals of the American Academy of Political and Social Science*, *597*(1), 189–208.

Kaiser, R. (2015). The birth of cyberwar. *Political Geography*, *46*, 11–20.

Kalathil, S. (2003). China's new media sector: keeping the state in. *The Pacific Review*, *16*(4), 489–501.

Kamluk, V. (2011). The Mystery of Duqu: Part Six (the Command and Control servers). Retrieved from http://securelist.com/blog/incidents/31863/the-mystery-of-duqu-part-six-the-command-and-control-servers-36/

Kaplan, C. (2006). Mobility and war: the cosmic view of US air power. *Environment and Planning A*, *38*(2), 395.

Keizer, G. (2007, August 12). "Hackers" deface UN site. Retrieved January 20, 2015, from http://www.computerworld.com/article/2543082/security0/-hackers--deface-un-site.html

Keizer, G. (2008, August 12). Russian hacker "militia" mobilizes to attack Georgia. Retrieved March 24, 2015, from http://www.networkworld.com/article/2274800/lan-wan/russian-hacker--militia--mobilizes-to-attack-georgia.html

Keller, J. (2010). Evaluating Iran's Twitter Revolution. *The Atlantic*, *18*.

Kelly, K. (2011). *What Technology Wants*. New York: Penguin Books.

Kelsey, J. T. (2008). Hacking into international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare. *Michigan Law Review*, 1427–1451.

Kesan, J. P., & Hayes, C. M. (2011). Mitigative counterstriking: Self-defense and deterrence in cyberspace. *Harvard Journal of Law & Technology*, *25*, 429.

King, C. (2004, August 25). Tbilisi Blues. *Foreign Affairs*. Retrieved from http://www.foreignaffairs.com/articles/64225/charles-king/tbilisi-blues

King, C. (2008). The Five-Day War: Managing Moscow after the Georgia Crisis. *Foreign Aff.*, *87*, 2.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *107*(02), 326–343.

Klimburg, A. (2011). Mobilising cyber power. *Survival*, *53*(1), 41–60.

Kline, S. J. (1985). What Is Technology? *Bulletin of Science, Technology & Society*, *5*(3), 215–218.

Klinke, I. (2013). Chronopolitics A conceptual matrix. *Progress in Human Geography*, *37*(5), 673–690.

Kolossov, V., & O'Loughlin, J. (2011). After the Wars in the South Caucasus State of Georgia: Economic Insecurities and Migration in the" De Facto" States of Abkhazia and South Ossetia. *Eurasian Geography and Economics*, *52*(5), 631–654.

Korns, S. W., & Kastenberg, J. E. (2008). Georgia's cyber left hook. *Parameters*, *38*(4), 60–76.

Krishna-Henzel, S. F. (2007). Cybersecurity: Perspectives on the challenges of the information revolution. *Power and Security in the Information Age. Investigating the Role of the State in Cyberspace. Burlington: Ashgate*.

Kruger, L. G. (2013). Internet Governance and the Domain Name System: Issues for Congress. Congressional Research Service, Library of Congress.

Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and National Security*, 26–28.

Kugler, R. L. (2009). Deterrence of cyber attacks. *Cyberpower and National Security*, 320.

Kumar, M. (n.d.). Anonymous Hackers Develop WebLOIC DDOS Tool for Android Mobiles. Retrieved from http://thehackernews.com/2012/02/anonymous-hackers-develop-webloic-ddos.html

Kushner, D. (2013). The real story of stuxnet. *IEEE Spectrum*, *50*(3), 48–53.

Lachow, I., & Richardson, C. (2007). *Terrorist use of the Internet: The real story*. DTIC Document.

Landwehr, C. E., Bull, A. R., McDermott, J. P., & Choi, W. S. (1994). A taxonomy of computer program security flaws. *ACM Computing Surveys (CSUR)*, *26*(3), 211–254.

Langer, R. (2013). Stuxnet's Secret Twin. *Foreign Policy, November*, *19*.

Langner, R. (2010). *The short path from cyber missiles to dirty digital bombs*. Langner.

Lawson, S. (n.d.). NATO & Cyber Conflict: Background & Challenges.

Leberknight, C. S., Chiang, M., Poor, H. V., & Wong, F. (2010). A taxonomy of Internet censorship and anti-censorship. In *Fifth International Conference on FUN WITH ALGORITHMS*.

Lee, D. (2012). Flame: Attackers "sought confidential Iran data." Retrieved March 24, 2015, from http://www.bbc.com/news/technology-18324234

Lesk, M. (2007). The new front line: Estonia under cyberassault. *Security & Privacy, IEEE*, *5*(4), 76–79.

Lévy, J. (2007). Globalization as a political invention: Geographical lenses. *Political Geography*, *26*(1), 13–19.

Lewis, J., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage. *Center for Strategic and International Studies, Washington, DC*.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Rand Corporation.

Liff, A. P. (2012). Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, *35*(3), 401–428.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404.

Liska, A. (2014). *Building an Intelligence-Led Security Program* (1 edition). Waltham, MA: Syngress.

Li, Z., Liao, Q., & Striegel, A. (2009). Botnet economics: uncertainty matters. In *Managing Information Risk and the Economics of Security* (pp. 245–267). Springer.

Lotrionte, C. (2011). Active Defense for Cyber: A Legal Framework for Covert Countermeasures. In *Inside Cyber Warfare: Mapping the Cyber Underworld* (pp. 273–284).

Lüders, S. (2011). Stuxnet and the impact on accelerator control systems. *Proceedings of ICALEPCS2011, Grenoble, France*, 1285–1288.

Lungescu, O. (2004, April 7). Tiny Estonia leads internet revolution. *BBC*. Retrieved from http://news.bbc.co.uk/2/hi/europe/3603943.stm

Lynn, W. J. (2010). Defending a New Domain: The Pentagon’s Cyberstrategy. *Foreign Affairs*, 97–108.

MacKenzie, D. (1984). Marx and the Machine. *Technology and Culture*, 473–502.

Mackey, R. (2010). “Operation Payback”attacks target MasterCard and PayPal sites to avenge WikiLeaks. *New York Times*.

MacKinnon, R. (2011). China’s “Networked Authoritarianism.” *Journal of Democracy*, *22*(2), 32–46.

Mahan, A. T. (1987). *The Influence of Sea Power Upon History, 1660-1783* (New edition edition). New York: Dover Publications.

Maitland, C. F., Thomas, H. F., & Tchouakeu, L.-M. N. (2012). Internet censorship circumvention technology use in human rights organizations: an exploratory analysis. *Journal of Information Technology*, *27*(4), 285–300.

Manjikian, M. M. (2010). From global village to virtual battlespace: the colonizing of the Internet and the extension of realpolitik. *International Studies Quarterly*, *54*(2), 381–401.

Mann, M. (1984). The autonomous power of the state: its origins, mechanisms and results. *European Journal of Sociology*, *25*(02), 185–213.

Mansel, T. (2013). How Estonia became E-stonia. Retrieved January 21, 2015, from http://www.bbc.co.uk/news/business-22317297

Markoff, J. (2008). Before the gunfire, cyberattacks. *New York Times*, *12*, 27–28.

Markoff, J. (2009, March 29). Vast Spy System Loots Computers in 103 Countries. *The New York Times*. Retrieved from http://www.nytimes.com/2009/03/29/technology/29spy.html

Markoff, J. (2011, February 11). Stuxnet Software Worm Hit 5 Industrial Facilities in Iran. *The New York Times*. Retrieved from http://www.nytimes.com/2011/02/13/science/13stuxnet.html

Markoff, J. (2013, January 16). Rights Group Reports on Abuses of Surveillance and Censorship Technology. *The New York Times*. Retrieved from http://www.nytimes.com/2013/01/16/business/rights-group-reports-on-abuses-of-surveillance-and-censorship-technology.html

Marquis-Boire, M., Dalek, J., & McKune, S. (2013). *Planet blue coat: Mapping global censorship and surveillance tools*. Citizen Lab: University of Toronto.

Marx, K. (1971). *The poverty of philosophy*. New York: International Publishers.

McAuley, D. (2005). The ideology of Osama Bin Laden: Nation, tribe and world economy. *Journal of Political Ideologies*, *10*(3), 269–287.

McKitrick, J., Blackwell, J., Littlepage, F., Kraus, G., Blanchfield, R., & Hill, D. (1995). The revolution in military affairs. *Air War College Studies in National Security: Battlefield of the Future, 3*, 65–97.

Mehan, J. E. (2009). *Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger*. IT Governance Ltd.

Metz, S., & Kievit, J. (1995). *Strategy and the Revolution in Military Affairs: From Theory to Policy*. DIANE Publishing.

Michaels, J. (2013). Pentagon expands cyber-attack capabilities. *USA TODAY*. Retrieved from http://www.usatoday.com/story/news/nation/2013/04/21/pentagon-expanding-offensive-cyber-capabilities/2085135/

Milone, M. (2003). Hacktivism: Securing the national infrastructure. *Knowledge, Technology & Policy*, *16*(1), 75–103.

Moore, R. (2011). *Cybercrime: investigating high-technology computer crime*. Burlington, MA; Oxford: Anderson ; Elsevier.

Morozov, E. (2009a). Iran: Downside to the“ Twitter Revolution.” *Dissent*, *56*(4), 10–14.

Morozov, E. (2009b). Iran elections: a Twitter revolution? *The Washington Post*, *17*.

Morozov, E. (2009c). The Internet: A room of our own? *Dissent, 56*(3), 80–85. http://doi.org/10.1353/dss.0.0065

Morozov, E. (2010). Battling the Cyber Warmongers. *The Wall Street Journal, 8*.

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. PublicAffairs.

Moseley, T. M. (2007). *The nation’s guardians: America’s 21st century air force*. DTIC Document.

Moteff, J., & Parfomak, P. (2004). Critical infrastructure and key assets: definition and identification. DTIC Document.

Mowthorpe, M. (2005). The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views. *The Journal of Social, Political, and Economic Studies*, *30*(2), 137.

Mueller, M. L. (2004). *Ruling the Root: Internet Governance and the Taming of Cyberspace*. The MIT Press.

Mueller, M. L. (2013). *Networks and States: The Global Politics of Internet Governance* (Reprint edition). The MIT Press.

Mullen, M. (2011). Admiral Michael Mullen, Chairman U.S. Joint Chiefs of Staff Interview. Retrieved from http://archive.defensenews.com/article/20110710/DEFFEAT03/107100301/Adm-Michael-Mullen

Mumford, L. (1963). *Technics and Civilization - Illustrated, with a New Introduction*. Harcourt Brace & World, Inc.

Mumford, L. (1964). Authoritarian and democratic technics. *Technology and Culture*, *5*(1), 1–8.

Murdoch, S. J., & Anderson, R. (2008). Tools and technology of Internet filtering. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access Denied: The practice and policy of global internet filtering* (pp. 57–72).

Murphy, A. B. (2012). Entente territorial: Sack and Raffestin on territoriality. *Environment and Planning-Part D*, *30*(1), 159.

Nagel, T. (1989). *The View From Nowhere* (Reprint edition). New York: Oxford University Press.

Nagl, J. A., Amos, J. F., Sewall, S., & Petraeus, D. H. (2008). *The US Army/Marine Corps Counterinsurgency Field Manual*. University of Chicago Press.

Nakashima, E. (2013, March 11). U.S. publicly calls on China to stop commercial cyber-espionage, theft of trade secrets. *The Washington Post*. Retrieved from http://www.washingtonpost.com/world/national-security/us-publicly-calls-on-china-to-stop-commercial-cyber-espionage-theft-of-trade-secrets/2013/03/11/28b21d12-8a82-11e2-a051-6810d606108d_story.html

Nazario, J. (2009). Politically motivated denial of service attacks. *The Virtual Battlefield: Perspectives on Cyber Warfare*, 163–181.

Newman, D. (2006). The lines that continue to separate us: borders in ourborderless' world. *Progress in Human Geography*, *30*(2), 143–161.

Norton, Q. (2012). How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down | Threat Level | Wired.com. Retrieved October 17, 2012, from http://www.wired.com/threatlevel/2012/07/ff_anonymous/

Nunes, M. (2005). Distributed Terror and the Ordering of Networked Social Space. *Media/ Culture Journal*, *7*(6), 1–3.

Obama, B. (2013). Improving critical infrastructure cybersecurity. *Executive Order*, *13636*.

Office of the National Counterintelligence Executive. (2011). *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*. Retrieved from http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Oliva, L. (2013). Is DDoS the New "Sit-In"? Retrieved November 25, 2013, from http://motherboard.vice.com/blog/is-ddos-the-new-civil-disobedience

Ōmae, K. (1995). *The end of the nation state: The rise of regional economies*. Simon and Schuster.

O'Malley, G. (2013). Hacktivism: Cyber Activism or Cyber Crime. *Trinity CL Rev.*, *16*, 137.

Ophardt, J. A. (2010). Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke L. & Tech. Rev.*, i.

Osborne, C. (2012). Kaspersky: Shamoon malware nothing more than “quick and dirty.” Retrieved from http://www.zdnet.com/article/kaspersky-shamoon-malware-nothing-more-than-quick-and-dirty/

Ó Tuathail, G. (2005). Being geopolitical: comments on Engin Isin’s Being Political: Genealogies of Citizenship. *Political Geography*, *24*(3), 365–372.

Ó Tuathail, G. Ó., & Dalby, S. (1998). *Rethinking geopolitics*. Routledge London.

Oxman, B. H. (2006). The territorial temptation: a siren song at sea. *American Journal of International Law*, 830–851.

Painter, J. (1995). *Politics, Geography, and “Political Geography”: A Critical Perspective*. London : New York, NY: Halsted Pr.

Papacharissi, Z. (2002). The virtual sphere The internet as a public sphere. *New Media & Society*, *4*(1), 9–27.

Patrikakis, C., Masikos, M., & Zouraraki, O. (2004). Distributed Denial of Service Attacks. *The Internet Protocol Journal*, *7*(4), 13–35.

Peet, R. (1985). The social origins of environmental determinism. *Annals of the Association of American Geographers*, *75*(3), 309–333.

Perkins, R., & Neumayer, E. (2011). Is the internet really new after all? The determinants of telecommunications diffusion in historical perspective. *The Professional Geographer*, *63*(1), 55–72.

Perlroth, N. (2012, October 23). Cyberattack on Saudi Oil Firm Disquiets U.S. *The New York Times*. Retrieved from http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Perlroth, N., & Hardy, Q. (2013, January 8). Online Banking Attacks Were Work of Iran, U.S. Officials Say. *The New York Times*. Retrieved from http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html

Perlroth, N., & Sanger, D. E. (2013, March 28). Corporate Cyberattacks, Possibly State-Backed, Now Seek to Destroy Data. *The New York Times*. Retrieved from http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html

Peterson, A. (2013). How Iranian Hackers Used The Cloud To Attack Major Banks And Why It Matters. Retrieved from http://thinkprogress.org/security/2013/01/09/1424171/bank-hackings-iran-botnets-cloud/

Pfanner, E. (2012, December 13). Citing Internet Standoff, U.S. Rejects International Telecommunications Treaty. *The New York Times*. Retrieved from http://www.nytimes.com/2012/12/14/technology/14iht-treaty14.html

Plak, R. S. (2014). *Anonymous Internet: Anonymizing peer-to-peer traffic using applied cryptography*. TU Delft, Delft University of Technology.

Plato. (2009). *Phaedrus*. (R. Waterfield, Trans.) (1st ed.). Oxford University Press, USA.

Pollitt, M. M. (1998). Cyberterrorism—fact or fancy? *Computer Fraud & Security*, *1998*(2), 8–10.

Porras, P., Saidi, H., & Yegneswaran, V. (2007). *A multi-perspective analysis of the storm (peacomm) worm*. Technical report, Computer Science Laboratory, SRI International.

Prins, J. R. (2011). *DigiNotar Certificate Authority breach: ’Operation Black Tulip’*. Fox-IT.

Qiang, X. (2011). The battle for the Chinese Internet. *Journal of Democracy*, *22*(2), 47–61.

Raffestin, C. (1984). Territoriality A Reflection of the Discrepancies Between the Organization of Space and Individual Liberty. *International Political Science Review*, *5*(2), 139–146.

Rahimi, B. (2007). The politics of the Internet in Iran. *Ali Banuazizi, Professor of Political Science, Boston College, and Past President of the Middle East Studies Association Iran Is Often Seen as a Series of Frozen Images, with Angry Clerics and Anti-American Shibboleths Being the Byproducts of a Stultifying Theocratic Order. In This Path-Breaking Book, a Different Iran Comes to Life, as a Number of*, 37.

Rattray, G. J. (2001). *Strategic warfare in cyberspace*. MIT press.

Rayman, N. (2014, December 30). New Research Blames Insiders, Not North Korea, for Sony Hack. *Time*. Retrieved from http://time.com/3649394/sony-hack-inside-job-north-korea/

Reporters Without Borders. (2013). Improve your privacy and security on the Internet using Tor. Retrieved April 7, 2015, from http://wefightcensorship.org/article/improve-your-privacy-and-security-internet-using-torhtml.html

Reporters Without Borders. (2014). Enemies of the Internet 2014: entities at the heart of censorship and surveillance. Retrieved from http://12mars.rsf.org/2014-en/enemies-of-the-internet-2014-entities-at-the-heart-of-censorship-and-surveillance/

Rhoads, C., Fassihi, F., & Gonzalez, A. (2011). Iran vows to unplug internet. *Wall Street Journal, 28*.

Rid, T. (2012a). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32.

Rid, T. (2012b). Think Again: Cyberwar. Retrieved from http://foreignpolicy.com/2012/02/27/think-again-cyberwar/

Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford ; New York: Oxford University Press.

Roberts, H., Larochelle, D., Faris, R., & Palfrey, J. (2011). Mapping local Internet control. In *Computer Communications Workshop (Hyannis, CA, 2011), IEEE*.

Robertson, J., & Riley, M. (2014). Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar. Retrieved January 24, 2015, from http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

Rogers, M., & Ruppersberger, C. D. (2012). *Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE: A Report*. US House of Representatives.

Rogers, R. (2002). Operating issue networks on the Web. *Science as Culture*, *11*(2), 191–213.

Rogers, R. (2010). Internet research: The question of method—A keynote address from the YouTube and the 2008 election cycle in the United States Conference. *Journal of Information Technology & Politics*, *7*(2-3), 241–260.

Rogers, R. (2013). *Digital Methods*. The MIT Press.

Romancov, M. (2003). From Geopolitics to Astropolitics. *The New Presence*, (1-Spring), 19–21.

Rosenfield, D. K. (2009). Rethinking Cyber War. *Critical Review*, *21*(1), 77–90. http://doi.org/10.1080/08913810902812156

Rousseau, J.-J. (1987a). Discourse on the Origin of Inequality. In D. A. Cress (Ed. & Trans.), *The Basic Political Writings* (1st ed., pp. 25–110). Hackett Publishing.

Rousseau, J.-J. (1987b). *The Basic Political Writings*. (D. A. Cress, Ed. & Trans.) (1st ed.). Hackett Publishing.

Ryan, J., & Ryan, D. (2013). Neutrality in the Context of Cyberwar. *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students*, 23.

Sabadello, M. (2011). The role of new media for the democratization processes in the Arab world. *The Arab Revolutions. Reflections on the Role of Civil Society, Human Rights and New Media in* *the Transformation Processes, SAFRAN Schlaininger Arbeitspapiere Für Friedensforschung, Abrüstung Und Nachhaltige Entwicklung*, 11.

Sack, R. D. (1986). *Human Territoriality: Its Theory and History*. Cambridge Cambridgeshire ; New York: Cambridge University Press.

Sage, D. (2008). Framing space: A popular geopolitics of American manifest destiny in outer space. *Geopolitics*, *13*(1), 27–53.

Sahlins, P. (1991). *Boundaries: The Making of France and Spain in the Pyrenees* (Reprint edition). Berkeley: University of California Press.

Sanger, D. (2012). Obama order sped up wave of cyberattacks against Iran. *The New York Times*, *1*, 2012.

Sanger, D. E., & Perlroth, N. (2014, December 17). U.S. Said to Find North Korea Ordered Cyberattack on Sony. *The New York Times*. Retrieved from http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html

Sauter, M., & Zuckerman, E. (2014). *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic.

Schecter, A. (2013). Exclusive: Corporate victims of Chinese hackers speak out. Retrieved March 6, 2014, from http://rockcenter.nbcnews.com/_news/2013/02/22/17058583-exclusive-corporate-victims-of-chinese-hackers-speak-out

Schilling, J. R. (2010). *Defining Our National Cyberspace Boundaries*. Retrieved from http://stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA518322

Schmid, A. P., Jongman, A. J., & Horowitz, I. L. (2005). *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature* (2 edition). New Brunswick, N.J: Transaction Publishers.

Schmidt, A. (2013). The Estonian cyberattacks. In J. Healey & K. Grindal (Eds.), *The fierce domain–conflicts in cyberspace* (Vol. 2012, pp. 174–193).

Schmidt, M. S., & Sanger, D. E. (2014, May 19). 5 in China Army Face U.S. Charges of Cyberattacks. *The New York Times*. Retrieved from http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html

Schmitt, P. M. N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Reprint edition). Cambridge ; New York: Cambridge University Press.

Schneier, B. (2010). Threat of “cyberwar” has been hugely hyped - CNN.com. Retrieved March 19, 2014, from http://www.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/

Schnurer, E. B. (2015, January 28). E-Stonia and the Future of the Cyberstate. *Foreign Affairs*. Retrieved from http://www.foreignaffairs.com/articles/142825/eric-b-schnurer/e-stonia-and-the-future-of-the-cyberstate

Schwartz, M. (2013). Google Aurora Hack Was Chinese Counterespionage Operation. Retrieved March 17, 2015, from http://www.informationweek.com/security/attacks/google-aurora-hack-was-chinese-counteres/240155268

Scott, J. C. (2009). *The art of not being governed: An anarchist history of upland Southeast Asia*. Yale University Press New Haven, CT.

Seattle Times. (2003). Georgia’s Saakashvili backs oil-pipeline plan. *The Seattle Times*. Retrieved from http://seattletimes.com/html/nationworld/2001802162_georgia27.html

Security-in-a-Box. (2012). Remain anonymous & bypass censorship | security in-a-box. Retrieved April 7, 2015, from https://securityinabox.org/en/guide/anonymity-and-circumvention

Shachtman, N. (2009, June 16). Web Attacks Expand in Iran’s Cyber Battle (Updated Again). Retrieved March 20, 2015, from http://www.wired.com/2009/06/web-attacks-expand-in-irans-cyber-battle/

Shakarian, P. (2011). *Stuxnet: Cyberwar revolution in military affairs*. DTIC Document.

Shamah, D. (2012). Latest viruses could mean “end of world as we know it,” says man who discovered Flame. Retrieved March 6, 2014, from http://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/

Sheikholeslami, A. (2010). Iran Condemned by BBC, VOA for Blocking Broadcasts. *Bloomberg*. Retrieved from http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aRcLphJZjb64

Shichor, Y. (2010). The Digitalization of the Uyghur Diaspora. In A. Alonso & P. J. Oiarzabal (Eds.), *Diasporas in the New Media Age: Identity, Politics, and Community* (pp. 291–316).

Shirky, C. (2009). *Here Comes Everybody: The Power of Organizing Without Organizations* (Reprint edition). New York: Penguin Books.

Simonite, T. (2013, February 13). Welcome to the Malware-Industrial Complex. Retrieved May 14, 2014, from http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/

Sims, C. (2000, March 2). Japan Software Suppliers Linked to Sect. *The New York Times*. Retrieved from http://www.nytimes.com/2000/03/02/world/japan-software-suppliers-linked-to-sect.html

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: what everyone needs to know*.

Sohrabi-Haghighat, M. H., & Mansouri, S. (2010). Where is my vote? *ICT Politics in the Aftermath of Iran’s Presidential Election. International Journal of Emerging Technologies and Society*, *8*, 24–41.

Soja, E. W. (1971). The Political Organization of Space, Resource Paper No. 8.

Sood, A. K., Bansal, R., & Enbody, R. J. (2013). Cybercrime: Dissecting the State of Underground Enterprise. *Ieee Internet Computing*, *17*(1).

Spade, J. M. (2011). *China's Cyber Power and America's National Security*. DTIC Document.

Sponsel, L. E. (2015). Sacred Caves of the World: Illuminating the Darkness. In *The Changing World Religion Map* (pp. 503–522). Springer.

Sreberny, A., & Khiabany, G. (2010). *Blogistan: The Internet and Politics in Iran*. I. B. Tauris.

Standage, T. (1998). *The Victorian Internet: the remarkable story of the telegraph and the nineteenth century's online pioneers*. Weidenfeld & Nicolson London.

Stapleton-Gray, R., & Woodcock, W. (2011). National internet defense---small states on the skirmish line. *Communications of the ACM*, *54*(3), 50–55.

Stark, H. (2011). Stuxnet Virus Opens New Era of Cyber War. *Spiegel Online, 8*.

Stohl, M. (2006). Cyber terrorism: a clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, Law and Social Change*, *46*(4-5), 223–238.

Stone, J. (2013). Cyber War Will Take Place! *Journal of Strategic Studies*, *36*(1), 101–108.

Sykes, E. C. (1910). *Persia and its People* (Vol. 9). Routledge.

Sykes, P. M. (1906). A fifth journey in Persia. *The Geographical Journal*, *28*(5), 425–453.

Symantec Security Response. (2011). W32.Duqu: The Precursor to the Next Stuxnet. Retrieved from http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet

Tăbușcă, S. (2010). The Internet Access as a Fundamental Right. *Journal of Information Systems & Operations Management*, *4*(2), 206–211.

Takhteyev, Y. (2012). *Coding Places: Software Practice in a South American City*. The MIT Press.

Tanner, J. (2007, May 1). Estonia Cancels Russia Talks Over Statue. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/05/01/AR2007050101505.html

Thayer, C. A. (2014). The Apparatus of Authoritarian Rule in Vietnam. *Politics in Contemporary Vietnam: Party, State, and Authority Relations*, 135.

The Economist. (2012, December 8). Hype and fear. *The Economist*. Retrieved from http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may

Thomas, J. (2001). Ethics of Hacktivism. *Information Security Reading Room*, *12*.

Thomas, T. L. (2000). The Russian View Of Information War. *The Russian Armed Forces at the Dawn of the Millennium*, 335.

Tikk, E., Kaska, K., & Vihul, L. (2010). *International cyber incidents: Legal considerations* (Vol. 112). Cooperative Cyber Defence Centre of Excellence.

Timberg, C., & Nakashima, E. (2013, February 20). Chinese cyberspies have hacked most Washington institutions, experts say. *The Washington Post*. Retrieved from http://www.washingtonpost.com/business/technology/chinese-cyberspies-have-hacked-most-washington-institutions-experts-say/2013/02/20/ae4d5120-7615-11e2-95e4-6148e45d7adb_story.html

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. Retrieved March 21, 2015, from http://www.theguardian.com/world/2007/may/17/topstories3.russia

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, krs019. http://doi.org/10.1093/jcsl/krs019

Tsui, L. (2008). The Great Firewall as Iron Curtain 2.0: The implications of China’s Internet most dominant metaphor for US foreign policy. In *sixth annual Chinese Internet Research Conference, Hong Kong University* (pp. 13–14).

Turner, M. (n.d.). *Is There Such a Thing as a Violent Act in Cyberspace?*.

Umiltà, M. A., Intskirveli, I., Grammont, F., Rochat, M., Caruana, F., Jezzini, A., … Rizzolatti, G. (2008). When pliers become fingers in the monkey motor system. *Proceedings of the National Academy of Sciences*, *105*(6), 2209–2213.

University of Toronto. (2011). *Behind Blue Coat: Investigations of commercial filtering in Syria and Burma*. Citizen Lab.

Urban, J. M., & Quilter, L. (2006). Efficient Process or’Chilling Effects’? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act. *Santa Clara Computer and High Technology Law Journal*, *22*, 621.

U.S. Army Training and Doctrine Command. (2005). *Cyber Operations and Cyber Terrorism. DCSINT Handbook No. 1.02*. Retrieved from http://www.au.af.mil/au/awc/awcgate/army/guidterr/sup2.pdf

U.S. Department of Defense. (2006). *National Military Strategy for Cyberspace Operations*.

Van der Meulen, N. (2013). DigiNotar: Dissecting the First Dutch Digital Disaster. *Journal of Strategic Security*, *6*(2), 4.

Villeneuve, N. (2006). The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace. *First Monday*, *11*(1).

Villeneuve, N., & Crete-Nishihata, M. (2012). Control and Resistance: Attacks on Burmese Opposition Media. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (pp. 153–176).

Virilio, P. (2007). *The Original Accident*. (J. Rose, Trans.) (1 edition). Cambridge ; Malden, Mass: Polity.

Wagner, B. (2012). Push-button-autocracy in Tunisia: Analysing the role of Internet infrastructure, institutions and international markets in creating a Tunisian censorship regime. *Telecommunications Policy*, *36*(6), 484–492.

Walker, G. K. (2000). Information Warfare and Neutrality. *Vand. J. Transnat'l L.*, *33*, 1079.

Wang, X., Juffermans, K., & Du, C. (2012). Harmony as language policy in China: An Internet perspective. *Urban Languages & Literacies*.

Ware, W. H. (1967). Security and privacy in computer systems. In *Proceedings of the April 18-20, 1967, spring joint computer conference* (pp. 279–282). ACM.

Warf, B. (2011). Geographies of global Internet censorship. *GeoJournal*, *76*(1), 1–23.

Warf, B. (2015). The Hermit Kingdom in cyberspace: unveiling the North Korean internet. *Information, Communication & Society*, *18*(1), 109–120.

Warner, M. (2012). Cybersecurity: a pre-history. *Intelligence and National Security*, *27*(5), 781–799.

Warrick, J. (2011, February 16). Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

White, G., & Conklin, A. (2004). The appropriate use of force-on-force cyberexercises. *Security & Privacy, IEEE*, *2*(4), 33–37.

Williams, A. J. (2011). Reconceptualising spaces of the air: performing the multiple spatialities of UK military airspaces. *Transactions of the Institute of British Geographers*, *36*(2), 253–267.

Wilson, C. (2014). Cyber threats to critical information infrastructure. In *Cyberterrorism* (pp. 123–136). Springer.

Winner, L. (1980). Do artifacts have politics? *Daedalus*, 121–136.

Winner, L. (1989). *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (1st ed.). University Of Chicago Press.

Wittgenstein, L. (2009). *Philosophical Investigations*. (P. M. S. Hacker & J. Schulte, Eds.) (4th ed.). Wiley-Blackwell.

Wolff, J. (2014, September 10). NATO's Empty Cybersecurity Gesture. *Slate*. Retrieved from http://www.slate.com/articles/technology/future_tense/2014/09/nato_s_statement_on_cyberattacks_misses_some_fundamental_points.html

Wright, J. (2012). Regional Variation in Chinese Internet Filtering.

Wu, T. (2010). Is Internet Exceptionalism Dead? *The Next Digital Decade-Essays on the Future of the Internet*, 179.

Yang, C. T., Jia Lynn, & Tsukayama, H. (2013, December 19). Target says 40 million credit, debit cards may have been compromised in security breach. *The Washington Post*. Retrieved from http://www.washingtonpost.com/business/technology/target-data-breach-affects-40-million-accounts-payment-info-compromised/2013/12/19/5cc71f22-68b1-11e3-ae56-22de072140a2_story.html

Yin, J., & Taylor, P. M. (2008). Information operations from an Asian perspective: A comparative analysis. *Journal of Information Warfare*, *7*(1), 1–23.

Young, M. D. (2010). National Cyber Doctrine: The Missing Link in the Application of American Cyber Power. *Journal of National Security Law & Policy*, *4*, 173.

Yurcik, W. (1997). Information warfare: Legal & ethical challenges of the next global battleground. In *Proceedings of the 2nd Annual Ethics and Technology Conference (Ethics' 97). Loyola University Chicago*. Citeseer.

Zetter, K. (2011a). How digital detectives deciphered Stuxnet, the most menacing malware in history. *Wired Magazine*, *11*, 1–8.

Zetter, K. (2011b, January 17). Did a U.S. Government Lab Help Israel Develop Stuxnet? Retrieved March 24, 2015, from http://www.wired.com/2011/01/inl-and-stuxnet/

Zetter, K. (2011c, September 20). DigiNotar Files for Bankruptcy in Wake of Devastating Hack. Retrieved March 24, 2015, from http://www.wired.com/2011/09/diginotar-bankruptcy/

Zetter, K. (2011d, October 18). Son of Stuxnet Found in the Wild on Systems in Europe. Retrieved March 24, 2015, from http://www.wired.com/2011/10/son-of-stuxnet-in-the-wild/

Zetter, K. (2012, May 28). Meet "Flame," The Massive Spy Malware Infiltrating Iranian Computers. Retrieved March 24, 2015, from http://www.wired.com/2012/05/flame/

Zetter, K. (2014, November 3). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Retrieved March 24, 2015, from http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Zetter, K. (2015). The NSA Acknowledges What We All Feared: Iran Learns from US Cyberattacks. Retrieved from http://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/

Zezima, K. (2015, February 12). Obama signs executive order on sharing cybersecurity threat information. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/post-politics/wp/2015/02/12/obama-to-sign-executive-order-on-cybersecurity-threats/

Zittrain, J., & Edelman, B. G. (2003). Internet filtering in China. *IEEE Internet Computing, March/April*.

Zittrain, J., & Palfrey, J. G. (2007). Internet Filtering: The Politics and Mechanisms of Control. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access Denied: The practice and policy of global internet filtering* (pp. 29–56). Oxford Internet Institute.

Zuckerman, E., Roberts, H., McGrady, R., York, J., & Palfrey, J. G. (2010). 2010 report on distributed denial of service (ddos) attacks. *Berkman Center Research Publication*, (2010-16).