CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Institutional Repository of the Freie Universität Berlin

Cyberspace and International Relations: Rising Powers, Proxies, and Norms

Dissertation

zur Erlangung des Grades eines Doktors
Dr. rer. pol. in Politikwissenschaft
am Fachbereich "Politik- und Sozialwissenschaften"
der Freien Universität Berlin

gemäß der Promotionsordnung zum Dr. rer. pol.
vom 23. April 2008 in Verbindung mit der Ersten Ordnung
zur Änderung dieser Promotionsordnung vom 26. Juni 2012

vorgelegt von
Tim Maurer

Berlin 2019

Teil 1 von 2: **Core Material**

VORBLATT

Erstgutachter:

Prof. Dr. Sven Chojnacki

Chair of the Research Unit Peace and Conflict Studies,
Department of Political and Social Sciences,
Otto Suhr Institute of Political Science,
Freie Universität Berlin

svencho@zedat.fu-berlin.de

Zweitgutachter:

Prof. Ronald Deibert

Director, Citizen Lab,
Munk School of Global Affairs and Public Policy and Department of Political Science,
University of Toronto

r.deibert@utoronto.ca

Tag der Disputation: 13. Dezember 2019

SHORT SUMMARIES*

Short Summary (English)

Analyzing shifts of power in global affairs is no longer complete without considering cyberspace. Today more than half of the world's population has access to the Internet. As the number of people and machines connected to the Internet continues to increase, so will its strategic value and impact on international affairs. This cumulative dissertation is therefore guided by the overarching research question, "How does cyberspace affect these power shifts in global affairs?" and three main lines of inquiry pursued across this body of work. The first focuses on the transition of power among states within the context of the rising powers of Brazil, Russia, India, China, and South Africa – the BRICS – and how they engage in the contestation of cyberspace vis-à-vis the U.S. The second focuses on the diffusion of power and projection of cyber power by non-state hackers, specifically focusing on proxy relationships between such actors and states. The third analyzes the emerging normative framework governing coercive cyber power consisting of existing international law and nascent norms. The Internet has contributed to several fundamental systemic shifts in significant ways. A key finding across the three lines of inquiry is that the Internet's single most important impact with respect to the international system is its *diffusion of reach* – "the ability to cause effects remotely not only over regional but also global distances." In addition, it is clear that how governments view cyberspace with respect to their domestic political system shapes how they behave in cyberspace internationally—including the use of coercive cyber power directly and indirectly via proxies. This also helps explain the intense contestation with respect to norms for cyberspace as part of the competition between open and closed systems.

Short Summary (German)

Cyberspace hat sich zu einem wichtigen Teil in Analysen von Machtverschiebungen im internationalen System zu Beginn des 21. Jahrhunderts entwickelt. Mehr als die Hälfte der Menschheit hat heute Zugang zum Internet, dessen strategische Bedeutung mit einer zunehmenden Anzahl von Nutzern und Maschinen weiter wachsen wird. Diese kumulative Dissertation beschäftigt sich daher mit der übergreifenden Forschungsfrage „Wie beeinflusst Cyberspace Machtverschiebungen im internationalen System?" In drei Artikel und einer Monographie wird untersucht (a) warum die BRICS-Staaten sich in ihrem Verhalten im Bereich der Informations- und Telekommunikationstechnologie mit Blick auf die USA unterscheiden, (b) warum und wie Staaten über Proxybeziehungen auf nichtstaatliche Akteure zur Machtprojektion im Cyberrraum zurückgreifen und (c) wie Normen für den Cyberraum konstruiert werden und welche Rolle die Vereinten Nationen in diesem Prozess bisher spielen. Es ist klar, dass das Internet zu verschiedenen systemrelevanten Veränderungen beigetragen hat. Ein Hauptfaktor ist die *diffusion of reach* – „die Möglichkeit für Akteure Effekte aus Distanz nicht nur über regionale sondern globale Entfernungen" über das Internet zu erzeugen. Darüber hinaus lässt sich das Verhalten von Staaten auf internationaler Ebene mit Blick auf das Internet, inklusive dessen offensive Nutzung, wesentlich dadurch erklären, wie diese Regierungen den Einfluss des Internets auf ihre innerstaatlichen Verhältnisse einschätzen. Dieser Umstand erklärt auch die Anfechtung von Normen in diesem Bereich als Teil der Konfrontation zwischen offenen und geschlossen Systemen.

---

* As required per §7 (5) of the *Promotionsordnung zum Dr. rer. pol. in Politikwissenschaft des Fachbereichs Politik- und Sozialwissenschaften der Freien Universität Berlin - FU-Mitteilungen 16/2008 vom 23.04.2008.*

CUMULATIVE DISSERATION - LIST OF PUBLICATIONS

As outlined in §7 (2) (b) of the *Promotionsordnung zum Dr. rer. pol. in Politikwissenschaft des Fachbereichs Politik- und Sozialwissenschaften der Freien Universität Berlin - FU-Mitteilungen 16/2008 vom 23.04.2008,* a cumulative dissertation comprises published and/or unpublished individual pieces of work. Such a cumulative dissertation requires an overarching title, an introduction, and conjoining text that analyzes, discusses, and presents the individual pieces. As agreed with my primary supervisor, this dissertation consists of three individual articles. In accordance with §7 (3), I specify my contribution to the conceptualization, execution, and writing of the two articles written in collaboration with another scholar. Following is a list of the individual and co-authored works of my cumulative dissertation, with details regarding my contribution to the co-authored publications.

Core Articles:

1. Core Article #1:
    - Ebert, Hannes and Tim Maurer. "Contested cyberspace and rising powers." *Third World Quarterly* 34, no. 6 (2013): 1054-1074. https://doi.org/10.1080/01436597.2013.802502.*
2. Core Article #2:
    - Maurer, Tim. "'Proxies' and Cyberspace." *Journal of Conflict and Security Law* 21, no. 3 (2016): 383-403. https://doi.org/10.1093/jcsl/krw015
3. Core Article #3:
    - Maurer, Tim. "A Dose of Realism: The Contestation and Politics of Cyber Norms." *Hague Journal on the Rule of Law* (2019). https://doi.org/10.1007/s40803-019-00129-8

Supplementary Material:

- Supplementary Material #1 – Monograph:
    - Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press, 2018. https://doi.org/10.1017/9781316422724.
- Supplementary Material #2 – Annotated Literature Review:
    - Ebert, Hannes and Tim Maurer. "International Relations - Cyber Security." *Oxford Bibliographies - Oxford University Press.* Last modified January 11, 2017. https://doi.org/10.1093/OBO/9780199743292-0196.**

---

* The division of labor between the co-authors Tim Maurer and Hannes Ebert was such that I (Tim Maurer) led the research and writing for the conceptualizations of cyberspace and control in cyberspace outlined in the theory parts of the article. I also conducted the research, including the collection, analysis, process-tracing and writing, of the Internet governance and cyber-security debates for the empirical sections. A translated version of this article was published in French as Ebert, Hannes and Tim Maurer. "Revendications sur le Cyberespace et Puissances Émergentes." *Hérodote Revue de Géographie et de Géopolitique*, no. 152 (2014): 276-297.

** Developing this annotated bibliography was a highly collaborative project between the two co-authors using a shared Google Doc and frequent interactions on the phone and via email. The division of labor was such that I (Tim Maurer) was the lead for writing the following parts: Introduction; Cyberthreats and Cyberrisks; Geopolitics of Cybersecurity; and Laws, Norms, and Response Mechanisms in Cybersecurity. Hannes Ebert took the lead on: General Overviews; Journals / Online Resources and Blogs; International-Relations Perspectives on Cybersecurity; and International Institutions. With that said, the conception, development, and execution were a truly equal collaboration with the work carried out and borne equally by both scholars.

BIOGRAPHY*

Tim Maurer is Co-director of the Cyber Policy Initiative at the Carnegie Endowment for International Peace. Prior to joining Carnegie in 2015, he was Head of Research of the Cybersecurity Initiative at the New America Foundation and Director of the Global Cybersecurity Norms and Resilience Project. This followed his time at the Center for Strategic and International Studies as a Research Associate in the Technology Policy Program.

With respect to academic roles, Tim was an adjunct faculty member at American University's School of International Service teaching a course in the fall of 2017 and in the fall of 2018. From 2016-2018, he was a Visiting Scholar at the University of Michigan's Gerald R. Ford School of Public Policy and, from 2013-2016, he was a Research Fellow at the University of Toronto's Munk School of Global Affairs affiliated with its Citizen Lab.

For the past decade, his research has focused on the Internet's impact on international relations and political systems, including international norms relating to cyberspace, the Internet's impact on the exercise of power, and issues relating to actors exploiting the gray space between war and peace. His publications have appeared in peer-reviewed journals, policy and media outlets including the Washington Post, Foreign Policy, CNN, Slate, Lawfare, TIME and Jane's Intelligence Review.

Through his policy work, he participates in U.S. track 1.5 cyber dialogues and served as a member of the Freedom Online Coalition's working group "An Internet Free and Secure," the Research Advisory Network of the Global Commission on Internet Governance, and co-chaired the Advisory Board of the Global Conference on CyberSpace.

In 2018, Cambridge University Press published his monograph *Cyber Mercenaries: The State, Hackers, and Power*, a comprehensive analysis examining proxy relationships between states and hackers.

---

* As required per §7 (5) of the *Promotionsordnung zum Dr. rer. pol. in Politikwissenschaft des Fachbereichs Politik- und Sozialwissenschaften der Freien Universität Berlin - FU-Mitteilungen 16/2008 vom 23.04.2008.*

Table of Contents

1. Introduction

Today more than half of the world's population has access to the Internet.[1] As the number of people and machines connected to the Internet continues to increase, so will its strategic value and impact on international affairs. The technology's hybrid character consists of a transnational virtual structure with information travelling through undersea cables and between physical devices located in and between the territories of nation-states. Importantly, a diverse range of actors from governments to nongovernmental actors, including technology companies and individual computer experts, build, use, and can ultimately affect the structure of the Internet.

In 2010, the U.S. military declared cyberspace to be a new "domain" akin to land, sea, air, and space.[2] For the world's sole remaining superpower to declare an entirely new domain for military operations is no small feat; simply consider the bureaucratic decision-making process required to reach such a decision and the available alternatives involving fewer costs. Announced in a *Foreign Affairs* article by U.S. Deputy Secretary of Defense William J. Lynn III, the decision foreshadowed not only the new U.S. Cyber Command, which became fully operational in November 2010, but the creation, strengthening, and expansion of similar institutional structures in other countries since then.[3]

The announcement made clear that the U.S. government and military viewed the Internet not simply as another new technology in a long list of emerging technologies in recent decades, but as qualitatively different in its ability to shape society and influence international affairs. Other countries made similar statements in the years thereafter.[4] Over the past decade, the number of states developing offensive cyber capabilities[a] has quadrupled from roughly half a dozen to over thirty countries by late 2016.[5] Beyond its military relevance, discussions in Germany about the need for a 'Ministry for the Internet' and various G20 and G7 statements highlight how cyberspace has risen from an issue of low to high politics.[6] Russia's interference in the 2016 U.S. presidential election and concerns that hacking could pose a risk to the nuclear deterrence regime underscore the political ramifications the technology has had around the globe and its significance relative to international peace and security.[7]

[a] "In general, an offensive cyber operation gains access to an adversary's computer system or network and takes advantage of a vulnerability in that system or network to deliver a payload," according to Herb Lin. See Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–47. It is the payload that determines what kind of effect. In other words, "offensive cyber operation" has become a bureaucratized synonym used usually by government agencies to describe hacking.

In short, for political scientists and International Relations scholars, the Internet presents an increasingly important subject to study. This ranges from questions about how the use of the Internet influences international peace and security to how it affects political systems, democratic backsliding, and domestic discourse. Moreover, unlike other strategic domains – land, sea, air, and space – cyberspace is manmade and its very structure can therefore be changed and is subject of intense political contestation.

The Internet's global impact is occurring within the context of broader changes that affect the international order in these early years of the 21st century. Joseph Nye describes two of these changes as the *transition* of power and the *diffusion* of power.[8] The *transition* of power refers to the shift in relative power among states away from the unipolar moment of the U.S. as the sole superpower during the 1990s toward a more multipolar system. The *diffusion* of power refers to the shift in relative power from states to non-state actors. His and other similar books[9] suggest that power relations in the evolving international system are changing fundamentally, including through a diffusion of power, while also highlighting the clear need for more systematic empirical research to analyze these trends.

This cumulative dissertation engages with this research agenda guided by the overarching research question, "How does cyberspace affect these power shifts in global affairs?" The goal is to contribute to a more systematic empirical analysis examining if and how the Internet changes international affairs and to what degree the new data weakens or strengthens theories in International Relations. It builds on the growing recognition among scholars that analyzing these shifts of power in global affairs is no longer complete without considering cyberspace given that it has become a new sphere of human interaction. For example, Joseph Nye discusses the Internet's impact on international relations in his 2011 *The Future of Power* and outlines the concept of "cyberpower" in his analysis of the transition and diffusion of power in the 21st century.[10]

To achieve the dissertation's objectives, it is necessary to address the overarching question by narrowing the scope of this endeavor and dividing it into discrete lines of inquiry that guided the three core articles and supplementary material comprising this cumulative dissertation. The three lines of inquiry pursued across this body of work focus on (i) the transition of power among states and the contestation of cyberspace, (ii) the diffusion of power and projection of cyber power by non-state hackers, specifically focusing on proxy relationships between such actors and states, and

(iii) the emerging normative framework governing coercive cyber power consisting of existing international law and nascent norms.

The first article focuses on how the rising powers of Brazil, Russia, India, China, and South Africa – the BRICS – engage in the contestation of cyberspace vis-à-vis the U.S. It details the different visions for cyberspace norms and institutions with respect to the two issue areas cybersecurity and Internet governance. Contrary to expectations derived from balance of power theories, the most potent rising powers have not aligned to balance the international system's hegemon with respect to cyberspace. Russia and China actively promote their 'sovereigntist' vision, whereas Brazil, India, and South Africa demonstrate hedging behavior as 'swing states.'[11] On the one hand, the latter are drawn toward the multistakeholder governance model that emerged organically in the U.S. and on the other, their approach is shaped by counter-hegemonic interests. The research questions guiding this first line of inquiry can therefore be summed up as: what explains the difference among the BRICS grouping's cyber foreign policies and the lack of joint BRICS proposals? Why do cyber-contestation policies vary among rising powers facing the same global hegemon?

The second line of inquiry pursued in core article #2 and the monograph - supplementary material #1 - focuses on the diffusion of power, specifically how non-state actors have become more powerful relative to states through the ability to hack computer systems remotely. The research questions examined in this part of the cumulative dissertation include: Can non-state actors wield the same cyber power – and cause similar effects and harm – as states, and if so why? What kind of effects can hacking cause today? How have these new coercive global cyber capabilities become organized and why?[b] Why do states use actors detached from the state to project power? And how do states that aspire to a monopoly over the legitimate use of force pursue these efforts in the context of offensive cyber operations?

The third line of inquiry goes beyond how power is shifting among actors to an examination of the normative regime governing offensive cyber operations and norms for cyberspace. Core article #3 therefore examines the following questions: how do norms emerge for cyberspace? What has been the contribution of the UN process to the international community's understanding of norms for

[b] This question mirrors the opening line of Janice Thomson's seminal work on mercenaries published in 1994: "Why are global coercive capabilities organized the way they are?" (Thomson, Janice E. *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe*. Princeton, NJ: Princeton University Press, 1994: 3.)

cyberspace? Why did this process collapse in 2017, the very same year that two of the biggest cyber attacks to date – WannaCry and NotPetya – caused indiscriminate economic harm worldwide, each with an estimated cost of several billion U.S. dollars? And why did member states, in an unprecedented move in the UN's history, create two separate processes dedicated to the same issue in 2018?

A key finding across the three lines of inquiry is that the Internet's single most important impact with respect to the international system is what I call its *diffusion of reach* – "the ability to cause effects remotely not only over regional but also global distances"[12] through the Internet. This diffusion of actors' reach has led to a flattening of international relations, shaping the transition of power among states and the diffusion of power from states to non-state actors as well as enabling regional politics and conflicts to globalize.

Yet, an additional line of inquiry that cuts across all three other research strands investigates the question: what is cybersecurity? Research in the early stages of this dissertation project[c] indicated that the term cybersecurity and the construction of the issue as a policy area are hotly contested, both conceptually and politically, by a variety of actors. The way in which actors use various terms and the way in which they actually behave necessitated a separate line of inquiry to assess the very essence, underlying preferences, and systemic pressures that shape international relations with respect to cyberspace.

This cumulative dissertation investigates these more specific questions raised by the Internet's expansion around the globe over the last 25 years. This umbrella text discussing the combined body of work is divided into three parts. The first part seeks to answer questions regarding the relevant time span, key concepts, and why this area of study matters in the broader context of international relations. The second part presents the conceptual points of departure for the research of the three core articles and monograph, as well as the theoretical and methodological connections between the individual works comprising this cumulative dissertation. The third part highlights how this dissertation contributes to both (a) the rapidly growing body of academic literature and scholarship

[c] In 2014, I led a project and co-authored a report compiling existing definitions relating to cybersecurity. This project was in support of the Swiss chairmanship of the Organization for Security and Co-operation in Europe (OSCE) and part of the OSCE's Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. More details available at Maurer, Tim and Robert Morgus. *Compilation of Existing Cybersecurity and Information Security Related Definitions*. Washington, DC: New America, 2014. https://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/.

focusing on cyberspace as a new issue area, as well as (b) the broader political science and International Relationship scholarship, namely its investigation of conflict and coercion in the 21st century, new forms of governance, and the construction, diffusion and translation of norms with respect to emerging technologies.

1.1. What Time Span is Relevant? The Internet's Global Expansion of the Past 25 Years

The U.S. government's announcement in 2010 regarding the designation of cyberspace as a new military domain is even more remarkable because it took place only 15 years after the birth of the 'modern Internet,' demonstrating the breathtaking pace at which the technology has influenced societies worldwide. The year 1995 has been called "year zero" in the history of the Internet because it marks the dividing point from its prehistoric days as a research network used by academics dating back to the 1960s to the open network and backbone for global communication, commerce, and trade that the modern Internet has since become.[13]

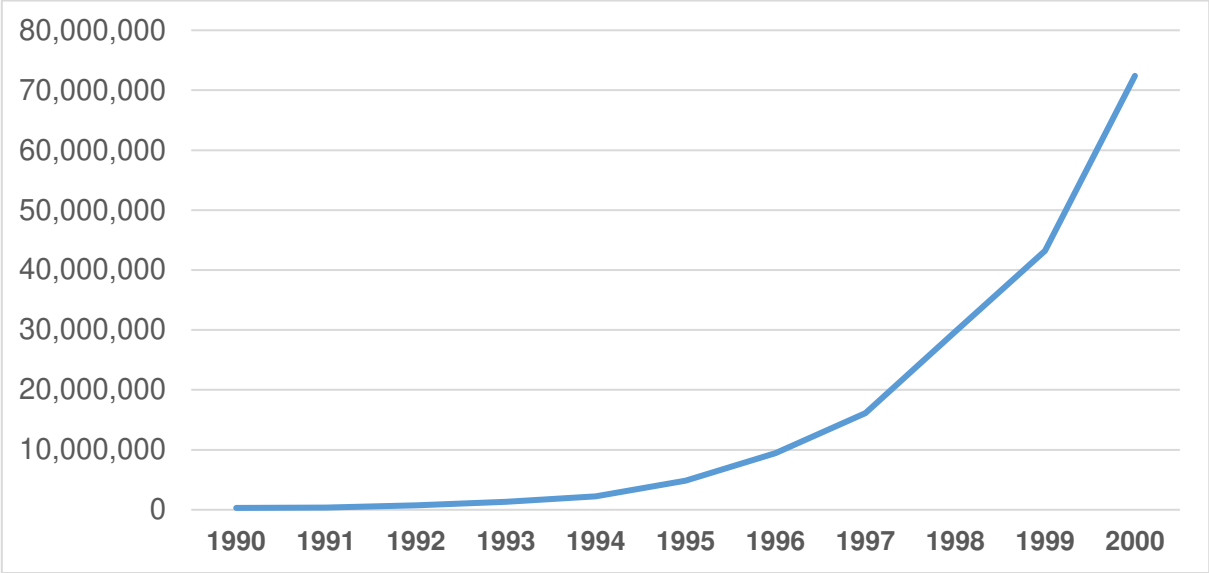
In 1995, the Internet formally transitioned from a research network[d] to commercial use, thus driving the technology's global expansion.[14] Only three years earlier, Tim Berners-Lee had developed the World Wide Web, which increased the Internet's accessibility and utility and paved the way for the so-called "Dot-Com" or "Internet" bubble in the late 1990s, subsequently raising awareness of the Internet's growing economic relevance.[15] Table 1 illustrates this exponential growth of Internet host servers.

From an International Relations scholarship perspective, the beginning of the modern Internet in 1995 constitutes a useful starting point for the research on the Internet generally and for this cumulative dissertation, specifically. It was during this period that many countries established their first Internet connection to the rest of the network. China, for example, connected to the Internet in 1994.[16] And as the Internet's commercial use started fueling its exponential transnational growth, the Internet's economic and political impact multiplied.[17] It also did not take long for the technology's potential military use to become evident. During the Kosovo war in 1999, the U.S.

[d] The decommissioning of the U.S. National Science Foundation Network (NSFNET) backbone is usually considered the formal marker for this transition in Internet's history. More details are available at: National Science Foundation. "A Brief History of NSF and the Internet." Updated August 13, 2003. https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050.

military penetrated military air defense systems and considered other attack options for its hackers - ultimately previewing the Pentagon's announcement in 2010.[18]

Figure 1. ***Growth of the Number of Internet Hosts Worldwide (1990-2000)***[19]



1.2. What Are We Talking About 1.0: The Internet vs Cyberspace

'What is the Internet?' is not a trivial question, neither from a technical or a societal or political perspective. Technically, the Internet is defined by the Internet Protocol that is its technical core and differentiates it from other similar technologies. During the 1980s, some institutions used a different network, not the Internet, to communicate with each other across countries. This other network was based on the X.25 protocol, which was eventually displaced by the IP/TCP protocol. The latter now forms the core of the Internet today after a period of contestation between the two competing standards.[20] Functionally, it is the Internet's modular architecture, which can be visualized as an hourglass with the Internet Protocol at its center, that gave it an advantage over other protocols and enabled its broader adoption and global expansion.[21]

As more and more users connected to the Internet and started using it for different social purposes, another term quickly gained traction: cyberspace. Often used synonymously with the Internet - including in this dissertation - the term 'cyberspace' has also been a source of debate. The prefix *cyber* generally refers to computer- and electronic-centered technologies.[22] It is commonly understood as "relating to or characteristic of the culture of computers, information technology, and

virtual reality."[23] Yet, definitions of *cyber*space are disputed both analytically and politically, and the contested nature of the concept has ontological implications for "what and whom we consider to be actors in cyberspace" and "for the operations of power, as it determines the purview of cyberspace strategies and the operations of cyber-power."[24]

Myriam Dunn-Cavelty was one of the first scholars to scrutinize the term cyberspace and cybersecurity through the lens of Securitization Theory.[25] The terms can be traced from their origins in fiction to its popularization by libertarian John Perry Barlow through his 'Declaration of the Independence of Cyberspace' to its adoption by actors advancing a national security agenda.[26] In Washington, cyberspace and cybersecurity became new buzzwords, partly the result of a marketing push by private military and security contractors in the first decade of the 21st century. In the meantime, no standard definition of 'cyberspace' has emerged. Instead, my aforementioned comprehensive review of definitions in 2014 found several dozen different definitions of 'cyberspace' used by governments, academics, even technical bodies, including different definitions outlined within the same government by different agencies.[27]

The most technically accurate definitions for the Internet and for cyberspace are arguably the ones provided by the Internet Engineering Task Force (IETF) and the International Organization for Standardization (ISO). The IETF defines the Internet as "the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks."[28] The ISO defines cyberspace as "The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."[29] These narrow definitions focus on the purely social and virtual realm between hardware components of computer networks, which are manifested in acts of human communication and the minds of the users.[30] In contrast, broader conceptualizations include the infrastructure layer necessary for the social communication to flow.[31] Such inclusive models imply a multi-layered structure of cyberspace distinguishing between the "physical layer" at the bottom followed by the "protocol layer," the "application layer," the "content layer," and finally the "social layer".[32] This approach posits that cyberspace is "a unique hybrid regime of physical and virtual properties."[33]

Importantly, unlike the other strategic domains – land, sea, air, and space - cyber*space* is not only a geographical space but is manmade. While it is nearly impossible to change the shape of continents or oceans, the architecture of cyberspace is changeable, as are the social and functional relations

based on its technical design. To use the chessboard analogy, the design of each chessboard is already determined with respect to land, sea, air, and space. Human interactions and the exercise of power is therefore limited to changing the rules of the game but not the game board itself. With respect to the Internet, actors can alter the physical infrastructure, the protocol, or the content layers to not only change the rules of the game but the game itself, which is illustrated by the contestation over data sovereignty and the debate over the rise of a "cybered Westphalian age."[34] Core article #3 and the contestation of the Internet's multistakeholder governance model illustrate this dimension.

1.3. Why Does It Matter? Cyberspace's Impact on International Relations

Over the past quarter century, the Internet has influenced many spheres of human behavior. For example, it transformed communication from the mass media's "one-to-many"[35] to the Internet's facilitation of "many-to-many"[36] communication. The latter in turn facilitated new forms of civic engagement and the rise of "leaderless movements."[37] The Internet gave rise to new political strategies such as U.S. Secretary of State Hilary Clinton proclaiming a new "Internet Freedom"[38] agenda, but the technology also enabled unprecedented surveillance systems, many initially developed and now exported by China.[39] Yet, many of these aspects arguably reflect incremental advances based on other technologies, for example, the radio and Radio Free Europe, thus begging the question: what is unique about the Internet? Specifically, what is its most fundamental impact on international relations? In short, why does it matter for International Relations scholars? This section therefore details how (i) the Internet's *diffusion of reach*, (ii) the new types of coercive effects it enables, and (iii) the unique mix of actors taking advantage of these new capabilities create (iv) systemic impacts for international relations.

1.3.1. The *Diffusion of Reach*

As outlined above, the most important characteristic of the Internet for international relations is what I call the *diffusion of reach*, defined as "the ability to cause effects remotely not only over regional but global distances" through the Internet. It is this feature that sets the Internet apart from previous phenomena and from previous analysis in the globalization literature.[40] For example, Robert Keohane wrote about global terrorism that "[s]uch [informal] violence becomes globalized when the networks of non-state actors operate on an intercontinental basis, so that acts of force in one society can be initiated and controlled from very distant points of the globe."[41] On 9/11, 2001, terrorists actually few the planes that resulted in mass casualties and physical destruction. What is

new is that the Internet removes physical proximity as a necessary condition for malicious actors to cause harm and coercive effects through hacking. (At what scale and level of severity is an open question, discussed in this dissertation.[42])

The Internet largely removes physical geographic barriers from the equation. While the invention of intercontinental ballistic missiles (ICBMs) had a similar impact with respect to the notion of distance, they remained limited to a small club of states and require substantial resources. The Internet has made it possible for a single person to cause an effect at the other end of the world through hacking without having to be physically near the target. The cost and barrier to entry can be as low as having access to a computer, the Internet, and the time to accumulate the required expertise. Much like ICBMs required scholars to rethink foundational concepts in International Relations theory, such as the notion of "a geographically defined defensive perimeter"[43] and the importance of "geographical distance,"[44] the modern Internet poses a similar challenge.

The Internet's *diffusion of reach* therefore goes beyond the existing studies on the increasing interdependence of globalized relations among people and nations including the forms of globalized violence it enables. Chief among its implications is that the *diffusion of reach* contributes to a further diffusion of power from state to non-state actors because of the low barriers of entry to hacking and the range of effects it enables. This range of effects is discussed in detail in the following section, including the relationship to existing conceptualizations of the use of force and the line between war and peace. Whether the *diffusion of reach* also contributes to a transition of power over the long-term is less clear, but there is some indication that hacking offers novel asymmetric advantages that empower states such as Iran and North Korea. In addition, there are growing concerns over the potential new risks for nuclear weapons systems, which imply consequences for the most important power structure in the international system to date, the deterrence regime keeping nuclear powers in check.

The degree to which the *diffusion of reach* affects international relations depends on the (changing) posture of both the attacker and the defender. For example, the defender's level of digital connectivity must be taken into consideration as well as the cyber maturity and resilience of the defender's infrastructure and society. Taken together, their respective postures determine the impact the *diffusion of reach* can achieve. As Rebecca Slayton highlights with respect to the 'cyber offense-defense balance,' "the offense-defense balance is shaped primarily by the relative skill with which adversaries manage complex information technology, and the relative complexity of their

goals."[45] She therefore provides a more nuanced assessment of the impact of hacking than the 'offense trumps defense' adage often referenced as a given by others.[46]

1.3.2. A New Range of Effects

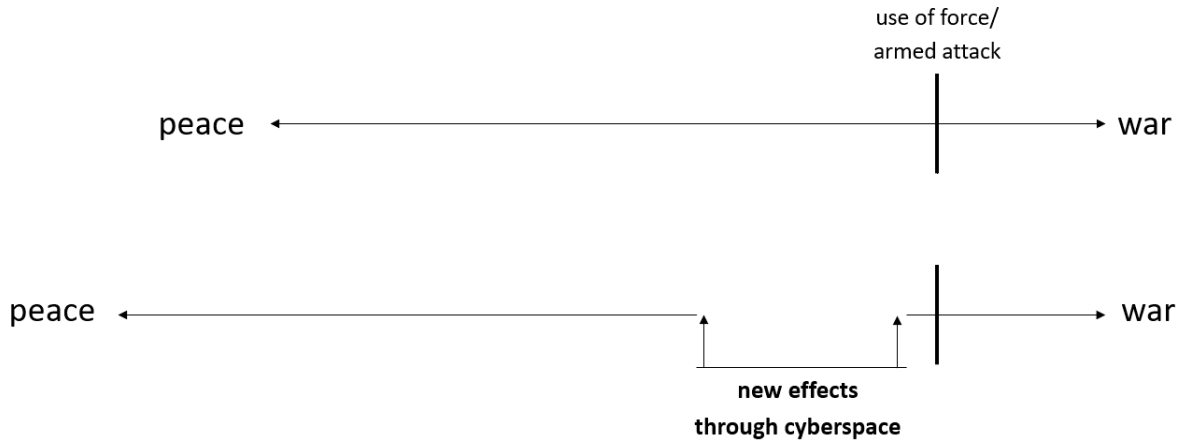
The Internet, apart from nullifying the variable 'geographic distance' through the *diffusion of reach*, has an important second consequence: it enables hacking and thereby a new range of coercive effects. Hacking enables effects that can serve as substitutes to conventional weapons. For example, one of the first publicly available demonstrations of physical damage caused through hacking was a video of a test run at Idaho National Laboratory published by CNN. The video shows a cyber attack destroying a generator used to produce electricity.[47] Hacking also enables effects that were previously impossible to achieve. For example, it is possible for a hacker to gain access to a bank and manipulate the integrity of the data, thereby changing the value of a person's bank account or the institution's ledger. Or instead of permanently destroying a critical infrastructure with a physical bomb, hacking can cause a temporary and, importantly from a political signaling perspective, reversible disruption.

These new types of effects are the most intriguing from a scholarly perspective, as well as for military planners and decision-makers.[48] Eric Rosenbach, the Pentagon's principal cyber advisor from 2011 to 2015 and former Chief of Staff to U.S. Secretary of Defense Carter, said in 2014 that "The place where I think it will be most helpful to senior policymakers is what I call in 'the space between.' What is the space between? … You have diplomacy, economic sanctions…and then you have military action. In between there's this space, right? In cyber, there are a lot of things that you can do in that space between that can help us accomplish the national interest."[49] Figure 2 illustrates this statement and connects it to Clausewitz's famous conceptualization of "war as the continuation of politics by other means."[50]

By 2018, the views expressed by Rosenbach's at a public think tank event in Washington, DC, in 2014, had become codified in official U.S. government doctrine. The 2018 Command Vision for U.S. Cyber Command states that "[U.S.] adversaries operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantages."[51] The Cyber Strategy of the Pentagon published the same year specifies that the U.S. military plans to "take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests […] We will defend forward to disrupt or halt malicious cyber activity at its source,

including activity that falls below the level of armed conflict."[52] The Pentagon's cyber strategy aligns with the 2018 National Defense Strategy, which highlights "the reemergence of long-term strategic competition, rapid dispersion of technologies, and new concepts of warfare and competition that span the entire spectrum of conflict."[53]

Figure 2. ***Cyber Effects and the Clausewitzian Spectrum of War as Continuation of Politics by Other Means***[e]

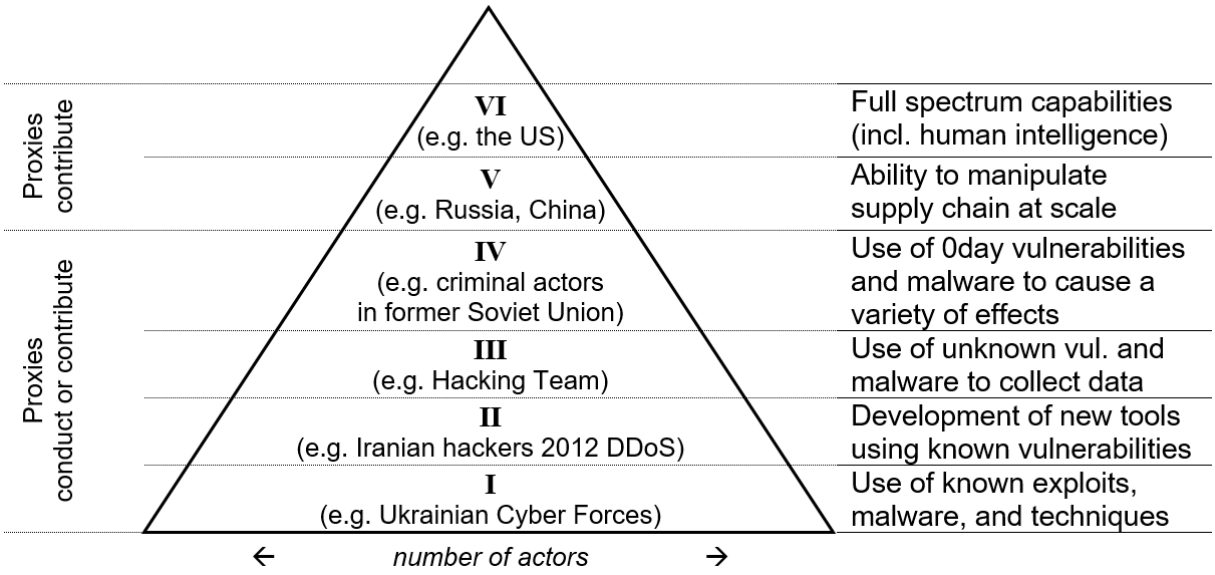


1.3.3. A Unique Mix of Actors

The low barriers to entry and the *diffusion of reach* create a unique mix of actors, including non-state actors, capable of projecting coercive cyber power globally. Yet, the existing literature is state-centric, despite the empirical evidence suggesting a very different environment. To provide a starting point and framework for future studies to help close this research gap, Figure 3 integrates the role non-state actors can play as independent actors and as proxies and provides additional information about the different levels of sophistication. The taxonomy shown in Figure 3 therefore addresses a shortcoming in the original taxonomy developed by the U.S. Defense Science Board with its state-centric approach.

[e] The graphic uses the international law thresholds of use of force/armed attack as the dividing line between war and peace rather than the 1,000 deaths/year definition often used in political science, see: Uppsala University. "Definitions." Department of Peace and Conflict Research. Accessed August 26, 2019. https://www.pcr.uu.se/research/ucdp/definitions/#Warring_party_2.

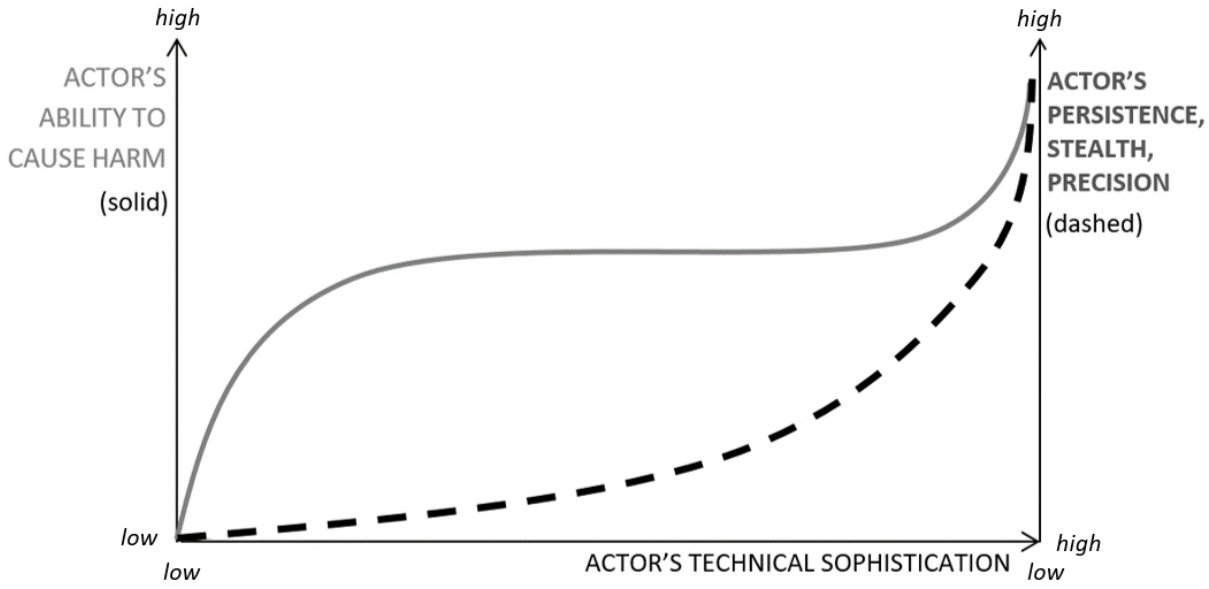
Figure 3. ***Taxonomy of actors capable of projecting coercive cyber power***[54]



Transcending the state-centric approach is important, because a biased focus on states risks ignoring a substantial part of the empirical reality and activity involving non-state actors ranging from hacktivists to malicious hackers and companies offering their services and tools for money.[55] For example, the largest data breach in history to date was carried out by a 29-year-old Russian cybercriminal on the FBI's Cyber Most Wanted list and a 22-year old Canadian citizen, both working as modern-day digital privateers for two Russian intelligence officers.[56] While non-state actors may be less sophisticated, particularly with respect to the full spectrum of capabilities, some are sophisticated enough to cause widespread harm. For example, it was only after four Iranians in their mid-20s joined the offensive cyber operation that turned the Distributed Denial of Service attack orchestrated by the Islamic Revolutionary Guard Corps against financial institutions in the U.S. from a "few yapping Chihuahuas into a pack of fire-breathing Godzillas."[57]

Importantly, the fact that non-state actors are less sophisticated compared to the most advanced nation-states implies that the former lack the ability to be as precise and to limit the intended effect of their activity. This increases the risk of accidental and unanticipated consequences of offensive cyber activity and potentially creating widespread unintended harm, while, the most advanced nation-states have the expertise and resources (and international lawyers) to first test any cyber weapon to ensure its precision and alignment with international and domestic laws. Figure 4 attempts to showcase this crucial distinction.

Figure 4. ***Relationship between an actor's technical sophistication, ability to cause harm, as well as persistence, stealth, and precision***[58]



1.3.4. Systemic Impacts

The *diffusion of reach* combined with the possibility of new coercive effects and the unique mix of actors able to leverage these capabilities are the key variables as to why cyberspace is affecting power in international relations. But how are these different factors having a systemic impact? While part of this question remains an open empirical one, this section discusses how these factors at least create a confluence of increased uncertainty, intensified globalized conflict, and new escalatory risks producing systemic impacts. For example, with direct conventional war among great powers highly unlikely, partly as a result of the Mutual Assured Destruction regime, hacking now enables new forms of coercion among nuclear powers.[f] Nuclear powers have certainly tested each others' limits in the past through other means such as proxy warfare on other continents. Yet, such activity was carefully calibrated not to pose a threat of direct escalation. The Internet having connected not only people, but more and more machines around the world, now presents a new frontier for these powers to exercise their power with several discernible consequences.

[f] For an important discussion whether hacking poses a new risk to the stability of the nuclear regime, see Acton, James M. "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War." *International Security* 43, no. 1 (Summer 2018): 56-99; Danzig, Richard J. *Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies*. Washington, DC: Center for a New American Security, 2014. https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies.

Increased Uncertainty. Offensive cyber activity increases uncertainty and mistrust exacerbating tensions and intensifying volatility in international relations. Three main factors are the source for this increased uncertainty and mistrust: (i) the attribution problem, (ii) the blurred lines between espionage and attack, and (iii) the specific characteristics of cyber tools.

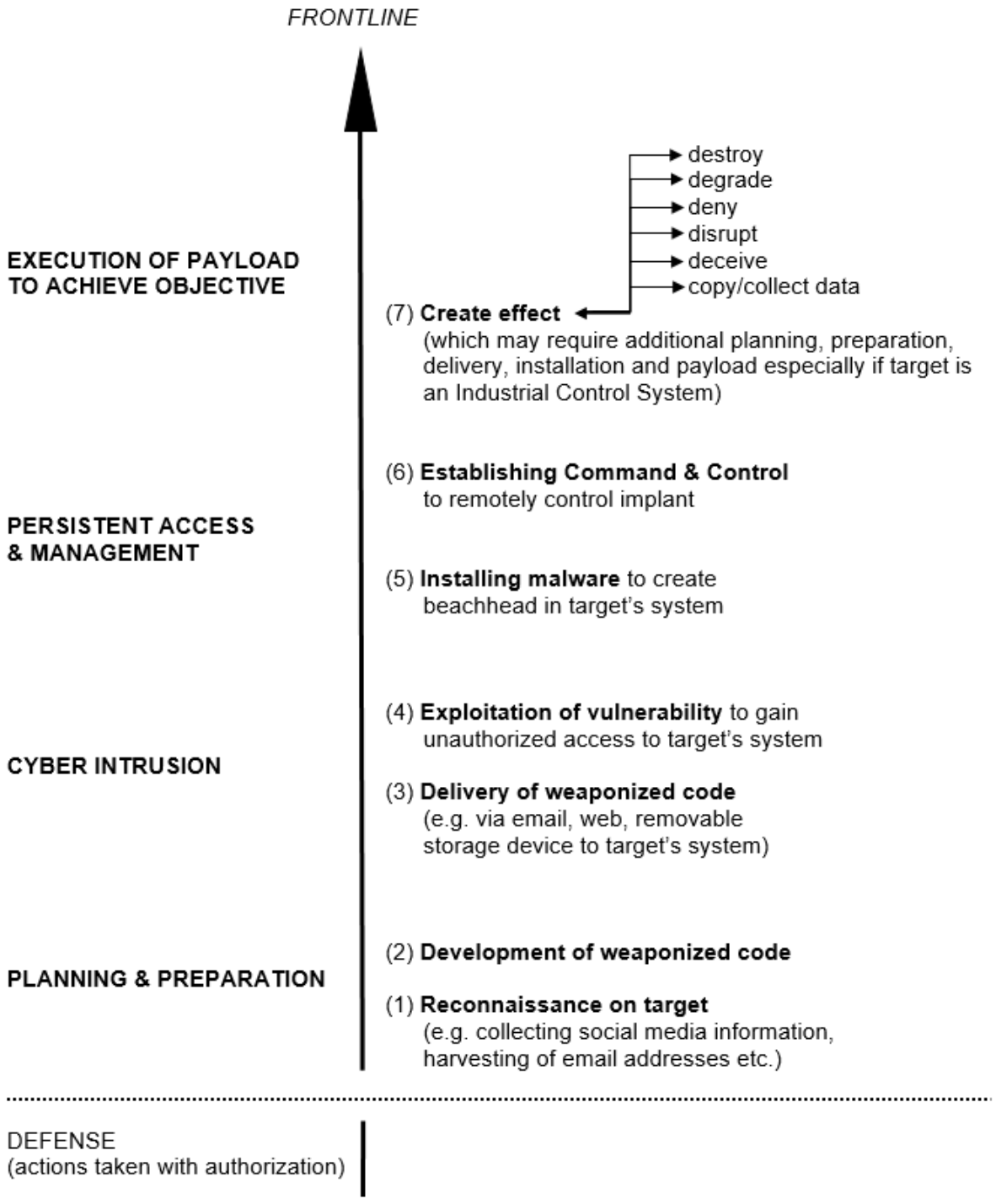
First, 'the attribution problem' describes the challenge of tracing offensive cyber activity back to its source.[59] Hackers can route their attack through different countries, hide their identity, and sometimes pretend to be someone else. For example, while experts cannot agree who is behind the Yemen Cyber Army, everybody agrees that it is not Yemeni.[60] Even for the most sophisticated actors with the best attribution capabilities, such as the U.S. government, attributing offensive cyber activity with a high degree of confidence usually requires significant resources, combining signals intelligence with human intelligence and requiring an amount of time exceeding that usually necessary for national security decision-making. For nearly all other governments, this remains an insurmountable task without outside assistance (and an important and fascinating issue ripe for further research).

The second source, the blurred line between espionage and attack, a particularly challenging aspect of hacking with implications for international peace and security, becomes clear when considering the different steps involved in an offensive cyber operation. Figure 5 visualizes the different stages by developing a modified version of the tip-of-the-spear framework used previously in International Relations literature. (Peter Singer applies the 'tip of the spear' framework from military thought to conceptualize different types of private military and security companies based on their geographic proximity to the battle space.)[61] Instead of geographic proximity, the key measure used here to conceptualize hacking is the proximity to an effect caused by a hacker given that geographic distance can be neglected.

Looking at the four stages and seven steps, the key insight is that it is only the last step that determines whether an intrusion is used to collect data, e.g., for espionage, or to undermine the availability of data or to manipulate it, e.g., to create a disruptive or destructive effect. That is why the mere intrusion can be considered escalatory once detected, as the victim does not know the intent behind the intrusion and whether it is limited to theft of data or is the precursor to an attack.[62] This close relationship between espionage/intelligence collection and attack is also evident in the institutional structures involved in offensive cyber operations. For example, U.S. Cyber Command

remains institutionally closely tied to the U.S. National Security Agency (NSA) with the commander of U.S. Cyber Command being dual-hatted simultaneously serving as head of NSA.[63]

Figure 5. ***"Tip of the Spear" framework applied to remote offensive cyber operations***[64]



Third, two additional characteristics of cyber tools are worth mentioning. First, the 'use and lose' character of some cyber weapons and second, the 'dual use' nature of cyber tools.[65] Some cyber weapons are 'use it or lose it' because they rely on a zero-day vulnerability, a vulnerability not known to anyone other than the attacker.[66] If discovered by others, there is an incentive to use the capability before it gets lost due to its getting patched subsequent to its discovery. A similar incentive exists if a system is about to be updated, for example, one version of Windows gets replaced with the next, creating an incentive to use a capability by using a vulnerability in the old version. The stealthy nature of these zero-day vulnerabilities is also what prevents actors from demonstrating their cyber capabilities through public display, such as military tests or exercises, and limits the ability to use such public displays for political signaling.[67] The dual-use character, on the other hand, refers not only to the civilian/military distinction commonly associated with the term 'dual-use,' but that cyber tools are often 'multi-use' and used by law enforcement and intelligence agencies and cybersecurity companies for legitimate purposes in addition to their potential abuse for nefarious purposes.[68] This complicates discerning the intent of actors' behavior, for example, with respect to the exports and use of such technologies.

New Risk for Escalation. A consequence not originally foreseen with the development of the Internet was that by connecting more and more people and more and more machines it made government, military, and private computer systems vulnerable to hackers. The founders of the Internet built the technology "with performance, not security, in mind," according to Howard Shrobe, computer science professor at MIT.[69] The amount of hacking has become so prevalent that cybersecurity experts have come to argue that 'It is no longer a question of whether you will be hacked but when you'll be hacked' or that 'there are two types of companies, those who have been hacked and those who don't know yet that they've been hacked.'[70]

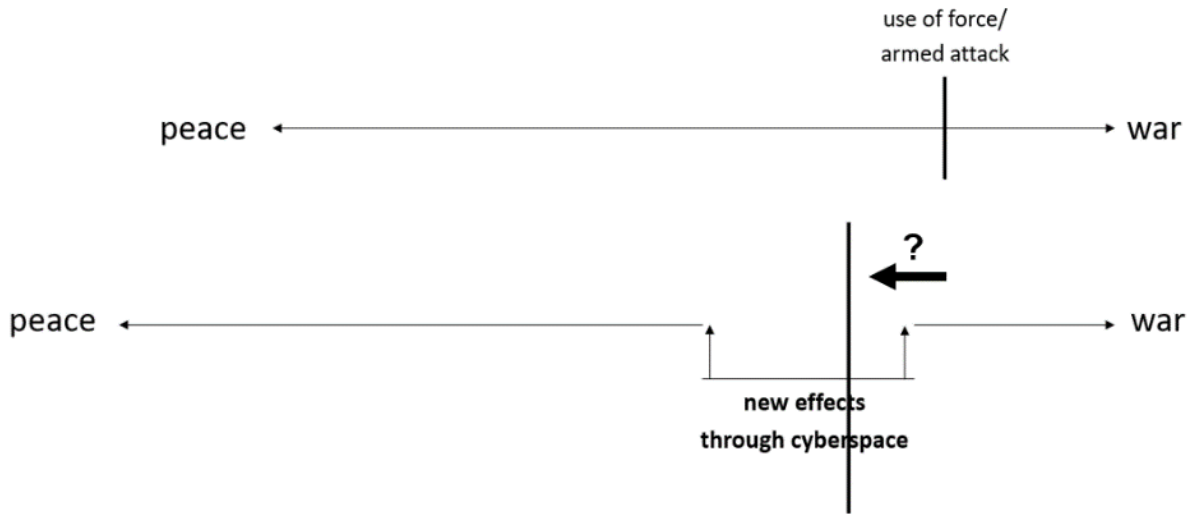
The resulting vulnerabilities have created new sources of insecurity and – paired with the *diffusion of reach* and the increased uncertainty – risks for (accidental) escalation.[71] For example, one of the first incidents involving such new escalatory risks occurred in 1998 when tensions between the U.S. and Iraq had reached a new high. While American troops were being deployed to the Middle East, the Pentagon realized that it had been hacked, leading to the President being briefed on the incident. Initially, it seemed that Iraq may be responsible, but ultimately the hack was traced back to two teenagers in California and an Israeli hacker.[72] Another complicating factor is that proxy actors ranging from politically motivated hacktivists to profit-driven companies or cybercriminals are often involved in offensive cyber activity. This incident also illustrates that the risk for

escalation is further compounded by the lack of intersubjective understanding how to interpret intrusions in cyberspace, even if it is clear who is behind them. For example, is Russia's probing[73] of the U.S. electrical grid a precursor for an attack similar to the cyber attack triggering the 2015 blackout in Western Ukraine,[74] is it espionage, political signaling, or all of the above?

Globalizing conflict. The *diffusion of reach* has had a flattening[75] effect on international relations and geopolitical tensions. In other words, geographic distances have shrunk and the *diffusion of reach* can be seen as an extension of globalization as "the process of increasing interconnectedness between societies such that events in one part of the world more and more have effects on peoples and societies far away."[76] For example, until recently, most observers expected that North Korea's ability to hit targets on U.S. soil remotely would be through the development of an ICBM as part of its nuclear program. They did not expect that the first damaging attack would consist of North Korean hackers targeting a Hollywood movie company when it hit Sony Pictures Entertainment. (Nor did most observers expect that the first time a U.S. president would publicly accuse another country of committing a cyber attack that it would be this type of attack.)[77] There is an obvious difference in severity between an ICBM hitting the U.S. and a cyber attack deleting data, but the latter nevertheless globalized what was previously a regional conflict from the U.S. perspective. (For North Korea, this has always been an issue of global dimension given the global reach of the U.S.). Another example for this globalizing effect is the Iranian cyber attacks against a range of targets in the U.S. from financial institutions to a casino and a dam.[78]

Looking ahead, these systemic impacts will be exacerbated by three overall and related trends that have emerged in recent years: (i) the number of actors developing and using offensive cyber capabilities is increasing, (ii) the number of attacks and effects caused are proliferating, and (iii) the new types of effects and reactions create new escalatory risks. The latter also points to the broader International Relations literature by raising the important question in the medium- to long-term whether current understandings of what constitutes use of force and armed attack will remain consistent or possibly change? Will use of force continue to be primarily associated with death or physical damage, or will the new types of coercive effects that cyberspace enables, such as targeting of a country's financial system, lead to the line and threshold being moved further in a direction to include non-kinetic effects as illustrated in Figure 6 (thereby enabling other types of counter-attacks)?

Figure 6. ***Cyber Effects and the Clausewitzian Spectrum of War as Continuation of Politics by Other Means***



1.4. Cyberspace and International Relations More Broadly: The Literature

1.4.1. A Few High-level Observations on the State of the (Still Nascent) Literature

It is important to begin with three main observations to place scholarship on cyberspace in the context of broader International Relations theory. First, there remains a disconnect between mainstream International Relations literature and the literature on cyberspace. When I conducted an in-depth literature review in 2017 to co-author an annotated bibliography for Oxford Bibliographies, it was striking how many of the works focusing on cyberspace considered seminal had been published outside conventional International Relations journals and publishers.[g] Relatedly, the study of cyberspace remains not necessarily an orphan issue but one in search of a home. Peer-reviewed publications have been scattered across academic disciplines ranging from law, political science, international relations to communications studies, sociology, and computer science.[h] To overcome the challenge of fragmentation, this dissertation is based on an interdisciplinary approach that draws on publications across the various disciplines. Third, some of the most influential insights in the scholarship on cyberspace have not been published in peer-

[g] For a comprehensive overview of the literature and annotated bibliography, see Hannes, Ebert and Tim Maurer. "International Relations - Cyber Security." *Oxford Bibliographies - Oxford University Press.* Last modified January 11, 2017. https://doi.org/10.1093/OBO/9780199743292-0196.

[h] Some newly created journals are trying to address this fragmentation such as Oxford University Press's *Journal of Cybersecurity* and Taylor & Francis's *Journal of Cyber Policy*.

reviewed publications but the "grey literature"[79] of think tank reports, university working papers, even reports by private companies[80] or obscure outlets that have brought unique research to light such as Scott Henderson's insight into the first Chinese hacker networks.[81]

With respect to how scattered the literature is, consider the following review of some of the key pieces of scholarship. For example, it was law professor Larry Lessig's seminal work arguing that code is law that changed the way scholars thought about governance and the Internet.[82] Sociologist Gabriela Coleman provided the most detailed analysis of one of the most notorious actors in cyberspace, the hacktivist group Anonymous.[83] Another sociologist, Jonathan Lusthaus, produced one of the most comprehensive studies of cybercrime globally.[84] The U.S. intelligence analyst Sean Kanuck offers one of the first in-depth discussions of the implications of cyberspace for sovereignty and international law.[85] A foundational analysis on encryption and globalization was also written by lawyers Peter Swire and Kenesa Ahmad.[86] Meanwhile, Monroe Price traces the evolution of communications technologies over the decades and draws out important distinctions in how the Internet differs from radio, television, and satellite communications.[87]

In political science, scholars such Ronald Deibert and Shanthi Kalathil focused on the Internet's impact on domestic political systems, namely authoritarian regimes, early on.[88] With respect to international security, John Arquilla warned in 1993 already that "Cyberwar is Coming!"[89] Two decades later, Nazli Choucri shed light on the international institutions relating to cyberspace while Joseph Nye popularized the notion of cyber power.[90] Meanwhile, Internet governance scholars formed their own epistemic community debating the political nature and the politics of cyberspace and asking who controls the Internet and why.[91] Area-specific publications also date back to the 1990s. For example, Timothy Thomas's consistent scholarship on Russia, increasingly complemented by the rise of the next generation of scholars from Collin Anderson's analysis of developments in Iran to Jenny Jun's focus on North Korea.[92]

Finally, it is worth noting that there is a noticeable break in the cybersecurity scholarship that occurred in 2001. After a growing body of literature started emerging in the 1990s in both academia and think tanks that focused on the Internet and its implications, the September 11 terrorist attacks led to a noticeable shift of attention among scholars toward counterterrorism and away from cyberspace. Apart from a few exceptions, such as Dorothy Denning, Ronald Deibert, Martin Libicki, and Myriam Dunn Cavelty,[93] it was not until the end of the first decade of the 21st century that interest in the topic resumed, leading to a revival of scholarship. Some scholars tend to

only focus on the more recent literature mainly because the Internet today differs significantly from its role in the 1990s. For example, social media remains a recent phenomenon, with Facebook being founded in 2004 and Twitter in 2006. However, the "Global Information Society" was already on the agenda of the G7 in 1995. Therefore, I deliberately included the scholarship dating back to this period for this dissertation.[94]

1.4.2. Key Debates in the Literature on Cyberspace[i]

The literature on cyberspace touches on several dimensions of the overarching research question of this cumulative dissertation - how cyberspace affects power shifts in global affairs - yet it remains rather siloed. One way to categorize this literature is based on the epistemic communities that scholars have formed over the years, namely: (i) the Internet governance scholarly community, (ii) the cybersecurity/conflict community, and (iii) the human rights online community. While a few scholars have started to study issues outside their original area in recent years,[95] and a few have crossed multiple communities,[96] these three communities nevertheless stand out as clearly delineated groups whose literature and scholars.[j] It reflects the observation by Rudra Sil and Peter Katzenstein about International Relations scholarship more broadly that "social scientific research is still organized around particular research traditions or scholarly communities, each marked by its own epistemic commitments, its own theoretical vocabulary, its own standards, and its own conceptions of 'progress.'"[97]

Internet governance. The first epistemic community has focused on some classic questions of International Relations theory in its scholarship on Internet governance such as 'who controls the Internet?',[98] what is Internet governance and how to distinguish "governance of the Internet" and "governance on the Internet,"[99] as well as how the transnational architecture of the Internet and data governance corresponds to notions of territorial sovereignty.[100] The scholarship on Internet governance is particularly interesting due to its focus on the Internet's "multi-stakeholder approach,"[101] which is subject to increased contestation by some nation-states trying to impose

[i] See also Ebert, Hannes and Tim Maurer. "International Relations - Cyber Security." *Oxford Bibliographies - Oxford University Press.* Last modified January 11, 2017. https://doi.org/10.1093/OBO/9780199743292-0196.

[j] Scholars focusing on Internet governance, for example, have created the Global Internet Governance Academic Network (www.giga-net.org) and usually meet at the annual Internet Governance Forum. Scholars focusing on cyberspace in the context of international peace and security have been convening annually in Cambridge, MA, through a MIT/Harvard conference series (https://ecir.mit.edu/). Scholars focusing on human rights online get together at RightsCon (https://www.rightscon.org/) and the Stockholm Internet Forum. The Cyber Dialogue series hosted by the University of Toronto's Munk School of Global Affairs is one of the few specifically designed to build bridges across these communities and scholarship (https://cyberdialogue.ca/).

greater state control through multilateral institutions.[102] Taking into account the current debate in International Relations theory about changes in global governance, namely the role of private transnational regulatory organizations,[103] the scholarship on Internet governance thus contributes a unique lens and voice to this debate.

This segment of the literature is therefore particularly focused on the diffusion of power and the extent to which cyberspace has empowered non-state actors relative to the state. Moreover, this epistemic community has stood out for its prescriptive streak centered around advancing the concept of multi-stakeholderism in addition to its empirical analysis of who governs the Internet, why, and how.[104] Interestingly, discussions about 5G technology and the growing influence of Chinese (state-owned) tech companies is bringing questions related to a potential transition of power from the U.S. to China into sharper focus within this community.

Cybersecurity. The second category consisting of the scholarship on cybersecurity ranges from the literature on cyber terrorism[105] to the debate over cyber war[106] that eventually led to more nuanced discussions away from cyber conflict as a standalone phenomenon to the recognition that cyberspace is increasingly used in conflict alongside other capabilities, i.e., "cybered conflict."[107] Analogies discussed in the literature now range from "Electronic Pearl Harbor"[108] to "Cyber 9/12"[109] and the outbreak of World War I in 1914[110] to entire volumes dedicated to analogies.[111] A separate strand focuses specifically on applying securitization theory to the topic.[112] More recent scholarship analyzes the structural dynamics of cybersecurity ranging from the 'cybersecurity dilemma'[113] to a detailed analysis of the 'cyber offense-defense balance.'[114] Current debates continue to discuss if and how the notion of deterrence applies to cyberspace[115] while new concepts such as "persistent engagement" are starting to emerge in addition to detailed country studies and analyses of high-profile cyber incidents.[116]

The most important debate of the past decade among scholars was about whether 'cyber war' will or will not take place. Triggered by Richard Clarke and Robert Knake's influential 2010 *Cyber War* and Thomas Rid's response a year later, this debate also found its way into mainstream International Relations journals.[117] Rid argues that cyber capabilities are most likely to be used for intelligence collection, sabotage, and subversion rather than for all out 'cyber war,' a view that has enjoyed growing consensus. However, his dismissal of cyber capabilities being able to cause widespread harm or even fatalities remains contested and increasingly tenuous considering recent developments. From the New York Times article referencing a comprehensive plan for cyber

attacks against Iran to the WannaCry malware requiring hospitals in the United Kingdom in 2017 to turn away patients,[118] indications are that states are capable of carrying out cyber attacks with effects that go far beyond what has been witnessed to date. (On the flipside, the decision by the Israeli Defense Force to carry out an airstrike against a building used by Hamas to launch a cyber attack demonstrates that cyber activity can be considered legitimate reasons to launch a kinetic counterstrike.[119]) Once 5G technology paves the way for the next generation of the Internet - the Internet of Things - connecting primarily machines with machines, the possibilities to create more severe impacts will increase.

The literature focusing on the security dimension of cyberspace has demonstrated an interesting evolution. It moved from a near obsession with cyber terrorism and the implied diffusion of power to then focus on state-centric cyber war. Most recently, the scholarship has seen a rise in studies with an emphasis on China that connects to the broader academic research examining China's rise and its implication for the transition of power. In addition, there has been a trend toward more empirical-driven analysis paving the way for more nuanced research output shedding light on the relationships between state and non-state actors.

Human rights. The third epistemic community, this one focusing on human rights in the digital age, has produced studies ranging from early analyses investigating the use of the Internet by authoritarian regimes and its impact on state surveillance,[120] including its utopian and dystopian manifestations,[121] to the role of tech companies[122] and the global trade and export controls of surveillance technologies.[123] During the period of tech optimism, research was driven by questions about the extent to which the Internet empowered the protection and realization of individuals' human rights. This set of studies essentially represents an examination of the diffusion of power with the underlying thesis being that the Internet results in a relative loss of power for the state with individuals being empowered to act as guarantors of their own interests and rights. For example, the outcome of the Crypto Wars saw encryption morph from being viewed and controlled by states as a weapon to becoming ubiquitous worldwide.[124]

Following Edward Snowden, the digital rights scholarship shifted to focus specifically on the intelligence activities of governments in liberal democracies and their implications for human rights.[125] The previously hidden power of the state became the subject of intense scrutiny marking the beginning of a much more pervasive tech pessimism. This period of tech pessimism is reflected in the type of research questions pursued and the conclusions drawn from it. Data protection and

privacy became a topic of interest globally including a burgeoning literature on the international regime governing espionage and privacy.[126] Importantly, this scholarship directly relates to the broader contemporary discussion among human rights scholars focused on questions of extraterritoriality.[127]

Similar to the other two strands of literature, the epistemic community focused on human rights in the digital age has also pursued research questions ranging from the diffusion of power to the transition of power. With respect to the latter, recent scholarship has focused particularly on the Internet's impact in countries such as China and Russia again. This includes investigating how China is exporting its behavior and norms to other countries and exploring questions of how the technology is affecting political systems and the stability and longevity of democratic and authoritarian regimes alike.[128]

Future trends. These separate epistemic communities and strands of scholarship have been increasingly converging over the past few years for several reasons.[129] First, an increasing number of universities have been establishing degree programs and concentrations dedicated to the study of cyberspace, including the creation of a new generation of PhD students who are integrating the scholarship of different academic disciplines.[130] Second, some scholars started to expand their research beyond their initial areas of focus. For example, Milton Mueller and Laura De Nardis who are known for their Internet governance expertise started to also publish research focused on cybersecurity. Whereas, James Lewis expanded his writings on cybersecurity to discuss broader governance questions.[131] Joseph Nye's outline of an emerging regime complex captures most of these various dimensions.[132] Third, International Relations journals have been publishing cyberspace-related scholarship more frequently and new handbooks have appeared dedicated to the study of cyberspace or to specific sub-fields such as cybersecurity.[133] These are promising developments that facilitate studies such as the ones pursued in this cumulative dissertation that is designed to close research gaps between and within the respective siloes and to be cross-cutting and multi-disciplinary in its examination of how cyberspace affects power shifts in international affairs.

2. Conceptual Framework for Cumulative Dissertation

2.1. 1st Conceptual Point of Departure: Analytic Eclecticism

While the key distinctions between the three main contemporary schools of thought in International Relations Theory[134] – liberalism,[135] realism,[136] and constructivism[137] – are relatively clear and easy to grasp, the modern incarnations, especially of the first two, continue to be the subject of intense debate. For example, scholars cannot even agree whether the work of neorealism's founding father, Kenneth Waltz, was based on microeconomics or not.[138] Others argue that his seminal work that established neorealism – *Theory of International Politics* - "was an attempt to reconceive classic realism in a liberal form. Neorealism, in short, was profoundly ideological."[139] They conclude that it was Waltz's personal beliefs, namely his desire to remove the anti-democratic elitism of classic realism and to marry realist assumptions with American ideals, that drove his shift to a systemic neorealist theory.[140] In short, the theories' scientific soundness and intellectual boundaries remain hotly debated.

Apart from these conflicting accounts, a key problem realists and liberalists continue to grapple with is how do domestic politics relate to international relations and vice versa? How can systemic outcomes be conceptualized and aligned with state behavior? In one of the most recent discussions of how the two research traditions address the topic, Kevin Narizny points out:

> "Each perspective represents an attempt to 'solve' the problem of combining levels of analysis in international relations theory. Liberalism is a bottom-up, domestic society-based theory that nevertheless incorporates external variables; neoclassical realism is a top-down, international system-based theory that nevertheless incorporates internal variables. If their strengths and weaknesses were parallel, the choice between them might simply be a matter of personal preference. Those who believe that systemic pressures matter more could declare themselves to be neoclassical realist, whereas those who believe that domestic politics matter more could declare themselves liberal, and it would make little difference for the progress of the field."[141]

Narizny ultimately argues that "Lacking internal coherence, neoclassical realism has become less a scientific paradigm than an invitation to methodological error"[142] concluding that "The underlying problem with neoclassical realism is that it attempts to operationalize an irretrievably amorphous intuition: that domestic politics matter, but not too much…In short, confusion reigns."[143] Further highlighting the confusing nature of the debate is the fact that the same piece of work by Ripsman, Taliaferro, and Lobell that is the focus of Narizny's liberal critique has also been criticized by

fellow neorealist scholars.[144] Further to this point, whereas some scholars reject one theory over the other, others have preferred to view them as complementary suggesting that "for better or worse, institutional theory is a half-sibling of neorealism."[145]

In light of these ongoing theoretical debates,[146] I selected a more pragmatic,[k] problem-centered approach and decided to use analytic eclecticism as the conceptual point of departure for this cumulative dissertation. As described by Rudra Sil and Peter Katzenstein, analytic eclecticism "is intended to generate diverse and flexible frameworks, each organized around a concrete problem, with the understanding that it is the problem that drives the construction of the framework."[147] Sil and Katzenstein offer a persuasive outline of the benefits and risks associated with analytic eclecticism, which on balance, is particularly promising for a cumulative dissertation investigating different aspects of a phenomenon – in this case cyberspace. This approach encourages the application of different frameworks and middle-range theoretical arguments tailored to the specific problem investigated through the various lines of inquiry. To buttress the choice of analytic eclecticism as a conceptual point of departure, the literature on power will serve as the second conceptual approach providing an overarching umbrella framework for the work of this cumulative dissertation.

2.2. 2nd Conceptual Point of Departure: The Literature on Power

2.2.1. A Brief Review of the Concept of Power

The concept of power has fascinated scholars for centuries and the literature on power has become rather eclectic in and of itself. Philosophers in ancient Greece explored the role of power in works such as Thucydides' well-known account of the Peloponnesian War. Machiavelli's *The Prince*

[k] "Pragmatism held that philosophy should concern itself with the messiness of human meaning" according to Sil and Katzenstein, with the "canonical trinity" of John Dewey, Charles Pierce, and William James as its foundation. Pragmatism saw a revival several decades later through Richard Rorty's publications. For a more in-depth discussion of their work and impact, see Legg, Catherine and Christopher Hookway. "Pragmatism." Stanford Encyclopedia of Philosophy. Last updated March 14, 2019. https://plato.stanford.edu/entries/pragmatism/. Sil, Rudra and Peter Katzenstein. "Analytic Eclecticism in the Study of World Politics: Reconfiguring Problems and Mechanisms across Research Traditions." Perspectives on Politics 8, no. 2 (June 2010): 417.
With respect to its application in the context of International Relations scholarship, Sil and Katzenstein also discuss (421-422) several specific examples where scholars have used a more pragmatic and eclectic approach in their studies combining different theoretical strands to explain a concrete problem ranging from Robert Jervis's *American Foreign Policy in a New Era* to Michael Barnett and Martha Finnemore's *Rules for the World*. Jervis, Robert. *American Foreign Policy in a New Era*. Routledge, 2013. Barnett, Michael, and Martha Finnemore. *Rules for the World: International Organizations in Global Politics*. Cornell University Press, 2004.

famously added to this literature and Max Weber provided new impetus with his reflections on the modern state.[148] More recently, Joseph Nye coined the distinction and popularized the notion of soft and hard power. Nye writes of a power behavior continuum ranging from *command* as the most extreme form of hard power to *co-option* as the most extreme form of soft power. He builds on the work of previous theorists such as E.H. Carr who wrote in 1939 that power over opinion, "the art of persuasion," was "not less essential for political purposes than military and economic power, and has always been closely associated with them."[149]

Yet, "power is an essentially contested concept" as Michael Barnett and Raymond Duvall highlight: "Its status owes not only to the desire by scholars to agree to disagree, but also to their awareness that power works in various forms and has various expressions that cannot be captured by a single formulation."[150] In their 2005 article Barnett and Duvall attempt to provide a comprehensive framework for thinking about power building on those different scholarly strands.[151] Their work is a fresh attempt to view the varying concepts of power as interconnected and to encourage scholars to examine the connections between concepts rather than to focus on how they might compete with one another. Arguably, it is a prime example of the application of analytic eclecticism. Their definition of power as "the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances and fate" goes beyond the actor-focused Dahlian concept of power to instead include structure as a dimension that culminates in a new taxonomy centered on four dimensions of power: "compulsory, institutional, structural, and productive."[152]

This broader conceptualization of power is useful for the inquiries pursued in this dissertation because several instances of contestation with respect to cyberspace touch on different dimensions of power. These dimensions include power among actors and over each other (the focus of my scholarship on cyber proxy actors); power through more diffuse relations such as international institutions (the focus of my co-authored article on the BRICS); and power in the context of constructing meaning (a central theme of my analysis of cyber norms).[153]

One of the more contested concepts is whether the Internet merits the stand-alone concept of cyber power. With the Internet's rapidly growing importance for international commerce, communications, and security, scholars started to think about how to conceptualize cyberspace in the context of power. Nye proposes the new concept of "cyberpower" defined as "the ability to use cyberspace to create advantages and influence events in other operational environments and across

the instruments of power. Cyberpower can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace."[154] By defining cyber power as a stand-alone term, Nye highlights the importance that the Internet has had and likely will have on international relations. (An alternative approach is to conceptualize cyberspace as a feature of the existing categories ranging from the compulsory, Dahlian end of the spectrum to the institutional, structural, and productive end of the power spectrum.)

2.2.2. Power and The International Order of the 21st Century

As outlined above, the international order shows signs of significant changes the beginning of the 21st century that the scholarship on power usefully divides into the transition and diffusion of power. Nye[1] describes the transition of power as a shift of power among states, namely from one dominant state to another, in contrast to power diffusion as the mechanism of power diffusing from states to non-state actors.[155]

With respect to the transition of power, the first decade of the twenty-first century witnessed the shift from the world's "unipolar moment" to a "uni-multipolar"[156] international system. Some scholars argue the world is moving toward a "G-zero"[157] or "non-polar"[158] world with others focusing on its "post-American"[159] character or the "civilizational"[160] undertones of the Trump administration's rhetoric.[161] Ultimately, the United States continues to be the global hegemon to date, accounting for 36 per cent of the world's military expenditure and commanding 11 of the world's 20 aircraft carriers which enable its unique global influence.[162] Yet, rising powers have been catching up in terms of resources and influence, with high rates of economic growth and military spending as well as a growing network connectedness.[163] The institutionalization of the Group of 20 and a new distribution of voting shares at the IMF underline this trend.[164]

The diffusion of power from state to non-state actors constitutes a second major shift. Nye argues, "What is distinctive about power in the cyberdomain is not that governments are out of the picture […] but that different actors possess different power resources and that the gap between state and nonstate actors is narrowing in many instances."[165] The Arab revolutions and the catalyst role of

[1] Nye discusses the concept of structural power briefly, namely Peter Digeser's 1992 article in the Journal of Politics on "The Fourth Face of Power," but rejects such expanded concepts of power on the grounds that "For my purposes, the insights that Foucault and other structuralists provide are purchased at too high a price in terms of conceptual complexity and clarity" (see Nye Jr, Joseph S. *The Future of Power.* New York: Public Affairs, 2011: 242-243.)

social media empowering individuals and small networks of people have become an often cited example. Another is the role an individual or a small group of hackers can play as showcased by the Iranian hackers allegedly responsible for the cyber attacks against financial institutions in the U.S. or the two cyber-criminals that carried out the largest data breach in history, the Yahoo hack.[166]

2.2.3. Power and Cyberspace

A key debate among scholars is about whether cyberspace fundamentally erodes the power of states by empowering non-state actors instead. One group of scholars, including Nye, argues that cyberspace empowers non-state actors due to three characteristics. First, the Internet was designed to be "open, minimalist, and neutral," organized to be decentralized and without any central authority.[167] Second, cyberspace facilitates asymmetrical relationships. Nye argues that "the low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics … a good example of the diffusion of power that typifies global politics in this century. The largest powers are unlikely to be able to dominate this domain as much as they have others like sea or air."[168] Finally, some argue that governing cyberspace is highly demanding both in terms of resources and expertise and that "states lack the authority and tools to effectively manage and regulate the globalized networks."[169]

Another group of scholars argues that states can control cyberspace. They point to the domestic regulatory systems in China, Iran, and Saudi Arabia which have enforced national laws and developed technologies such as China's Great Firewall through state authority.[170] These domestic controls translate into attempts by these countries to reassert national governmental authority in global governance regimes.[171] The more pervasive cyberspace becomes, the keener key stakeholders including powerful states will become to draw on "traditional structures of authority to control its content and restrict the ability of users to exchange information."[172] Additionally, these authors claim that great powers remain the primary actors, as posited by Daniel W. Drezner, because they command a range of foreign policy tools including "coercion, inducements, delegation, and forum shopping across international institutions to advance their desired preferences into desired outcomes."[173] Their role of "basic organizing principles for authority in the international system," is particularly hard to replace when it comes to providing security.[174]

This debate highlights that the technology's long-term impact on the transition and diffusion of power is an open empirical question. For example, as the Arab regimes fell, their archives provided a glimpse into elaborate surveillance systems - often sold by Western companies - that in the age of "Big Data" have allowed for unprecedented levels of information to be collected by states. There are therefore two competing empirical observations that contrast the increasingly empowered citizen actors of the Arab Spring with the increasingly empowered states to surveil and censor its citizens. How the two ultimately affect the power balance between states and individuals, the stability and longevity of political systems, and the relationship between democratic and authoritarian regimes constitute open empirical questions to be examined.

2.3. Three Lines of Inquiry

The three lines of inquiry guiding this cumulative dissertation focus on (i) cyberspace's impact on the transition of power, (ii) cyberspace's impact on the diffusion of power, and (iii) the normative governance of coercive cyber power.

Since states retain and are likely to retain their central roles in the international system in the foreseeable future, the first line of inquiry focuses on the impact of cyberspace with respect to power among states and the transition of power among them. This is narrowed further by focusing specifically on the rising powers Brazil, Russia, India, China, and South Africa given the crucial role they have been ascribed in the shifting international system as a "subgroup," or subnetwork, in the international order.[175] In addition, the focus on the BRICS enables an assessment as to whether variation in political systems is a relevant variable to consider for this line of inquiry or if they can be black-boxed and considered as "like units,"[176] namely by comparing within the BRICS China and Russia as authoritarian regimes with Brazil, India, and South Africa as liberal democracies.[m]

With respect to the diffusion of power, the second line of inquiry examines if and how cyberspace offers new resources to non-state actors to project power. It analyzes different groups of actors detached from the state, their motives, and costs associated with such power projection and the range of (technically) possible effects. Given the empirical absence of terrorist activity based on

[m] The *Freedom in the World 2019* report by Freedom House classified Brazil, India, and South Africa as "free" whereas China and Russia were classified as "not free": Freedom House. "Freedom in the World Countries." Accessed August 26, 2019. https://freedomhouse.org/report/countries-world-freedom-2019?order=field_fiw_status&sort=asc.

hacking (except for one case[177]) and other scholars[n] focusing exclusively on profit-driven cyber criminals, this line of inquiry focuses specifically on proxy relationships between states and non-state hackers. This includes the digital version of privateering[178] and mercenarism,[179] and sheds light on the growing market of cyber force.[180]

The third line of inquiry goes beyond the actor-focused perspective of the first two strands to investigate the emerging intersubjective understanding of the normative regime governing coercive cyber power. The main locus of this emerging regime has been the UN based on a first UN General Assembly resolution dedicated to the topic adopted in 1998 and a series of UN groups of governmental experts (UNGGE) that the UN started convening in 2004. In the twenty years since then, the construction of norms for cyberspace can be best characterized as a process of contestation, including contestation of the validity and contestation of the application of existing norms as well as contestation over access to contestation[o] in the first place.[181]

Finally, the conclusion points to an additional line of inquiry that cuts across the previous three. This additional strand is derived from an empirical finding that emerged independently in each line of inquiry but was common to all (demonstrating the utility of analytic eclecticism as an approach to reveal such broader explanations.) In short, the distinction between cybersecurity and information security matters not only from a definitional point of view but also directly affects and shapes the behavior of the actors involved from the projection of compulsory cyber power by states and proxy actors to governments' behavior in international institutions. It reflects the underlying competing interests and values advanced by authoritarian governments and liberal democracies.

[n] In parallel to my dissertation project, Jonathan Lusthaus at Oxford University carried out a research project focusing specifically on cyber criminals leading to his monograph: Lusthaus, Jonathan. *Industry of Anonymity: Inside the Business of Cybercrime.* Cambridge, MA: Harvard University Press, 2018.

[o] Given the nascent yet maturing status of norms regarding cyberspace, research on the translation of cyber norms with respect to local contexts constitutes a noteworthy research gap in growing need of in-depth study. For a detailed discussion of the theoretical concept of norm translation, see: Berger, Tobias. *Global Norms and Local Courts: Translating the Rule of Law in Bangladesh*. Oxford University Press, 2017

2.3.1. Transition of Power: Core Article #1

Ebert, Hannes and Tim Maurer. "Contested cyberspace and rising powers." ***Third World Quarterly*** **34, no. 6 (2013): 1054-1074.**

ABSTRACT: *The USA developed and has therefore historically played a lead role in cyberspace. Yet rising powers, including BRICS, have been increasingly challenging the established regime. China and Russia submitted a joint proposal on information security to the United Nations in 2011. India, Brazil, and South Africa have been focusing on the information society since their 2003 Brasilia Declaration. These initiatives demonstrate that cyberspace has become hotly contested. However, there is still a need to explain this divergence. Are rising powers challenging the USA because of their national interests, the urge to maximise their security, or do factors such as values and political structures explain the different trajectories vis-à-vis the hegemon? This article examines the foreign policies of BRICS from 1995 to date, explaining the influence of different path-dependent origins, of the systemic shift and the type of political system, together with rising civil society pressure.*

Puzzle. Despite the Internet's globally distributed and transnational architecture, the U.S. is perceived to play a hegemonic role. This is partly the result of the technology's historic evolution having originated in the U.S. with the network expanding and internationalizing from the U.S. outward. As the network grew, its governance also shifted from individuals to institutions with the latter being concentrated in the U.S.[p] As the Internet grew in political importance, balance of power theory would predict that rising powers contest U.S. dominance and balance against its hegemonic role.[182] Indeed, the BRICS have focused on information and communications technology (ICT) as a strategic priority of their counter-hegemonic movement and the "battle over the soul of the Internet."[183] Yet, contrary to expectations, the BRICS' responses to U.S. hegemony have differed noticeably among them and there is lack of joint balancing.

Research questions. Therefore, the research questions guiding core article #1 is: what explains the difference among the BRICS's cyber foreign policies and the lack of joint BRICS proposals, for example, at the UN and elsewhere? More generally: why, in contrast to the prevailing wisdom of balancing theory, do cyber-contestation policies vary among rising powers facing the same global hegemon?

[p] The best example is the function carried out by the "God of the Internet," Jon Postel, - the Internet Assigned Numbers Authority function - transitioning to ICANN in 1998.

Theoretical and methodological orientation. This article uses qualitative research methods combining its small-N cross-case analysis with the longitudinal comparison of the BRICS foreign (rather than domestic) cyber policy primarily using the process-tracing technique.[184] It draws from the Security Studies literature on balance of power and contestation, including the literature's discussion of secondary power behavior. Moreover, the research design integrates a comparison across two issue areas – Internet governance and cybersecurity – which up to that point were predominantly studied within the siloes of their respective epistemic communities and relies on key concepts developed in the literature of those two communities.

Findings and implications. Comparing the two issue areas of cybersecurity and Internet governance, this line of inquiry revealed that the variation in the BRICS behavior can be explained by four primary factors. The first is the origin and path dependence of countries' responses to U.S. hegemony. Russia's contestation focused on information security early on whereas the engagement by India, Brazil, and South Africa grew out of an economic-driven 'G7 of the Global South' effort. Second, the term 'information security' itself is intensely contested and viewed not only as a security but a human rights issue, which, third, has shaped civil society's engagement and mobilization pressuring liberal democracies to align their foreign policies with international human rights. Finally, as an increasing number of observers described China's rise, some of the other BRICS countries, namely India, no longer focused solely on the U.S. but started balancing and hedging also with respect to China.

Core article #1 contributes to the existing scholarship in that it is one of the first in the literature on cyberspace that focuses on cybersecurity and Internet governance in a comparative manner including investigating the interlinkages between the two. The research questions investigated in this first line of inquiry matter more broadly because they relate to the broader International Relations scholarship on revisionism.[185] Goddard's four ideal types distinguishing "integrated revisionists" from the other three ("bridging revisionists," "isolated revisionists," and "rogue revisionists") is a useful framework to assess China's and Russia's behavior.[186] This research also matters more broadly because part of the divergence among the BRICS relates to the type of international institution their governments prefer and the future of global governance. The "sets of interconnected rules and practices that prescribe behavior"[187] by multilateral institutions such as the International Telecommunication Union favored by Russia and China differ significantly from the rules and practices embodied by the "private transnational regulatory organizations"[188] that are the foundation of the "multistakeholder"[189] Internet governance model supported by Brazil and others.

Finally, the research also has utility for policy and can help inform the future policy development of the various stakeholders.

2.3.2. Diffusion of Power: Core Article #2 + Supplementary Material #1 - Monograph

Maurer, Tim. "'Proxies' and Cyberspace." *Journal of Conflict and Security Law* 21, no. 3 (2016): 383-403.

ABSTRACT*: States use proxies to project power through cyberspace, some capable of causing significant harm. In recent years, media outlets have published reports about proxies using Information and Communications Technologies (ICTs) from Northeast Asia to India, Pakistan, the Middle East, and Eastern Europe. Two of the landmark documents providing insight into how the international community thinks about rules of the road for cyberspace explicitly reference the term 'proxies'. However, neither report defines 'proxy,' nor does the term easily translate into non-English languages. This article therefore reviews what this term means and how it has been used in various contexts. It focuses on the subset of proxies that are non-state actors used by a state actor, analysing the different logical distinctions and levels of detachment between a state and a non-state actor's activity. The goal is 2-fold: first, to provide a framework to think about the diverse array of existing proxy definitions; second, to conceptualise the relationships between a state and non-state proxies that can offer a guide for political decision-makers and a roadmap for future research on proxy actors and cyberspace.*

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press, 2018.

ABSTRACT: *Cyber Mercenaries explores the secretive relationships between states and hackers. As cyberspace has emerged as the new frontier for geopolitics, states have become entrepreneurial in their sponsorship, deployment, and exploitation of hackers as proxies to project power. Such modern-day mercenaries and privateers can impose significant harm undermining global security, stability, and human rights. These state-hacker relationships therefore raise important questions about the control, authority, and use of offensive cyber capabilities. While different countries pursue different models for their proxy relationships, they face the common challenge of balancing the benefits of these relationships with their costs and the potential risks of escalation. This book examines case studies in the United States, Iran, Syria, Russia, and China for the purpose of establishing a framework to better understand and manage the impact and risks of cyber proxies on global politics.*

Puzzle. A key motivating factor for the second line of inquiry was a research puzzle I encountered in the early phase of this dissertation project. In 2013, the academic debate centered on whether cyber war will or will not take place.[190] Apart from the central question of what constitutes 'cyber war' and how cyber capabilities will be used, this rather abstract debate stands out for its state-centricity. Yet, conversations with experts investigating cyber incidents on a day-to-day basis, including law enforcement and other national security officials as well as cyber threat intelligence analysts at private companies, revealed a very different and much more complex empirical picture. They pointed not only to states but to a range of non-state actors from profit-driven criminals to hacktivists and companies offering their services. In short, the theoretical cyber war debate was decoupled from the available data, reflecting a puzzle to be investigated.[191]

Research questions. The second line of inquiry examines this puzzle through a single-authored research article as well as a single-authored monograph,[q] included as part of the supplementary material. The questions guiding the research for core article #2 center on: what is a proxy actor? When does a non-state actor become the proxy of a state? And when can a state be held responsible for a non-state actor's activity? Building on the conceptual framework of core article #2, the questions guiding the research of the monograph then focused on the following: Why do proxy relationships between states and hackers form in the first place? How do governments interact with these actors detached from the state, when, and for what purpose? What is common to proxy actors over time? Can non-state actors, and by extension proxies, wield the same cyber power – and cause similar effects and harm – as states? What kind of effects? What are the broader implications for international relations? How is this private market of cyber force organized? How can it be governed? Who is responsible?

Theoretical and methodological orientation. The framework and taxonomy developed in core article #2 is based on two main sources: (i) concepts of international law, namely the law of state responsibility and specific cases that are relevant and (ii) related frameworks in International Relations, namely insights from the counterterrorism literature about notions of active and passive support associated with expectations tied to sovereignty and due diligence.[192] Both studies also build on the early works of Deborah Avant, Janice Thomson, Peter Singer, Željko Branović and

[q] Please note that the title of the monograph "Cyber Mercenaries" was chosen by the publisher not the author. I had proposed and preferred "Cyber Proxies" as a title instead since the monograph analyzes proxy relationships more broadly and explicitly rejects other more historically-laden terms such as "mercenaries" or "privateers." See Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 30-31.

Sven Chojnacki as well as those preceding them such as Francis Stark's 1897 *The Abolition of Privateering and the Declaration of Paris*.[193] The empirical analysis, namely of the monograph, is based on qualitative research methods, the lessons learned from the early stages of this research,[r] and an unprecedented collection of primary and secondary data and literature that previously was highly fragmented and diffuse. In short, the monograph and core article #2 constitute an analysis of the market of 'cyber force' and how states use non-state resources and actors to project power and the variables shaping such use. That is also how they relate to the literature on the diffusion of power and relative increase in the power of non-state actors as the second major shift in the international system.

Findings and implications. Core article #2 was the starting point for this line of inquiry focusing on how to conceptualize "proxies."[194] This was partly in response to growing interest in this topic among government officials and policy circles. For example, the UNGGE focusing on cybersecurity specifically stated that "States must not use proxies to commit internationally wrongful acts."[195] Yet, the term "proxies" was not defined. Core article #2 therefore tries to close this definitional research gap by outlining the first conceptual framework that combines key relevant concepts and thresholds in international law with the related literature by cybersecurity scholars and incorporating insights from counterterrorism studies. The latter was crucial for incorporating the concept of active and passive support to provide a foundation to fully capture the empirical data and analysis outlined in the monograph.

Building on the findings of core article #2, the monograph – supplementary material #1 – adds analytical depth by conceptualizing the logic of the cybersecurity market and the proxy relationships between states and hackers while drawing on principal-agent theory and its critique.[196] In the first part, the monograph outlines several key concepts such as cyber power, *the diffusion of reach*, and the components of an offensive cyber operations. It also includes preliminary observations with respect to the pool of potential proxies, what they are likely used for, and the challenges associated with the attribution problem. It explains why non-state actors can cause a significant amount of harm and the challenges associated with the attribution problem. The second part consists of five case studies focused on the U.S., Iran and Syria, Russia, and China. The first four outline proto case studies and different types of proxy relationships based on a spectrum of control ranging from delegation to orchestration and sanctioning. The chapter on China constitutes

[r] For more details, see p. 46.

a case study for change over time detailing how the Chinese government tightened its control over proxy actors during the past 20 years.[197] The third part then discusses the shortcomings of existing international law and how and why the market of cyber force is currently organized as it is followed by an outline of how proxy relationships could be shaped in the future. The latter includes a discussion of what constitutes inherently governmental functions, the role of the private sector, and the phenomenon of hacktivism. Ultimately, considering the paucity of comprehensive empirical analyses of such proxy relationships, the monograph represents an empirical deep dive providing one of the most comprehensive studies to date of proxy relationships between states and hackers.

2.3.3. The (Normative) Governance of Cyber Power: Core Article #3

Maurer, Tim. "A Dose of Realism: The Contestation and Politics of Cyber Norms." ***Hague Journal on the Rule of Law*** **(2019).**

ABSTRACT*: Norms for cyberspace remain highly contested internationally among governments and fragmented domestically within governments. Despite diplomatic activities at the United Nations over the past two decades, intersubjective agreement on norms governing coercive cyber power is still nascent. Agreed upon, explicitly stated norms are considered voluntary, defined vaguely, and internalized weakly. Implicit state practice is slowly emerging, yet poorly understood, and cloaked in secrecy. This begs the question: what has been the contribution of the UN process to the international community's understanding of norms for cyberspace? Why did the process collapse in 2017, the very same year that two of the biggest cyber attacks to date – WannaCry and NotPetya – caused indiscriminate economic harm worldwide each with an estimated cost of several billion USD? And why did member states, in an unprecedented move in the UN's history, create two processes dedicated to the same issue in 2018? To answer these questions, this article analyses the various factors feeding into the dynamic process of norm contestation including an in-depth discussion of the process at the United Nations, the role of international law, and the main points of critiques.*

Puzzle. To complement the two lines of inquiry investigating how cyberspace has been influencing the transition and diffusion of power among key actors, the third line of inquiry focuses on the normative governance of cyber power as a new instrument to create coercive effects. Diplomatic negotiations focusing on these implications of cyberspace for international peace and security, in other words a process for constructing norms for cyberspace, have been in place for twenty years. Yet, despite this diplomatic process, despite cybersecurity having moved from low to the highest level of world politics, and despite the two biggest cyber attacks to date – WannaCry and NotPetya

– causing indiscriminate economic damage worldwide, the international community failed to reach consensus on next steps for this norms process the very same year of those two attacks.

Research questions. The third line of inquiry and core article #3 were thus motivated by the question: why did the process collapse in 2017, the very same year that two of the biggest cyber attacks to date? And why did member states, in an unprecedented move in the UN's history, create two separate processes dedicated to the same issue in 2018? Moreover, what has been the contribution of the UN process to the international community's understanding of norms for cyberspace generally? And what does that tell us about how norms emerge for cyberspace?

Theoretical and methodological orientation. Similar to the conceptualization of proxy relationships, this research has strong ties to international law[198] while using contestation theory to organize and guide the analysis, which was also applied in core article #1. Core article #3 combines recent scholarship on cyber norms, such as *Constructing Norms for Global Cybersecurity* by Martha Finnemore and Duncan Hollis,[199] with recent scholarship on norm contestation more broadly, namely the useful distinction between norm 'validity contestation' and norm 'application contestation'[200] - highlighted by Lisbeth Zimmermann, Nicole Deitelhoff, and Max Lesch - and contestation over 'access to contestation' discussed in Antje Wiener's recent work.[201] Core article #3 relies on qualitative research methods, namely process-tracing as a technique, and draws not only on secondary literature but also on expertise acquired through the involvement in various track 1.5 fora and informal discussions with individuals involved in policy-making.

With respect to the meta-theoretical debates referenced in section 2.1., it is worth highlighting that, with respect to core article #3, the literature on norms is fully cognizant that actors' norm-driven behavior exists in interplay with actors' interests and does not ignore the latter.[202] The key finding of the scholarship on norms is that in addition to interests driving how actors behave through a logic of consequences, actors are also influenced by their identity and expectations of behavior associated with that identity and their role through a logic of appropriateness.[203] Moreover, norms are not static but dynamic; they can emerge, potentially weaken, and even disappear. Contestation theory therefore emerged to complement Finnemore and Sikkink's seminal work on how norms emerge, reach a tipping point, and become internalized.[204]

Findings and implications. Norms for cyberspace remain weak despite international discussions dating back to the 1990s and the increase in the use of offensive cyber operations by a growing number of actors, particularly over the past decade. While the process at the UN has influenced the international community's understanding of norms for cyberspace, it is subject to significant contestation. Therefore, the UN process so far has (i) helped crystallize the core tensions, (ii) affirmed the applicability of existing international law, and (iii) become an incubator for the construction of new norms and diffusion thereof. The 2017 collapse of the process marks a caesura in this international discussion on cyber norms so far. Rising geopolitical tensions, namely between the U.S. and Russia, competing tactics, and growing pressure to open the process to others led to this outcome. This combination of factors also explains why the international community created two separate processes at the UN to start in the fall of 2019 that will supersede the previous single process.

To illustrate the obstacles to reaching greater intersubjective agreement on norms for cyberspace also consider this example which was beyond the scope of core article #3: the U.S. government has faced significant challenges communicating its nuanced view and its differentiation between what it considers legitimate political espionage and illegitimate economic espionage. Instead, Washington encountered repeated misunderstandings and misperceptions, particularly by the Chinese government. In 2015, the U.S. government requested that Beijing arrest Chinese hackers Washington considered responsible for economic espionage.[205] Beijing eventually responded by presenting the arrest of hackers allegedly responsible for the breach of the Office of Personnel Management (OPM) and theft of confidential data of U.S. government employees.[206] In light of the public outrage among members of the U.S. Congress over the OPM breach, Beijing apparently believed the arrests would address the U.S. government's demand.[207] However, the White House was subsequently at pains to explain to Beijing that the U.S. government actually considered the OPM breach – as much as it despised its occurrence – not an illegitimate activity but political espionage not prohibited under international law. Therefore, the U.S. had not expected the arrest of these hackers, but rather wanted Beijing to crack down on those carrying out economic espionage. This example illustrates some of the conceptual and semantic challenges specifically associated with the construction of norms for cyberspace also discussed in more detail in the dissertation's conclusion.

2.4. Methodology

This cumulative dissertation is based on qualitative research methods with a focus on comparative case studies[s] and historical analysis. Applying quantitative methods to studies focusing on cyberspace and international relations remains challenging for several reasons. Chief among them is data access. For example, with respect to analyzing cyber incidents, most comprehensive data sets are either classified and housed within government agencies or are proprietary and belong to cyber threat intelligence companies monetizing their knowledge for customers. While some public databases exist,[208] the attribution problem severely limits the type of quantitative analysis possible and the robustness of their explanatory power.

Another challenge with respect to quantitative analysis in the context of state actors is that the number of cyber powers, while expanding quickly, was estimated to be just a handful of countries only a decade ago. As recently as 2010, the U.S., Russia, China, France, and Israel would usually be mentioned by experts as cyber powers (occasionally complemented by other members of the Five Eyes signals intelligence group, the United Kingdom, Australia, Canada, and New Zealand).[209] By 2012, Iran and North Korea emerged as serious players.[210] By late 2016, the number of countries developing offensive cyber-attack capabilities had grown to over 30.[211] This context demonstrates why a small-N approach remained the most promising avenue to pursue for this cumulative dissertation.

The benefits of the qualitative case study approach[212] were another reason to pursue this method. To start, cyberspace remains a comparatively new issue area to study in International Relations, and at the time of designing the dissertation research there was a growing demand (i) to test whether existing frameworks and concepts applied in this domain and (ii) to develop new concepts and taxonomies to capture its unique characteristics. In fact, given the current information-poor environment, the case study approach "gives the researcher an opportunity to fact-check, to consult multiple sources, to go back to primary materials, and to overcome whatever biases may affect the secondary literature" according to John Gerring.[213] Finally, the protean[214] nature of this field of study increases the value of a more inductive approach to help develop frameworks that can be tested over time as more data becomes available.

[s] George and Bennett define a case study as "the detailed examination of an aspect of a historical episode to develop or test historical explanations that may be generalizable to other events," see George, Alexander and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences.* Cambridge, MA: MIT Press, 2005: 17.

This methodological orientation is best illustrated by the monograph in the supplementary material focusing on analyzing a small number of cases. Based on the insights offered by Jack Levy,[215] the monograph's methodological approach was designed to facilitate the development of illustrative ideal types for a phenomenon of growing significance in international relations. The goal was to provide a conceptual framework that could be applied in future empirical research once a growing body of cases and data become available to be tested and for the framework to be populated with.[216] In other words, the case studies discussed in the monograph fall into the hypothesis-generating category of Levy's ideal types. The case studies represent a small-N comparison across four cases (U.S., Iran, Syria, Russia) plus an additional single case study focusing on a specific case and change over time (China). There is an obvious risk of selection bias, which I attempted to mitigate in the first stage of the research, in which I considered other potential case studies, namely North Korea and Israel, that I subsequently discarded after a first review of the empirical data and literature complemented by preliminary expert interviews.

Overall, the methodology applied across this cumulative dissertation aligns with the ambition of analytic eclecticism to be "more modest and pragmatic. It is intended to generate diverse and flexible frameworks, each organized around a concrete problem, with the understanding that it is the problem that drives the construction of the framework" [217] in order to "offer complex causal stories that extricate, translate, and selectively recombine analytic components"[218] while paying special attention to mitigating the risk of theoretical incoherence. With respect to the three core articles, the methodology and theory applied therefore also differ depending on the research question.

Data sources for this the cumulative dissertation range from secondary literature, such as peer-reviewed academic articles and books as well as reports by think tanks and the media, to primary literature, such as government documents, statements, and agreements. With that said, publicly available information remains limited generally and the quality of such data can be poor occasionally even contradictory. In addition, to capture information that is not accessible elsewhere, the research also draws on some unconventional sources for International Relations scholarship including technical reports by cybersecurity companies and information provided on hacker fora. Last but not least, while all references are based on publicly available data, in some cases, interviews with experts in the research community, private sector, and governments helped to determine which source to use in cases of contradictory or divergent data.

Finally, it is also worth mentioning that lessons learned from the research for core article #1 fed into the remaining research of the cumulative dissertation and included the following insights:

(1) The analysis must consider the exploratory character of research of a new field and its limitations;
(2) Special attention must be paid to scrutinizing the available data and primary literature as the body of secondary literature having reviewed and tested primary sources remains comparatively small;
(3) Studying cyberspace requires a multidisciplinary and cross-cutting approach and a basic level of familiarity with related scholarship in other disciplines, namely computer science, legal scholarship, sociology, and economics.

3. Conclusion, Contribution to International Relations Theory, and Future Research

In the 25 years of its modern existence, the Internet has not upended the international system, but it has certainly contributed to several fundamental systemic shifts in significant ways. The best illustration for the significant impact the technology has had is the fact that actions through cyberspace have become such a big concern to the world's only remaining superpower that its political leaders have made it a priority. Consider, for example, U.S. president Obama's televised statement accusing North Korea to be responsible for the hack of Sony Pictures Entertainment and his deal with China's president Xi to limit (Chinese) cyber-enabled theft of (U.S.) intellectual property. Were it not for the exceptional behavior of Donald Trump, any other U.S. president would have likely also made Russia's interference in the 2016 U.S. elections a top priority for the White House.

While the Internet has challenged states' power, the hopes of the Internet's libertarian founding fathers (and mothers, like Elizabeth Feinler) and their utopian vision never fully materialized. John Perry Barlow proclaimed in his 1996 *Declaration of the Independence of Cyberspace*,

> "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. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear."[219]

Twenty years later, it is clear that "great powers are the most important actors in international politics,"[220] a finding most neorealists and neoliberalists can agree on. Moreover, states have also demonstrated how they can use their power to create effects through cyberspace and to shape cyberspace itself. Examples for the latter range from the White House exerting its control over Jon Postel, "the God of the Internet" in 1998, [221] to China's Great Firewall[222] and recent discussions in the U.S. and its allied countries about 5G and discussions about a 'decoupling' of systems between the West and China.[223] The findings of this cumulative dissertation lend weight to Nye's argument that "What is distinctive about power in the cyberdomain is not that governments are out of the picture […] but that different actors possess different power resources and that the gap between state and nonstate actors is narrowing in many instances."[224]

A key finding of this cumulative dissertation is that to empirically assess how exactly the Internet is affecting power in the international system requires the black box of the state to be opened up. It is not useful to assume states are unitary and that they "differ chiefly in size, not in composition."[225] In fact, this assumption carries significant risks of distorting empirical analysis, for example, by exacerbating mirror-imaging problems.[226] It is clear that how governments view cyberspace and their domestic political system shapes how they behave in cyberspace internationally—including the use of coercive cyber power directly and indirectly via proxies.

Another often cited example is the Arab "Twitter"[227] and "Facebook"[228] revolutions and the catalytic role of social media empowering individuals and small networks of people. However, the governmental archives of the fallen regimes also provided a glimpse into elaborate surveillance systems. There are therefore two competing empirical observations between the empowered individual of the Arab Spring and concerns over increasingly powerful state surveillance and censorship. How the two ultimately affect the power balance between states and individuals remains an open question and dependent on the specific regional, cultural, and legal context.

A second key observation across the different lines of inquiry pursued in this dissertation centers on the term 'cybersecurity' and reflects the findings of the additional, cross-cutting line of inquiry outlined in the introduction that merits its own sub-section.

3.1. What Are We Talking About 2.0: Information Security vs Cybersecurity

Complementing the existing literature that applies securitization theory[229] to the study of cyberspace,[230] it is worth highlighting the strategic importance of the debate over 'information security' and 'cybersecurity' and the geo-politics involved. The different studies of this cumulative dissertation have all pointed to the importance of this distinction. This definitional cleavage shapes states' behavior in international negotiations as well as states' use of offensive cyber capabilities. The importance of this ongoing debate between partisans of "information security" and partisans of "cybersecurity" emerged throughout my in-depth study and comparison of the BRICS and into my analysis of the contestation of norms for cyberspace and the use of proxies to project cyber power. The recurrence and salience of this debate across all three lines of inquiry suggest that this dimension ought to be integrated in scholars' research design and baseline assumptions. This is a weakness in much of the literature to date.

To summarize the findings across the three lines of inquiry of this cumulative dissertation, the term 'information security' has essentially taken on a life of its own on the international stage over the past two decades. Originally, information security was a technical term that focused on the protection of the confidentiality, integrity, and availability of information.[231] Moscow and later Beijing started arguing that information itself – content in other words – can be a threat. This effectively broadened the original conceptualization of information security with significant implications for the protection of human rights and democratic societies. In response, liberal democracies opted to use 'cybersecurity' in juxtaposition to this broadened concept of 'information security.' International negotiations have therefore touched on essentially two issues: (i) hacking and the related use of ICT and (ii) content and the related use of ICT.[232]

The beginnings of this politicization and contestation over terms date back to the first UN General Assembly resolution on the issue adopted in January 1999 referencing both "unauthorized interference with ICT" as well as "information terrorism" as threats to be combatted.[233] The former has been a concern shared by liberal democratic governments that view 'information' as a human right to be protected rather than as a security threat to be addressed.[t] Their concern is that authoritarian governments are trying to use 'information security' to advance what can be described as 'illiberal norms'[234] justifying the control of information that liberal democratic governments are opposing. In other words, there is no intersubjective agreement among states "what problems need addressing."[235] Instead, the terminology used leaves a high degree of ambiguity and thereby lack of intersubjective agreement on the meaning of norms.[236]

Government officials have made these different views explicit. For example, Ilya Rogachev, Director of the Department of New Challenges and Threats at the Russian Ministry of Foreign Affairs, stated at a conference in 2015 that: "For the Russian government, information security is also about content."[237] This approach is reflected in the draft International Code of Conduct for Information Security that the Russian and Chinese governments have been promoting in international fora since 2011. The envisioned code expects states to pledge cooperation in "curbing the dissemination of information that incites terrorism, secessionism or extremism or that

[t] This was part of the reason why the working group 'An Internet Free and Secure' of the Freedom Online Coalition, a coalition of governments focused on protecting human rights online, developed a human-centric definition of cybersecurity in response in 2014 (Freedom Online Coalition. "Recommendations for Human Rights Based Approaches to Cybersecurity." September 21, 2015. https://freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf.) Full disclosure: The author of this dissertation co-developed this definition with other members of the working group.

undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment."[238]

On the other hand, the UK government has made clear in a submission to the UN that while many businesses and standards organizations use the term 'information security' given its technical origins, it "is also used by some countries and organizations as part of a doctrine that regards information itself as a threat against which additional protection is needed." Therefore, like other liberal democratic governments,[u] "the United Kingdom does not recognize the validity of the term 'information security' when used in this context, since it could be employed in attempts to legitimize further controls on freedom of expression beyond those agreed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."[239]

An important, related difference is what states consider to be the primary object of their contestation. For some countries, namely autocracies, protecting the state is paramount including through content control. For others, namely liberal democracies, protecting the individual and human is paramount, namely human rights such as freedom of speech. This divergence became evident at the 2012 World Conference on International Telecommunications in Dubai when an Iranian diplomat attempted to redefine international human rights along the lines of state interest.[240] This debate is neither limited to cyber norms nor new. It is the decades-old contestation of sovereignty and human rights.[v]

Looking ahead, this distinction between terms matters with respect to the bigger picture for several reasons. First, the contestation of the term 'information security' relates to the emerging discussion among foreign policy experts with respect to U.S.-China relations.[241] While during the Cold War, the American and Soviet systems were clashing on two levels – (i) a clash between political systems, namely liberal democracy and de facto dictatorships, and (ii) a clash between economic systems, namely capitalism and communism – in the post-Cold War era, China has fully embraced capitalism and turbo-charged it with state-backed funding and support. This reduces the

[u] It is worth noting that this issue is not as black and white as it seems. For example, in India, the forwarding of false rumors through WhatsApp messages incited violence and led to the killing of some 30 people (Purohit, Kunal. "WhatsApp rumours have led to 30 deaths in India." *South China Morning Post.* February 25, 2019. https://www.scmp.com/week-asia/society/article/2187612/whatsapp-rumours-have-led-30-deaths-india-social-media.) Certain types of content therefore also represent significant challenges for liberal democracies. Nevertheless, content is analytically clearly different from hacking.

[v] According to Duncan Hollis, these different views help explain though "why some states will accept some content controls (e.g., prohibiting child porn) because they think they will serve individual interests at the same time they reject other content control, which focus on protecting the state itself." Hollis. Email message to author. March 1, 2019.

fundamental clash that some scholars believe is on the horizon to one between competing political systems, namely between open systems and closed systems.[242] In this line of logic, preserving the political system and ensuring regime stability becomes the single most important goal. These dynamics help explain the intense contestation with respect to information security and norms for cyberspace despite the significant costs associated with cyber incidents such as WannaCry and NotPetya.

Second, how states view these terms influences how they organize themselves, what institutions they create, and how they behave. For example, the institutional structure of U.S. Cyber Command differs significantly form the institutional structures for offensive cyber operations in Russia. This difference can be partly explained by the countries' differing views of the terms and related conceptual approaches. The detailed analysis of Russia's interference in the 2016 U.S. elections demonstrates Moscow's highly integrated approach to influence operations that are carried out by different government agencies and reflects its notion of 'information security.'[243] Moreover, my empirical analysis of how states use proxy relationships to project coercive cyber power also reveals that states that embrace 'information security' as a concept, namely Russia, Iran, and China, also pursue effects and use proxies aligned with this approach, for example, targeting with espionage and other offensive cyber activities not only foreign governments but dissidents and other sources of content critical of the respective regimes.

3.2. Contribution to International Relations Scholarship and Future Research

Beyond the findings outlined above, this cumulative dissertation offers some additional insights to inform the broader International Relations scholarship and future research:

First, with respect to conceptualizing revisionism, core article #3 substantiates the assessment of China as "an emerging bridging revisionist"[244] that "will seek rule-based revolution"[245] rather than full integration or rejection of the international order.[246] This is illustrated by China first contesting that international law applies to cyberspace while simultaneously advancing the idea of an International Code of Conduct for Information Society in partnership with Russia. This points to interesting questions for future research, namely how will China's participation in institutional processes like the UNGGE shape its revisionist behavior and if and how it will "mobilize significant material and ideological resources in pursuit of its aims"?[247]

Second, with respect to the literature on balancing, the expectation has been that "every great power has carefully monitored its peer competitors and calibrated its efforts accordingly."[248] However, the analysis pursued through the second line of inquiry points to a fascinating divergence with respect to offensive cyber operations. Whereas some countries, namely Russia, pursue a much more integrated approach combining hacking with information campaigns to maximize the impact of its influence operations, others, namely the U.S. and Western governments, continue to treat these two dimensions as separate following the institutional split between them in the early 2000s. Despite Russia's successful influence operations in Ukraine and the 2016 U.S. elections, Western governments do not appear to have "calibrated" their efforts significantly to emulate the Russian approach.

This raises several important questions, for example, to what extent are characteristics of the domestic political system and democratic values interfering with pressures to calibrate efforts? Or are Russia's activities not considered a success? Or has the pressure to emulate Russia not been great enough in the absence of "the cauldron of war."[249] In addition, considering the expected proliferation of cyber capabilities with more than 30 countries developing offensive cyber capabilities as of 2017,[250] what approach will other countries adopt? And what will these proliferation dynamics look like (ideally broken down by the transfer of tools, sharing of expertise, and rise of the "ex" i.e. individuals trained by their respective governments in offensive cyber capabilities who will eventually leave government service)?[251]

Relatedly, another interesting area for future research centers on Russia's interference in the 2016 U.S. elections. My research across the three lines of inquiry found that different actors conceptualize cybersecurity and information security very differently. The surprising effect of Russia's activity and lack of preparedness by the U.S. therefore raises an important question: Have analysts and decision-makers in the U.S. suffered from a mirror-imaging problem that "imposes personal perspectives and cultural background on incomplete data, undermining objectivity"?[252] As Hafner-Burton et al point out, "systematic failures in perception can fundamentally change the strategic setting."[253] As part of the broader interest in the "Behavioral Revolution" in International Relations theory as Hafner-Burton et al have called it, further investigating the beliefs that fed into the analysis and decision-making processes from 2014-2016 would be a promising case study to better understand if this may be an example of "application of faulty heuristics to explain strategic situations" or explained by "time-weighed differences in time-weighed behavior."[254]

Fourth, Russia's and China's behavior insisting on their view of information security that prioritizes regime stability above all else raises a separate fascinating question: to what extent have authoritarian regimes internalized lessons learned from the "Helsinki effect"?[255] Have they resisted separating into different diplomatic baskets their concerns over information as a threat as a distinct category from their concerns over hacking as a threat because of the Soviet experience[256] with the third basket of the Helsinki Accords? These questions arose specifically in the context of the analysis of the contestation of norms for cyberspace. This further investigation would benefit from analysis of primary sources that shed light on the thinking of Russian and Chinese officials.

Fifth, with respect to the scholarship on global governance and functionalist theory, the Internet presents an important case study in the broader inquiry of "Governance without a state: Can it work?"[257] Core article #1 and the first line of inquiry focus on this question in a slightly more expanded format by including "whether the Internet's current governance model will be tolerated by states?" Some states insist on the sovereigntist, multilateral top-down intergovernmental model to supersede the private transnational institutions that have emerged in recent decades. The intensifying contestation of the latter will shed light on the nature and stages of the "organizational life cycle"[258] of private transnational regulatory organizations. Beyond institutions such as the IETF, this includes recent initiatives such as the *Paris Call for Trust and Security in Cyberspace* established by the French government in 2018, driven behind the scenes by Microsoft acting as a norm entrepreneur, and subsequently signed by 67 states, 139 international and civil society organizations, and 358 private-sector companies including Huawei.[259] In the wake of the 2017 collapse of the UNGGE, the Paris Call was created by actors who were keen to "act when divergent interests block intergovernmental agreement."[260] If these governance models demonstrate longevity, the questions about their legitimacy, constituencies, and influence will grow in importance.

Relatedly, after a decade-long hiatus in the history of international commissions, the Global Commission on Internet Governance and the Global Commission on the Stability of Cyberspace offer new case studies to reassess the findings of the 2005 comprehensive review of global commissions within global governance.[261] While some conclusions about their limited impact (with the exception of the Brundtland report that created the framing of "sustainable development"[262]) and disconnect from ongoing policy processes seem to hold true, their creation nevertheless raises the question why global commissions saw a revival and why specifically in this area.

Seventh, the international community is facing growing demands to cultivate norms for emerging technologies. Societies worldwide are experiencing a technological revolution from increased digitization and artificial intelligence to additive manufacturing and synthetic biology which are all enabled by increasing computing power. The third line of inquiry and its findings with respect to how norms apply to cyberspace offers a case study for how the international community is approaching these emerging technologies in the 21st century. Comparing the dynamics in the construction of international norms for cyberspace with the norms process focusing on other emerging technologies, for example, the application of artificial intelligence in the military context (note Human Rights Watch's "Killer Robot Campaign"[263]), the discussion of norms for outer space, or the renewed interest in biotech,[264] may yield useful insights if states approach norms governing emerging technologies differently than norms in other areas or differently across technologies.

Eighth, as some states attempt to enforce nascent norms for cyberspace, recent insights in International Relations theory focusing on the benefits and costs of "publicizing noncompliance" as well as "the language of compromise"[265] offer useful conceptual frameworks to empirically test states' behavior and reactions with respect to cyber incidents.[266] This applies, for example, to the criminal charges against actors having carried out a cyber attack or the release of public statements to hold states accountable for transgressions. This line of inquiry is therefore also connected to the broader discussion about how to conceptualize deterrence with respect to cyberspace.[267] The emergence of new concepts such as "persistent engagement" [268] and ongoing debates about how to conceptualize "cyber stability"[269] point to further innovative scholarship in this area.

Ninth, while some foundational concepts in International Relations theory have already been discussed in the context of cyberspace ranging from whether or not it is revolutionary for military conflict,[270] to the notion of 'cyber power'[271] and the cultivation of norms for cybersecurity,[272] other concepts, namely that of sovereignty, require more attention by International Relations scholars. The current debates among international lawyers as well as U.S. military lawyers has important implication for the concept of sovereignty.[273] These build on earlier works discussing sovereignty in the context of cyberspace[274] and merit future research comparing those discussions with the existing seminal International Relations works on sovereignty.[275] This strand of research also encompasses the ongoing debate about "The Rise of a Cybered Westphalian Age"[276] especially in the wake of the 5G and "decoupling" discussions between the U.S. and China.

Finally, a clear systemic change created by the Internet is the "Golden Age of Surveillance"[277] predicted by Robert Kaplan in the late 1990s.[278] Governments have unprecedented capabilities to collect data today. Since Edward Snowden, the NSA is no longer simply known as "No Such Agency" but has become a household name known to the public much like "The Five Eyes." From an International Relations theory perspective, this raises the interesting question whether this expansion of intelligence collection has reduced uncertainty, known[279] in political science to be a major cause for war and risk of accidental escalation. Has the unprecedented access to information alleviated the pressure "on the need for self-help," a key assumption of neorealism, since "not knowing others' intentions and aware that there is no higher authority to protect them, great powers understand that they must provide for their own security"?[280] Or is "big data" bigger but not big enough? Or is the capability to analyze the data outpaced by the ability to collect data? Or is the data confusing or mixed with misleading information? Will artificial intelligence change any of these factors in the near future? And how does it interact with the increased uncertainty discussed in section 1.3.4.

If anything, this cumulative dissertation demonstrates the importance of studying the impact the Internet is having on international affairs, which cuts across issue areas and affects the transition as well as the diffusion of power shaping the international system writ large. The first line of inquiry revealed that while rising powers contest the historical dominance of the U.S., their reactions differ significantly and can be partly explained by the divergence of political systems. Core article #1 in Appendix 1 outlines this analysis in detail. How this difference in behavior will influence the transition of power and balancing behavior in the long-run remains an open empirical question for future research. Meanwhile, the second line of inquiry highlights the arguably even more interesting set of questions associated with the diffusion of power and *diffusion of reach* the Internet has enabled. Core article #2 in Appendix 2 and the monograph included in the supplementary material shed light on this topic conceptually and empirically. Why and how non-state actors will yield coercive cyber power in the future, including whether and to what extent they will work with the growing number of states interested in acquiring and using such power, will be an important topic to study further. Last but not least, the third line of inquiry went beyond analyzing whose power will be affected by focusing on how norms for cyberspace are being constructed. Core article #3 in Appendix 3 explains why the cyber norms process has unfolded as it has over the past twenty years including the recent collapse of the process at the UN in 2017 and its revival and reincarnation as two processes thereafter. This third line of inquiry also outlines some broader insights for the construction of norms for cyberspace and emerging technologies generally,

namely the influential role of state practice, considering that the speed of the technologies' evolution and impact outpaces the speed of conventional diplomacy and international cooperation.

References

[1] International Telecommunication Union. “New ITU statistics show more than half the world is now using the Internet.” December 6, 2018. https://news.itu.int/itu-statistics-leaving-no-one-offline/.
[2] Lynn III, William J. “Defending a New Domain.” *Foreign Affairs*, September/October 2010. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.
[3] Office of the Assistant Secretary of Defense. “Cyber Command Achieves Full Operational Capacity.” November 3, 2010. https://www.stratcom.mil/Media/News/News-Article-View/Article/983818/cyber-command-achieves-full-operational-capability/.
[4] North Atlantic Treaty Organization. “Warsaw Summit Communiqué.” July 9, 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
[5] U.S. Office of the Director of National Intelligence, U.S. Department of Defense, U.S. National Security Agency. *Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States*, by James R. Clapper, Marcel Lettre, and Michael S. Rogers. Washington, DC, 2017. https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.
[6] Lerche, Jelka, Götz Hamann, and Inge Kutter. “Jetzt ein Internetministerium!” *Die Zeit.* November 21, 2013. https://www.zeit.de/2013/48/infografik-internetministerium; For example: G8. *G8 Deauville Declaration: Renewed Commitment for Freedom and Democracy.* Deauville: G8, 2011. http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html; International Telecommunication Union. "One Third of the World`s Population Is Online." Geneva: International Telecommunication Union, 2011. http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf.
[7] U.S. Office of the Director of National Intelligence. National Intelligence Council. *Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution.* Washington, DC, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[8] Nye, Joseph S. *The Future of Power*. Public Affairs, 2011.
[9] See, for example, Naím, Moisés. *The End of Power: From Boardrooms to Battlefields and Churches to States, Why Being in Charge Isn't What it Used to Be*. Basic Books, 2014.
[10] Nye, Joseph S. *The Future of Power*. Public Affairs, 2011; See also: Nye Jr, Joseph S. *Cyber Power*. Harvard University – Belfer Center for Science and International Affairs, 2010.
[11] For of the first uses of the term “swing states” in an international relations rather than domestic U.S. election context, see Kliman, Daniel M., and Richard Fontaine. *Global swing states: Brazil, India, Indonesia, Turkey and the future of international order*. Center for a New American Security, 2012.
[12] Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 7.
[13] Carr, John. “Online Crimes Against Children.” *Freedom from Fear* 7. July 2010, 26–29.
[14] Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. "A brief history of the Internet." *ACM SIGCOMM Computer Communication Review* 39, no. 5 (2009): 22-31; “Evolution of the Cyber

Domain: The Implications for National and Global Security." International Institute for Strategic Studies, December 2, 2015: 54.

[15] Scheli, S. and G D Garson. "E-Government." In *The Internet Encyclopedia*, edited by H. Bidgoli. New Jersey: John Wiley & Sons, 2004: 590–601.

[16] Nigel Inkster. *China's Cyber Power*. New York: Routledge, 2016: 124; China Education and Research Network. "Evolution of Internet in China." Accessed May 27, 2012. http://www.edu.cn/introduction_1378/20060323/t20060323_4285.shtml (site discontinued).

[17] It is important to clearly identify the period covered by studies focusing on the Internet and to distinguish important milestones in the technology's history. One indicator for the disconnect between broader International Relations scholarship and scholarship specific to cyberspace is how casual the former has treated the subject including leading to factual errors. For example, Kenneth Abbott, Jessica Green, and Robert Keohane in their 2016 *International Organization* article write that the Internet "did not exist before 1990" (see Abbott, Kenneth W., Jessica F. Green, and Robert O. Keohane. "Organizational ecology and institutional change in global governance." *International Organization* 70, no. 2 (2016): 248.) Not only does the Internet date back to the 1960s but the private transnational regulatory organizations of interest to the authors such as the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers also precede 1990.

[18] Arkin, W M."The Cyber Bomb in Yugoslavia." *The Washington Post*. October 25, 1999; Borger, J. "Pentagon Kept the Lid on Cyberwar in Kosovo." *The Guardian*. November 9, 1999.

[19] Based on Internet Systems Consortium. "Internet host count history." Accessed May 18, 2012. http://www.isc.org/solutions/survey/history (site discontinued); Internet Systems Consortium. "Internet Domain Survey, January, 2018." Accessed August 26, 2019. https://downloads.isc.org/www/survey/reports/2018/01/.

[20] For a detailed analysis of the history of the competing protocols, see Goldsmith, Jack and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press, 2006.

[21] Zittrain, Jonathan. *The Future of the Internet - and How to Stop it*. Yale University Press, 2008: 67-68.

[22] Nye Jr, Joseph S. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*. 5, no. 4 (Winter 2011): 18–38.

[23] Oxford Dictionaries. "Cyber." *Oxford Dictionaries*, 2013. http://oxforddictionaries.com/definition/english/cyber?q=cyber.

[24] Betz, David J. and Tim Stevens. "Chapter One: Power and Cyberspace." *Adelphi Series* 51, no. 424 (2011): 36, 39.

[25] Cavelty, Myriam Dunn. *Cyber-security and Threat Politics: US Efforts to Secure the Information Age*. Routledge, 2008; Dunn Cavelty, Myriam. "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse." *International Studies Review* 15, no. 1 (2013): 105-122. Cavely's work on securitzation builds on Buzan, Barry, Ole Wæver, and Jaap De Wilde. *Security: A New Framework for Analysis*. Lynne Rienner Publishers, 1998.

[26] Gibson, William. *Neuromancer*. Vol. 1. Aleph, 2015; Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Electronic Frontiers Foundation. February 8, 1996. https://www.eff.org/cyberspace-independence; Dunn Cavelty, Myriam. "From cyber-bombs to

political fallout: Threat representations with an impact in the cyber-security discourse." *International Studies Review* 15, no. 1 (2013): 105-122.

[27] Maurer, Tim and Robert Morgus. *Compilation of Existing Cybersecurity and Information Security Related Definitions*. Washington, DC: New America, 2014. https://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/.

[28] Internet Engineering Task Force. "Internet Security Glossary, Version 2." Fremont, CA: the IETF Trust, 2007. https://tools.ietf.org/html/rfc4949.

[29] International Organization for Standardization. "ISO/IEC Glossary of IT Security Terminology," ISO/IEC, 2013.

[30] Betz, David J. and Tim Stevens. "Chapter One: Power and Cyberspace." *Adelphi Series* 51, no. 424 (2011): 37; ISO, *Information Technology - Security Techniques - Guidelines for Cybersecurity* (Berlin: International Standardisation Organization/DIN Deutsches Institut für Normung e.V., 2009), vii. Accessed January 22, 2013. http://www.first.org/vendor-sig/isodocs/iso-iec-n7558.pdf.

[31] Nye Jr, Joseph S. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*. 5, no. 4 (Winter 2011): 19.

[32] Zittrain, Jonathan. *The Future of the Internet - And How to Stop It.* New Haven/London: Yale University Press, 2009: 67–71.

[33] Nye Jr, Joseph S. "Cyberpower". Cambridge, Mass.: Harvard Belfer Center for Science and International Affairs, May 2010: 3.

[34] Demchak, Chris C. and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32-61. https://www.jstor.org/stable/26270509.

[35] Peters, John Durham. *Speaking into the Air: A History of the Idea of Communication*. Chicago: University of Chicago Press, 2012.

[36] Shirky, Clay. *Here Comes Everybody: The Power of Organizing Without Organizations*. London: Penguin Books, 2008.

[37] Klein, Hans K. "Tocqueville in Cyberspace: Using the Internet for Citizen Associations." *The Information Society* 15, no. 4 (1999): 213-220; Leon, Gabriel. "How the long history of leaderless movements helps us understand the 'yellow vests' protests." Monkey Cage. *Washington Post.* December 12, 2018. https://www.washingtonpost.com/news/monkey-cage/wp/2018/12/12/did-the-yellow-vests-protests-spread-only-because-of-social-media-no-leaderless-mass-movements-changed-nations-long-before-this/?utm_term=.2c5ac46c8e19.

[38] Clinton, Hillary Rodham. "Remarks on Internet Freedom." Speech, Washington, DC, January 21, 2010. U.S. Department of State Archives. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[39]Mozur, Paul, Jonah M. Kessel, and Melissa Chan. "Made in China, Exported to the World: The Surveillance State." *New York Times.* April 24, 2019. https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

[40] For a comprehensive overview of the literature on globalization, see Baylis, John, Patricia Owens, and Steve Smith, eds. *The Globalization of World Politics: An Introduction to International Relations*. Oxford University Press, 2008.

[41] Keohane, Robert O. "The Globalization of Informal Violence, Theories of World Politics, and 'The Liberalism of Fear.'" Paper presented at the Annual Meeting of the American Political Science Association, Boston, MA, August 28, 2002.
[42] Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 9-12.
[43] Keohane, Robert O. "The Globalization of Informal Violence, Theories of World Politics, and 'The Liberalism of Fear.'" Paper presented at the Annual Meeting of the American Political Science Association, Boston, MA, August 28, 2002.
[44] Parent, Joseph M., and Sebastian Rosato. "Balancing in neorealism." *International Security* 40, no. 2 (2015): 56.
[45] Slayton, Rebecca. "What is the cyber offense-defense balance? Conceptions, causes, and assessment." *International Security* 41, no. 3 (2017): 74.
[46] Lynn III, William F. "Defending a New Domain - The Pentagon's Cyberstrategy." *Foreign Affairs* 89 (2010): 97; Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Rand Corporation, 2009; Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no. 2 (2013): 7-40; Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. University of Georgia Press, 2011; Lieber, Keir. "The offense-defense balance and cyber warfare." *Cyber Analogies* (2014): 96-107.
[47] "Sources: Staged cyber attack reveals vulnerability in power grid." *CNN*. Accessed July 25, 2008. https://edition.cnn.com/2007/US/09/26/power.at.risk/ (site discontinued).
[48] Lin, Herbert. "Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion." *Geo. J. Int'l Aff.* 11 (2010): 127; Gartzke, Erik, and Jon R. Lindsay. "Weaving tangled webs: offense, defense, and deception in cyberspace." *Security Studies* 24, no. 2 (2015): 316-348; Kello, Lucas. *The Virtual Weapon and International Order*. Yale University Press, 2017: 78.
[49] "Cyber Leaders: A Discussion with the Honorable Eric Rosenbach." Panel discussion, Center for Strategic and International Studies. Washington, DC. October 2, 2014. http://csis.org/event/cyber-leaders.
[50] Von Clausewitz, Carl. *Vom Kriege*. Berlin: Dümmlers Verlag, 1832. http://www.clausewitz.com/readings/VomKriege1832/Book1.htm.
[51] U.S. Cyber Command. *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.* Fort Meade, MD, 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
[52] U.S. Department of Defense. *Summary: Department of Defense Cyber Strategy.* Washington, DC, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[53] U.S. Department of Defense. *Summary of the 2018 National Defense Strategy of the United States of America. Washington, DC, 2018.* https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
[54] See Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 16.
[55] See Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 16-17.

[56] U.S. Department of Justice. “U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts.” Press release no. 17-278. March 15, 2017. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.
[57] Perlroth, Nicole and Quentin Hardy. “Bank Hacking Was the Work of Iranians, Officials Say.” *New York Times.* January 8, 2013. https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.
[58] See Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 11.
[59] Lynn III, William J. “Defending a New Domain.” *Foreign Affairs*. September/October 2010. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain; Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37.
[60] See Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 24.
[61] Singer, Peter Warren. *Corporate Warriors: The Rise of the Privatized Military Industry*. Cornell University Press, 2008: 91
[62] Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford University Press, 2016: 2-3; Lin, Herb. “Still More on Loud Cyber Weapons.” *Lawfare* (blog). Brookings Institution. October 19, 2016. https://www.lawfareblog.com/still-more-loud-cyber-weapons; Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009: 65.
https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf; Herr, Trey. "PrEP: A Framework for Malware & Cyber Weapons." *Journal of Information Warfare* 13, no. 1 (2014): 87-106.
[63] Chesney, Robert. “Should NSA and CYBERCOM Split? The Legal and Policy Hurdles as They Developed Over the Past Year.” *Lawfare* (blog). Brookings Institution. July 24, 2017. https://www.lawfareblog.com/should-nsa-and-cybercom-split-legal-and-policy-hurdles-they-developed-over-past-year.
[64] See Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 15.
[65] See also Herr, Trey, and Paul Rosenzweig. "Cyber Weapons and Export Control: Incorporating Dual Use with the Prep Model." *J. Nat'l Sec. L. & Pol'y* 8 (2015): 301; Maurer, Tim. “Internet Freedom and Export Controls: Briefing before the Commission on Security and Cooperation in Europe.” March 3, 2016. https://carnegieendowment.org/files/Tim_Maurer_final_briefing_-_03.03.20162.pdf; Slayton, Rebecca. "What is the cyber offense-defense balance? Conceptions, causes, and assessment." *International Security* 41, no. 3 (2017): 108.
[66] Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009: 57-59. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.
[67] Farrell, Henry and Charles L. Glaser. "The role of effects, saliencies and norms in US Cyberwar Doctrine." *Journal of Cybersecurity* 3, no. 1 (March 2017): 10.
[68] Maurer, Tim. “Internet Freedom and Export Controls: Briefing before the Commission on Security and Cooperation in Europe.” March 3, 2016.
https://carnegieendowment.org/files/Tim_Maurer_final_briefing_-_03.03.20162.pdf

[69] Perlroth, Nicole. "Reinventing the Internet to Make It Safer." *Bits* (blog). *New York Times.* December 2, 2014. https://bits.blogs.nytimes.com/2014/12/02/reinventing-the-internet-to-make-it-safer/?mtrref=www.google.com&gwh=83EA0353A5EC87F294F247A7D195CB0B&gwt=pay&assetType=REGIWALL; see also: Timberg, Craig. "A Flaw in the Design." *Washington Post.* May 30, 2015. https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?utm_term=.c203c4326601.

[70] Bejtlich, Richard. "The Origin of the Quote 'There Are Two Types of Companies.'" *TaoSecurity* (blog). December 18, 2018. https://taosecurity.blogspot.com/2018/12/the-origin-of-quote-there-are-two-types.html.

[71] Lin, Herbert. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 46–70. https://www.jstor.org/stable/26267261.

[72] Maurer, Tim. "SOLAR SUNRISE: Cyber Attack from Iraq?" In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, edited by Jason Healey. Vienna, VA: Cyber Conflict Studies Association, 2013.

[73] Hay Newman, Lily. "Russian Hackers Haven't Stopped Probing the US Power Grid." *WIRED.* November 18, 2018. https://www.wired.com/story/russian-hackers-us-power-grid-attacks/.

[74] Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *WIRED*. Mark 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[75] Friedman, Thomas L. *The World Is Flat: A Brief History of the Twenty-First Century*. New York: Macmillan, 2005.

[76] Baylis, John, Patricia Owens, and Steve Smith, eds. *The Globalization of World Politics: An Introduction to International Relations*. 4th ed. New York: Oxford University Press, 2008: 8.

[77] Sanger, David E., Michael S. Schmidt, and Nicole Perlroth, "Obama Vows a Response to Cyberattack on Sony." *New York Times*. December 19, 2014. www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html; Elkind, Peter. "Inside the Hack of the Century." *Fortune*. July 1, 2015. http://fortune.com/sony-hack-part-1/; Hess, Amanda. "Inside the Sony Hack." *Slate*. November 22, 2015. www.slate.com/articles/technology/users/2015/11/sony_employees_on_the_hack_one_year_later.html.

[78] U.S. Department of Justice. U.S. Attorney's Office for the Southern District of New York. "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities." Press release no. 16-065. March 24, 2016. www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.

[79] For example, one of the first comprehensive history books of cyber incidents was edited and published by the director of the Atlantic Council's Cyber Statecraft Initiative: Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Vienna, VA: Cyber Conflict Studies Association, 2013. Another example is Martin Libicki's publication on cyber deterrence: Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf. Another example is James Lewis's writings through the Center for Strategic and International Studies:

Lewis, James. *Conflict and Negotiation in Cyberspace.* Washington, DC: Center for Strategic and International Studies, 2013. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf.

[80] A good example is the highly influential report "APT1 - Exposing One of China's Cyber Espionage Units" published by cybersecurity threat intelligence company Mandiant in 2013 providing detailed insight into a Chinese state-sponsored espionage campaign: Mandiant. *APT1 - Exposing One of China's Cyber Espionage Units*. 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[81] Henderson, Scott J. *The dark visitor: Inside the world of Chinese hackers*. Self-published, Lulu, 2007; Henderson, Scott. "Beijing's Rising Hacker Stars: How Does Mother China React?'" *IO Sphere* (2008): 23-28.

[82] Lessig, Lawrence. *Code and Other Laws of Cyberspace*. Basic Books, 1999.

[83] Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Verso books, 2014.

[84] Lusthaus, Jonathan. *Industry of Anonymity: Inside the Business of Cybercrime*. Harvard University Press, 2018.

[85] Kanuck, Sean. "Sovereign discourse on cyber conflict under international law." *Tex. L. REv.* 88 (2009): 1571.

[86] Swire, Peter, and Kenesa Ahmad. "Encryption and Globalization." *Columbia Science and Technology Law Review* 23 (2012).

[87] Price, Monroe E. *Free Expression, Globalism, and the New Strategic Communication*. Cambridge University Press, 2015.

[88] Kalathil, Shanthi, and Taylor C. Boas. "The Internet and state control in authoritarian regimes: China, Cuba and the counterrevolution." *First Monday* 6, no. 8 (2001); Deibert, Ronald, and Rafal Rohozinski. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21, no. 4 (2010): 43-57.

[89] Arquilla, John, and David Ronfeldt. "Cyberwar is coming!." *Comparative Strategy* 12, no. 2 (1993): 141-165.

[90] Choucri, Nazli. *Cyberpolitics in International Relations*. MIT Press, 2012; Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda. "Institutions for cyber security: International responses and global imperatives." *Information Technology for Development* 20, no. 2 (2014): 96-121; Nye Jr, Joseph S. *Cyber power*. Harvard University - Belfer Center for Science and International Affairs, 2010.

[91] Hofmann, Jeanette, Christian Katzenbach, and Kirsten Gollatz. "Between coordination and regulation: Finding the governance in Internet governance." *New Media & Society* 19, no. 9 (2017): 1406-1423; Hofmann, Jeanette. "Multi-stakeholderism in Internet governance: putting a fiction into practice." *Journal of Cyber Policy* 1, no. 1 (2016): 29-49; Mueller, Milton L. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. MIT press, 2009; Mueller, Milton L. *Networks and States: The Global Politics of Internet Governance*. MIT press, 2010; Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. "Internet security and networked governance in international relations." *International Studies Review* 15, no. 1 (2013): 86-104; DeNardis, Laura. *Protocol politics: The globalization of Internet governance*. MIT Press, 2009; DeNardis, Laura. "Hidden levers of Internet control: An infrastructure-based theory of Internet governance." *Information, Communication & Society* 15, no. 5 (2012): 720-738; DeNardis, Laura. *The Global War for Internet Governance*. Yale University Press, 2014; Raymond, Mark,

and Laura DeNardis. "Multistakeholderism: anatomy of an inchoate global institution." *International Theory* 7, no. 3 (2015): 572-616; Drake, William J., Monroe E. Price, and Joana Varon Ferraz. *Internet Governance*. USC Annenberg Press, 2014; Drake, William J., ed. *The Working Group on Internet Governance: 10th Anniversary Reflections*. Johannesburg: Association for Progressive Communications, 2015. http://www.mediachange.ch/media/pdf/publications/IG_10_Final.pdf.

[92] Thomas, Timothy L. *Russian Views on Information-Based Wafare*. Air Force University Maxwell AFB Airpower Journal, 1996; Thomas, Timothy. "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *The Journal of Slavic Military Studies* 27, no. 1 (2014): 101-130; Anderson, Collin. "Dimming the Internet: Detecting throttling as a mechanism of censorship in Iran." *arXiv preprint arXiv:1306.4361* (2013); Anderson, Colin and Karim Sadjadpour. *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*. Washington, DC: Carnegie Endowment for International Peace, 2018. Lewis, James, Victor Cha, Jenny Jun, Scott LaFoy, and Ethan Sohn. *North Korea's Cyber Operations: Strategy and Responses.* Washington, DC: Center for Strategic and International Studies, 2015. https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations.

[93] Denning, Dorothy Elizabeth Robling. *Information Warfare and Security*. Vol. 4. Reading, MA: Addison-Wesley, 1999; Denning, Dorothy E. "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy." *Networks and netwars: The future of terror, crime, and militancy* 239 (2001): 288; Lewis, James Andrew. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic & International Studies, 2002; Lewis, James Andrew, ed. *Cyber security: Turning national solutions into international cooperation*. No. 25. Center for Strategic & International Studies, 2003; Libicki, Martin C. *Conquest in cyberspace: national security and information warfare*. Cambridge University Press, 2007; Libicki, Martin C. "The strategic uses of ambiguity in cyberspace." *Military and Strategic Affairs* 3, no. 3 (2011): 3-10; Cavelty, Myriam Dunn. *Cyber-security and threat politics: US efforts to secure the information age*. Routledge, 2007; Deibert, Ronald J. "Dark guests and great firewalls: The Internet and Chinese security policy." *Journal of Social Issues* 58, no. 1 (2002): 143-159; Deibert, Ronald J. "The geopolitics of internet control: Censorship, sovereignty, and cyberspace." In *Routledge Handbook of Internet Politics*. Routledge, 2008: 339-352.

[94] G7. *G7 Ministerial Conference on the Global Information Society. Ministerial Conference Summary* 1995. Accessed November 15, 2012. http://aei.pitt.edu/33414/1/A161.pdf.

[95] Mueller, Milton, Karl Grindal, Brenden Kuerbis, and Farzaneh Badiei. "Cyber Attribution." *The Cyber Defense Review* 4, no. 1 (2019): 107-122; DeNardis, Laura. *The Internet in Everything*. New Haven, CT: Yale University Press, forthcoming; Lewis, James. "Internet Governance: Inevitable Transitions." Internet Governance paper series. Waterloo: Center for International Governance Innovation, 2013. https://www.cigionline.org/publications/internet-governance-inevitable-transitions.

[96] Deibert, Ron. "Authoritarianism goes global: Cyberspace under siege." *Journal of Democracy* 26, no. 3 (2015): 64-78; Deibert, Ron. "The geopolitics of cyberspace after Snowden." *Current History* 114, no. 768 (2015): 9; Deibert, Ronald. *Black code: Surveillance, privacy, and the dark side of the Internet*. McClelland & Stewart Limited, 2013; Nye, Joseph S. "The regime complex for managing global cyber activities." *Global Commission on Internet Governance* (2014).

[97] Sil, Rudra, and Peter J. Katzenstein. "Analytic eclecticism in the study of world politics: Reconfiguring problems and mechanisms across research traditions." *Perspectives on Politics* 8, no. 2 (2010): 412.
[98] Wu, Tim, and Jack Goldsmith. "Who Controls the Internet? Illusions of a Borderless World." (2006); Drezner, Daniel W. "The global governance of the Internet: Bringing the state back in." *Political Science Quarterly* 119, no. 3 (2004): 477-498.
[99] Kleinwächter, Wolfgang. "Sharing Decision Making in Internet Governance: The Impact of the WGIG Definition." In *The Working Group on Internet Governance: 10th Anniversary Reflections*, edited by William J. Drake, 66-88. Johannesburg: Association for Progressive Communication, 2015: 87. http://www.mediachange.ch/media/pdf/publications/IG_10_Final.pdf.
[100] Daskal, Jennifer. "The Un-territoriality of data." *Yale LJ* 125 (2015): 326; Daskal, Jennifer. "Law enforcement access to data across borders: The evolving security and rights issues." *J. Nat'l Sec. L. & Pol'y* 8 (2015): 473.
[101] Raymond, Mark, and Laura DeNardis. "Multistakeholderism: anatomy of an inchoate global institution." *International Theory* 7, no. 3 (2015): 572-616.
[102] Mueller, Milton L. *Networks and States: The Global Politics of Internet Governance*. MIT press, 2010.
[103] Abbott, Kenneth W., Jessica F. Green, and Robert O. Keohane. "Organizational ecology and institutional change in global governance." *International Organization* 70, no. 2 (2016): 247-277.
[104] For a more detailed description of this element, see Budnitsky, Stanislav. "Milton Mueller, Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace." *International Journal of Communication* 11 (2017): 5.
[105] United Nations. Counter-Terrorism Implementation Task Force. *Report of the Working Group on*
Countering the Use of the Internet for Terrorist Purposes. New York: United Nations, February 2009; United Nations. Counter-Terrorism Implementation Task Force. *Working Group Compendium – Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects*. New York: United Nations, May 2011; David P. Fidler, Overview of International Legal Issues and Cyber Terrorism (Bloomington, IN: International Law Association Study Group on Cybersecurity, Terrorism, and International Law, 2015); Conway, Maura. "What Is Cyberterrorism?" *Current History* 101, no. 659 (December 2002): 436–342. http://www.currenthistory.com/pdf_org_files/101_659_436.pdf; Singer, Peter W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014: 96–97; Kingsbury, Alex. "Documents Reveal Al Qaeda Cyberattacks." *U.S. News*. April 14, 2010. https://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks; Pagliery, Jose. "ISIS Is Attacking the U.S. Energy Grid (and Failing)." *CNN*. October 16, 2015. http://money.cnn.com/2015/10/15/technology/isis-energy-grid/; U.S. Department of Justice. "ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges." Press release no. 15-1280. October 15, 2015. www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges; Turla, Jay. "Getting to Know Kosova Hacker's Security Crew plus an Exclusive Interview with Th3 Dir3ctorY." InfoSec Institute. June 11, 2013. http://resources.infosecinstitute.com/getting-to-know-kosova-hackers-security-crew-plus-an-exclusive-interview-with-th3-dir3ctory/; Coker, Margaret, Danny Yadron, and Damian Paletta. "Hacker Killed by Drone Was Islamic State's 'Secret Weapon.'" *Wall Street Journal*. August 27,

2015. www.wsj.com/articles/hacker-killed-by-drone-was-secret-weapon-1440718560; Franceschi-Bicchierai, Lorenzo. “How a Teenage Hacker Became the Target of a US Drone Strike.” Motherboard. *Vice*. August 28, 2015. http://motherboard.vice.com/read/junaid-hussain-isis-hacker-drone.

[106] Clarke, Richard Alan, and Robert K. Knake. *Cyber War*. HarperCollins, 2011; Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, USA, 2013.

[107] Dombrowski, Peter, and Chris C. Demchak. "Cyber war, cybered conflict, and the maritime domain." *Naval War College Review* 67, no. 2 (2014): 70-96; Deibert, Ronald J., Rafal Rohozinski, and Masashi Crete-Nishihata. "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war." *Security Dialogue* 43, no. 1 (2012): 3-24; Geers, Kenneth, ed. *Cyber War in Perspective: Russian Aggression against Ukraine.* Tallin: NATO Cooperative Cyber Defence Centre of Excellence, 2015. https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf; Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible digital front: Can cyber attacks shape battlefield events?." *Journal of Conflict Resolution* 63, no. 2 (2019): 317-347.

[108] Penenberg, Adam. “Info-terror.” *Forbes.* October 10, 1997. https://www.forbes.com/1997/10/10/col.html#42c6c38c2bf8.

[109] “The Cyber 9/12 Project.” Atlantic Council and Science Applications International Corporation. Washington, DC. December 8, 2011. https://www.atlanticcouncil.org/events/past-events/the-cyber-9-12-project.

[110] Gavin, Francis J. “Crisis Instability and Preemption: The 1914 Railroad Analogy.” In *Understanding Cyber Conflict: 14 Analogies,* edited by George Perkovich and Ariel E. Levite, 111-122. Washington, DC: Georgetown University Press, 2017. https://carnegieendowment.org/2017/10/16/crisis-instability-and-preemption-1914-railroad-analogy-pub-73401.

[111] Perkovich, George and Ariel E. Levite. “Introduction to Understanding Cyber Conflict: 14 Analogies.” In *Understanding Cyber Conflict: 14 Analogies,* edited by George Perkovich and Ariel E. Levite, 1-13. Washington, DC: Georgetown University Press, 2017. https://carnegieendowment.org/2017/10/16/introduction-to-understanding-cyber-conflict-14-analogies-pub-73392.

[112] Cavelty, Myriam Dunn. "Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate." *Journal of Information Technology & Politics* 4, no. 1 (2008): 19-36.; Dunn Cavelty, Myriam. "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse." *International Studies Review* 15, no. 1 (2013): 105-122.

[113] Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford University Press, 2016.

[114] Slayton, Rebecca. "What is the cyber offense-defense balance? Conceptions, causes, and assessment." *International Security* 41, no. 3 (2017): 72-109.

[115] Libicki, Martin C. *Cyberdeterrence and cyberwar*. Rand Corporation, 2009; Stevens, Tim. "A cyberwar of ideas? Deterrence and norms in cyberspace." *Contemporary Security Policy* 33, no. 1 (2012): 148-170; Nye Jr, Joseph S. "Deterrence and dissuasion in cyberspace." *International Security* 41, no. 3 (2017): 44-71; Harknett, Richard J., and Joseph S. Nye Jr. "Is Deterrence Possible in Cyberspace?" *International Security* 42, no. 2 (2017): 196-199.

[116] Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence is not a credible strategy for cyberspace." *Orbis* 61, no. 3 (2017): 381-393; Lindsay, Jon R. "The impact of China on cybersecurity: Fiction and friction." *International Security* 39, no. 3 (2015): 7-47; Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press, USA, 2015; Inkster, Nigel. *China's Cyber Power*. Routledge, 2018; Anderson, Collin. "Dimming the Internet: Detecting throttling as a mechanism of censorship in Iran." *arXiv preprint arXiv:1306.4361* (2013); Anderson, Collin and Karim Sadjadpour. *Iran's Cyber Threat: Espionage, Sabotage, and Revenge.* Washington, DC: Carnegie Endowment for International Peace, 2018. https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134; Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul. "Cyber attacks against Georgia: Legal lessons identified." *Tallin, Estonia, November* (2008); Farwell, James P., and Rafal Rohozinski. "Stuxnet and the future of cyber war." *Survival* 53, no. 1 (2011): 23-40; Bronk, Christopher, and Eneken Tikk-Ringas. "The cyber attack on Saudi Aramco." *Survival* 55, no. 2 (2013): 81-96; Zetter, Kim. *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Broadway books, 2014; Sharp, Travis. "Theorizing cyber coercion: The 2014 North Korean operation against Sony." *Journal of Strategic Studies* 40, no. 7 (2017): 898-926.

[117] Clarke, Richard Alan and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It.* New York: HarperCollins, 2010; Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (October 2011): 5-32; Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (Fall 2013): 41-73; Lindsay, Jon. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (August 2013): 365-404; Brenner, Joel and Jon R. Lindsay. "Correspondence: Debating the Chinese Cyber Threat." *International Security* 40, no. 1 (August 2015): 191-195. http://hdl.handle.net/1721.1/100538.

[118] Sanger, David E. and Mark Mazzetti. "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict." *New York Times.* February 16, 2016. https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html; Field, Matthew. "WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled." *Telegraph.* October 11, 2018. https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

[119] Chesney, Robert. "Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility." *Lawfare* (blog). Brookings Institution. May 6, 2019. https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility.

[120] Zittrain, Jonathan L., John Gorham Palfrey, Ronald Deibert, Rafal Rohozinski, Nart Villeneuve, and Derek Bambauer. "Internet Filtering in China 2004-2005." (2005); Deibert, Ronald J. "The geopolitics of internet control: Censorship, sovereignty, and cyberspace." In *Routledge Handbook of Internet Politics*. Routledge, 2008: 339-352; Zittrain, Jonathan, and John Palfrey. "Internet filtering: The politics and mechanisms of control." *Access denied: The practice and policy of global Internet filtering* 41 (2008); Kalathil, Shanthi, and Taylor C. Boas. *Open networks, closed regimes: The impact of the Internet on authoritarian rule*. Carnegie Endowment, 2010.

[121]Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Electronic Frontiers Foundation. February 8, 1996. https://www.eff.org/cyberspace-independence; Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs, 2012.

[122] Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect your Data and Control your World*. WW Norton & Company, 2015; MacKinnon, Rebecca. *Consent of the Networked*. New York: Basic Books, 2013.

[123] Maurer, Tim, Edin Omanovic, and Ben Wagner. "Uncontrolled Global Surveillance." *New America Foundation, Digitale Gesellschaft, & Privacy International* (2014); Herr, Trey. "Malware counter-proliferation and the Wassenaar arrangement." In *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE, 2016: 175-190; Bohnenberger, Fabian. "The proliferation of cyber surveillance technologies: Challenges and prospects for strengthened export controls." *Strategic Trade Review* 4 (2017): 81-102.

[124] Swire, Peter, and Kenesa Ahmad. "Encryption and Globalization." *Columbia Science and Technology Law Review*23 (2012).

[125] Heumann, Stefan, and Ben Scott. "Law and policy in Internet surveillance programs: United States, Great Britain and Germany." *Impulse* 25, no. 13 (2013): 2; Landau, Susan. "Making sense from Snowden: What's significant in the NSA surveillance revelations." *IEEE Security & Privacy* 11, no. 4 (2013): 54-63; Deibert, Ron. "The geopolitics of cyberspace after Snowden." *Current History* 114, no. 768 (2015): 9; Clarke, Richard A., Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. *The NSA Report: Liberty and Security in a Changing World*. Princeton University Press, 2014.

[126] Abdenur, Adriana Erthal, and Carlos Frederico Pereira da Silva Gama. "Triggering the norms cascade: Brazil's initiatives for curbing electronic espionage." *Global Governance* (2015): 455-474; Buchan, Russell. "Cyber espionage and international law." In *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing, 2015; Libicki, Martin. "The coming of cyber espionage norms." In *2017 9th International Conference on Cyber Conflict (CyCon)*. IEEE, 2017: 1-17.

[127] Milanovic, Marko. *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy*. Oxford University Press, 2011.

[128] MacKinnon, Rebecca. "Liberation Technology: China's 'Networked Authoritarianism.'" *Journal of Democracy* 22, no. 2 (2011): 32-46; King, Gary, Jennifer Pan, and Margaret E. Roberts. "How censorship in China allows government criticism but silences collective expression." *American Political Science Review* 107, no. 2 (2013): 326-343; Inkster, Nigel. *China's Cyber Power*. Routledge, 2018; Soldatov, Andrei, and Irina Borogan. *The Red Web: The Struggle between Russia's Digital Dictators and the New Online revolutionaries*. Hachette UK, 2015.

[129] See, for example: Choucri, Nazli, Stuart Madnick, and Jeremy Ferwerda. "Institutions for cyber security: International responses and global imperatives." *Information Technology for Development* 20, no. 2 (2014): 96-121.

[130] For example, Herr, Trey. "PrEP: A Framework for Malware & Cyber Weapons." *Journal of Information Warfare* 13, no. 1 (2014): 87-106; Herr, Trey. "Malware counter-proliferation and the Wassenaar arrangement." In *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE, 2016: 175-190; Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37; Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford University Press, 2016; Smeets, Max. "A matter of time: On the

transitory nature of cyberweapons." *Journal of Strategic Studies* 41, no. 1-2 (2018): 6-32; Smeets, Max. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly* 12, no. 3 (2018): 90-113; Kostyuk, Nadiya. "International and domestic challenges to comprehensive national cybersecurity: A case study of the Czech Republic." *Journal of Strategic Security* 7, no. 1 (2014): 68-82; Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible digital front: Can cyber attacks shape battlefield events?" *Journal of Conflict Resolution* 63, no. 2 (2019): 317-347.

[131] Mueller, Milton, Karl Grindal, Brenden Kuerbis, and Farzaneh Badiei. "Cyber Attribution." *The Cyber Defense Review* 4, no. 1 (2019): 107-122; DeNardis, Laura. *The Internet in Everything*. New Haven, CT: Yale University Press, forthcoming; Lewis, James. "Internet Governance: Inevitable Transitions." Internet Governance paper series. Waterloo: Center for International Governance Innovation, 2013. https://www.cigionline.org/publications/internet-governance-inevitable-transitions.

[132] Nye, Joseph S. "The regime complex for managing global cyber activities." *Global Commission on Internet Governance* (2014).

[133] Kello, Lucas. "The meaning of the cyber revolution: Perils to theory and statecraft." *International Security* 38, no. 2 (2013): 7-40; Lindsay, Jon R. "The impact of China on cybersecurity: Fiction and friction." *International Security* 39, no. 3 (2015): 7-47; Brenner, Joel, and Jon R. Lindsay. "Correspondence: Debating the Chinese Cyber Threat." *International Security* 40, no. 1 (2015): 191-195; Raymond, Mark, and Laura DeNardis. "Multistakeholderism: anatomy of an inchoate global institution." *International Theory* 7, no. 3 (2015): 572-616; Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." *American Journal of International Law* 110, no. 3 (2016): 425-479; Nye Jr, Joseph S. "Deterrence and dissuasion in cyberspace." *International Security* 41, no. 3 (2017): 44-71; Slayton, Rebecca. "What is the cyber offense-defense balance? Conceptions, causes, and assessment." *International Security* 41, no. 3 (2017): 72-109; Singer, Peter W., and Allan Friedman. *Cybersecurity: What Everyone Needs to Know*. Oxford University Press USA, 2014; Cavelty, Myriam Dunn, and Camino Kavanagh. "Cybersecurity and human rights." In *Research Handbook on Human Rights and Digital Technology*. Edward Elgar Publishing, 2019.

[134] Rather than 'schools of thought,' Sil and Katzenstein call them "research traditions," see Sil, Rudra and Peter Katzenstein. "Analytic Eclecticism in the Study of World Politics: Reconfiguring Problems and Mechanisms across Research Traditions." *Perspectives on Politics* 8, no. 2 (June 2010): 413.

[135] Knock, Thomas J. *To End All Wars, New Edition: Woodrow Wilson and the Quest for a New World Order*. Princeton University Press, 2019; Nye, Joseph S., and Robert O. Keohane, eds. *Transnational Relations and World Politics*. Cambridge, MA: Harvard University Press, 1972; Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence: World Politics in Transition*. Boston: Little, Brown, 1977; Doyle, Michael W. *Ways of War and Peace Realism, Liberalism, and Socialism*. New York: WW Norton, 1997; Legro, Jeffrey W., and Andrew Moravcsik. "Is anybody still a realist?" *International Security* 24, no. 2 (1999): 5-55.

[136] Carr, E.H. *The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations.* London: Macmillan, 1939; Morgenthau, Hans J. *Politics Among Nations: The Struggle for Power and Peace*. New York: Knopf, 1948; Waltz, Kenneth N. *Theory of International Politics*. Reading, Mass.: Addison-Wesley, 1979; Mearsheimer, John J. *The Tragedy of Great Power Politics*. WW Norton & Company, 2001; Snyder, Jack, and Keir A. Lieber. "Defensive Realism

and the “New” History of World War I." *International Security* 33, no. 1 (2008): 174-194; Rose, Gideon. "Neoclassical realism and theories of foreign policy." *World Politics* 51, no. 1 (1998): 144-172.

[137] Wendt, Alexander. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999; Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change." *International Organization* 52, no. 4 (1998): 887-917; Finnemore, Martha, and Kathryn Sikkink. "Taking stock: the constructivist research program in international relations and comparative politics." *Annual Review of Political Science* 4, no. 1 (2001): 391-416; Adler, Emanuel. "Constructivism in international relations: sources, contributions, and debates." *Handbook of International Relations* 2 (2013): 112-144.

[138] Bessner and Guilhot in their in-depth analysis of Waltz’s scholarship argue it was not while (see Bessner, Daniel, and Nicolas Guilhot. "How realism Waltzed Off: liberalism and decisionmaking in Kenneth Waltz's neorealism." *International Security* 40, no. 2 (2015): 87-118.) while other scholars, for example, Narizny continue to claim that neorealism is based on microeconomic theory (see Narizny, Kevin. "On systemic paradigms and domestic politics: A critique of the newest realism." *International Security* 42, no. 2 (2017): 158.).

[139] Bessner, Daniel, and Nicolas Guilhot. "How realism Waltzed Off: liberalism and decisionmaking in Kenneth Waltz's neorealism." *International Security* 40, no. 2 (2015): 87.

[140] Bessner, Daniel, and Nicolas Guilhot. "How realism Waltzed Off: liberalism and decisionmaking in Kenneth Waltz's neorealism." *International Security* 40, no. 2 (2015): 87-88; 96

[141] Narizny, Kevin. "On systemic paradigms and domestic politics: A critique of the newest realism." *International Security* 42, no. 2 (2017): 155-156.

[142] Narizny, Kevin. "On systemic paradigms and domestic politics: A critique of the newest realism." *International Security* 42, no. 2 (2017): 188.

[143] Narizny, Kevin. "On systemic paradigms and domestic politics: A critique of the newest realism." *International Security* 42, no. 2 (2017): 181.

[144] See Parent, Joseph M., and Sebastian Rosato. "Balancing in neorealism." *International Security* 40, no. 2 (2015): page 59.

[145] Keohane, Robert Owen, and Lisa L. Martin. *Institutional Theory, Endogeneity and Delegation*. No. 99. Weatherhead Center for International Affairs, Harvard University, 1999: 3.

[146] Sil and Katzenstein suggest that “the battles among research traditions recur not because of hardened differences over substantive issues but over preexisting epistemic convictions about what kinds of social phenomena are amenable to social analysis, what kinds of questions are important to ask, and what kinds of processes and mechanisms are most likely to be relevant (Sil and Katzenstein: 413).” This argument is not surprising considering the sometimes direct and sometimes rather indirect references to scholars’ “beliefs” as a driving force for their scholarship. For example, Bessner and Gulihot write that “In essence, realists believed that liberalism was bad for U.S. foreign policy – just as it had been for the Weimar Republic and international relations throughout the 1930s (see Bessner, Daniel, and Nicolas Guilhot. "How realism Waltzed Off: liberalism and decisionmaking in Kenneth Waltz's neorealism." *International Security* 40, no. 2 (2015): 96).” And Narizny writes in the concluding remarks of his critique of neoclassical realism that “Of course, realists who believe that domestic politics is unimportant have no reason to change their minds (see Narizny, Kevin. "On systemic paradigms and domestic politics: A critique of the newest realism." *International Security* 42, no. 2 (2017): 190).” Importantly, this finding matters

because as Sil and Katzenstein further argue "Research traditions give themselves permission to bypass aspects of a complex reality that do not neatly fit within the metatheoretical parameters they have established by fiat. These aspects are either 'blackboxed,' relegated to 'context,' or treated as 'exogenous.' Such simplifying moves, while helpful for the purpose of generating elegant knowledge claims about particular aspects of reality, are not independently capable of generating a more comprehensive understanding of complex, multi-faceted problems that interest scholars and policymakers alike (Sil and Katzenstein: 413)."

[147] Sil, Rudra, and Peter J. Katzenstein. "Analytic eclecticism in the study of world politics: Reconfiguring problems and mechanisms across research traditions." *Perspectives on Politics* 8, no. 2 (2010): 415.

[148] Thucydides. *History of the Peloponnesian War*. Rex Warner (trans.) Harmondsworth: Penguin Books, 1972. Machiavelli, Niccolo. *The Prince.* Q. Skinner and R. Price (eds.) Cambridge: Cambridge University Press, 1988.

Weber, Max. *The Theory of Social and Economic Organization*. New York: Oxford University Press, 1947.

Arendt, Hannah. *The Human Condition*. Chicago: University of Chicago Press, 1998.

[149] Carr, Edward H. *The Twenty Years' Crisis 1919-1939*. New York: Harper Torchbooks, 1939: 132.

[150] Barnett, Michael and Raymond Duvall. "Power in International Politics". *International Organization* 59.1 (Winter 2005): 41.

[151] Barnett, Michael and Raymond Duvall. "Power in International Politics". *International Organization* 59.1 (Winter 2005): 39-75.

[152] Barnett, Michael and Raymond Duvall. "Power in International Politics". *International Organization* 59.1 (Winter 2005): 39.

[153] Barnett, Michael, and Raymond Duvall. "Power in international politics." *International Organization* 59, no. 1 (2005): 43.

[154] Nye Jr, Joseph S. "Cyberpower". Cambridge, Mass.: Harvard Belfer Center for Science and International Affairs, May 2010: 4 citing Kuehl.

[155] Nye Jr, Joseph S. *The Future of Power*. New York: Public Affairs, 2011: xv + 113.

[156] Huntington, Samuel. "Culture, Power, and Democracy." In *Globalization, Power, and Democracy,* edited by Marc Plattner and Aleksander Smolar, 3-13. Baltimore: Johns Hopkins University Press, 2000.

[157] Bremmer, Ian. "Every Nation for Itself: Winners and Losers in a G-zero World." *New York* (2012).

[158] Haass, Richard N. "The age of nonpolarity: what will follow US dominance." *Foreign Affairs* (2008): 44-56.

[159] Zakaria, Fareed. "The post-American world." New York: WW Norton & Company, 2008.

[160] Huntington, Samuel. The Clash of Civilizations and the Remaking of World Order. London: Penguin Books, 1997.

[161] Taylor, Adam. "The worst justification for Trump's battle with China? The 'clash of civilizations.'" WorldViews. *Washington Post.* May 2, 2019. https://www.washingtonpost.com/world/2019/05/02/worst-justification-trumps-battle-with-china-clash-civilizations/.

[162] Brimelow, Ben. "These are the 20 aircraft carriers in service today." *Business Insider.* April 8, 2018. https://www.businessinsider.com/aircraft-carriers-list-in-service-patrolling-the-world-2018-2#hms-queen-elizabeth-is-the-newest-aircraft-carrier-of-the-royal-navy-and-currently-the-only-active-one-as-well-1;
Tian, Nan, Aude Fleurant, Alexandra Kuimova, Pieter D. Wezeman, and Siemon T. Wezeman. *SIPRI Yearbook 2019.* Solna: Stockholm International Peace Research Institute, 2019. https://www.sipri.org/yearbook/2019/04.
[163] "Military spending around the world is booming." *Economist*. April 28, 2019. https://www.economist.com/international/2019/04/28/military-spending-around-the-world-is-booming.
[164] International Monetary Fund. "G20 Agreement on Quotas and Governance." Last modified July 28, 2017. https://www.imf.org/external/np/exr/faq/quotasgov.htm.
[165] Nye Jr, Joseph S. *The Future of Power*. New York: Public Affairs, 2011: 132.
[166] U.S. Department of Justice. "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector." Press release no. 16-348. March 24, 2016. https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged; U.S. Department of Justice. "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts." Press release no. 17-278. March 15, 2017. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.
[167] Goldsmith, Jack and Timothy Wu. *Who Controls the Internet?*, 23; Reagle, Joseph. *Why the Internet Is Good*, Berkman Center Working Draft, Cambridge, MA: Harvard Law School, 1999.
[168] Nye Jr, Joseph S. "Cyberpower". Cambridge, Mass.: Harvard Belfer Center for Science and International Affairs, May 2010, 1.
[169] Choucri, Nazli and Robert J. Reardon. "Cyberspace in International Relations: A View of the Literature." 2011: 14–15.
[170] Choucri, Nazli and Robert J. Reardon. "Cyberspace in International Relations: A View of the Literature." 2011: 15.
[171] Deibert, Ronald J. and Masashi Crete-Nishihata. "Global Governance and the Spread of Cyberspace Controls." *Global Governance* 18, no. 3 (2012): 339.
[172] Choucri, Nazli and Robert J. Reardon. "Cyberspace in International Relations: A View of the Literature." 2011: 15.
[173] Drezner, Daniel. "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly* (2004): 478. For another argument against the decline of state authority over cyberspace, see Henry Farrell. "Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement." *International Organization* 57, no. 02 (2003): 277–306.
[174] Choucri, Nazli and David Clark. *Cyberspace and International Relations. Toward an Integrated System*. 2011: 22. http://ecir.mit.edu/images/stories/Salience%20of%20Cyberspace%208-25.pdf; Dunn Cavelty, Myriam. *The Militarisation of Cyber Security as a Source of Global Tension.* Zurich: Center for Security Studies, October 2012. http://www.isn.ethz.ch/isn/Digital-Library/Special-Feature/Detail?lng=en&id=153888&contextid774=153888&contextid775=153887&tabid=1453349960.

[175] O'Neil, Jim. "Building Better Global Economic BRICs." *Goldman Sachs - Global Economics Paper* 66 (2001); Armijo, Leslie Elliott. "The BRICs countries (Brazil, Russia, India, and China) as analytical category: mirage or insight?" *Asian Perspective* (2007): 7-42; Stuenkel, Oliver. "The financial crisis, contested legitimacy, and the genesis of intra-BRICS cooperation." *Global Governance* (2013): 611-630; Stuenkel, Oliver. *The BRICS and the Future of Global Order*. Lexington Books, 2015; Goddard, Stacie E. "Embedded revisionism: Networks, institutions, and challenges to world order." *International Organization* 72, no. 4 (2018): 767.

[176] Narizny, Kevin. "On systemic paradigms and domestic politics: A critique of the newest realism." *International Security* 42, no. 2 (2017): 188.

[177] U.S. Department of Justice. "ISIL-Linked Hacker Arrested in Malaysia on U.S. Charges." Press release no. 15-1280. October 15, 2015. www.justice.gov/opa/pr/isil-linked-hacker-arrested-malaysia-us-charges; Coker, Margaret, Danny Yadron, and Damian Paletta. "Hacker Killed by Drone Was Islamic State's 'Secret Weapon.'" *Wall Street Journal*. August 27, 2015. www.wsj.com/articles/hacker-killed-by-drone-was-secret-weapon-1440718560; Franceschi-Bicchierai, Lorenzo. "How a Teenage Hacker Became the Target of a US Drone Strike." Motherboard. *Vice*. August 28, 2015. http://motherboard.vice.com/read/junaid-hussain-isis-hacker-drone.

[178] Thomson, Janice E. *Mercenaries, Pirates, and Sovereigns: State-building and Extraterritorial Violence in Early Modern Europe*. Vol. 63. Princeton University Press, 1996; Stark, Francis Raymond. *The Abolition of Privateering and the Declaration of Paris*. Vol. 8, no. 3. Columbia University, 1897.

[179] Zarate, Juan Carlos. "The emergence of a new dog of war: Private international security companies, international law, and the new world disorder." *Stan. J. Int'l L.* 34 (1998): 75; Singer, Peter W. "Corporate Warriors: The Rise of the Privatized Military Industry and its ramifications for International Security." *International Security* 26, no. 3 (2002): 186-220; Percy, Sarah. *Mercenaries: The History of a Norm in International Relations*. Oxford University Press, 2007.

[180] Avant, Deborah D. *The Market for Force: The Consequences of Privatizing Security*. Cambridge University Press, 2005.

[181] Zimmermann, Lisbeth, Nicole Deitelhoff, and Max Lesch. "Unlocking the agency of the governed: contestation and norm dynamics." *Third World Thematics: A TWQ Journal* 2, no. 5 (2017): 691-708; Wiener, Antje. "Agency of the governed in global international relations: access to norm validation." *Third World Thematics: A TWQ Journal* 2, no. 5 (2017): 709-725; For an excellent summary of the scholarship on norm contestation, see also Lantis, Jeffrey S. "Theories of International Norm Contestation: Structure and Outcomes." In *Oxford Research Encyclopedia of Politics*. 2017.

[182] Waltz, Kenneth N. *Theory of International Politics*. Reading, Mass.: Addison-Wesley, 1979; Pape, Robert A. "Soft balancing against the United States." *International Security* 30, no. 1 (2005): 7-45.

[183] Noss, Eliott. "A battle for the soul of the Internet." CNET News. June 8, 2005. http://news.cnet.com/A%20battle%20for%20the%20soul%20of%20the%20Internet/2010-1071_3-5737647.html.

[184] Checkel, Jeffrey T. "Tracing causal mechanisms." *International Studies Review* 8, no. 2 (2006): 362-370; Checkel, Jeffrey T. "Process tracing." In *Qualitative Methods in International Relations*. Palgrave Macmillan, London, 2008: 114-127.
[185] Friedberg, Aaron L. *A Contest for Supremacy: China, America, and the Struggle for Mastery in Asia*. WW Norton & Company, 2011; Ikenberry, G. John. "The Future of the Liberal World Order: Internationalism after America." *Foreign Affairs* (2011): 56-68; Mearsheimer, John J. "Can China rise peacefully?" *The National Interest* 25 (2014): 23-37.
[186] Goddard, Stacie E. "Embedded revisionism: Networks, institutions, and challenges to world order." *International Organization* 72, no. 4 (2018): 763.
[187] Abbott, Kenneth W., Jessica F. Green, and Robert O. Keohane. "Organizational ecology and institutional change in global governance." *International Organization* 70, no. 2 (2016): 247-277.
[188] Abbott, Kenneth W., Jessica F. Green, and Robert O. Keohane. "Organizational ecology and institutional change in global governance." *International Organization* 70, no. 2 (2016): 247-277.
[189] Kleinwächter, Wolfgang. "Sharing Decision Making in Internet Governance: The Impact of the WGIG Definition." In *The Working Group on Internet Governance: 10th Anniversary Reflections*, edited by William J. Drake, 66-88. Johannesburg: Association for Progressive Communication, 2015: 87. http://www.mediachange.ch/media/pdf/publications/IG_10_Final.pdf
[190] Clarke, Richard Alan and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It.* New York: HarperCollins, 2010; Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (October 2011): 5-32; Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (Fall 2013): 41-73.
[191] Brandon Valeriano and Ryan Maness make a similar critique in their book (despite the significant challenges with respect to data collection and analysis making a robust quantitative assessment difficult), see: Valeriano, Brandon and Ryan C. Maness. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press, 2015.
[192] See, for example: Byman, Daniel. "Passive sponsors of terrorism." *Survival* 47, no. 4 (2005): 117-144; Schmitt, Michael N. "In defense of due diligence in cyberspace." *Yale LJF* 125 (2015): 68.
[193] Thomson, Janice E. *Mercenaries, Pirates, and Sovereigns: State-building and Extraterritorial Violence in Early Modern Europe*. Vol. 63. Princeton University Press, 1996; Avant, Deborah D. *The Market for Force: The Consequences of Privatizing Security*. Cambridge University Press, 2005; Singer, Peter Warren. *Corporate Warriors: The Rise of the Privatized Military Industry*. Cornell University Press, 2008; Branović, Željko, and Sven Chojnacki. "The logic of security markets: Security governance in failed states." *Security Dialogue* 42, no. 6 (2011): 553-569; Chojnacki, Sven, Nils Metternich, and Johannes Münster. "Mercenaries in civil wars, 1950-2000." WZB Discussion Paper SP II 2009 – 05 (2009): 42; Harris, Shane. *@War: The Rise of the Military-internet Complex*. Houghton Mifflin Harcourt, 2014; Percy, Sarah. *Mercenaries: The History of a Norm in International Relations*. Oxford University Press, 2007; Stark, Francis Raymond. *The Abolition of Privateering and the Declaration of Paris*. Vol. 8, no. 3. Columbia University, 1897; Egloff, Florian. "Cybersecurity and the Age of Privateering." *Understanding Cyber Conflict: Fourteen Analogies. Georgetown University Press: Washington, DC* (2017): 231-247.
[194] Byman, Daniel. "Passive sponsors of terrorism." *Survival* 47, no. 4 (2005): 117-144.

[195] United Nations. United Nations Group of Governmental Experts. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." UN Doc A/68/98. June 24, 2013. https://digitallibrary.un.org/record/753055.
[196] Abbott, Kenneth W., Philipp Genschel, Duncan Snidal, and Bernhard Zangl, eds. *International Organizations as Orchestrators*. Cambridge University Press, 2015.
[197] Florian Eggloff uses a similar concept of "state proximity" in his insightful scholarship focused on historical analogies. See Egloff, Florian. "Cybersecurity and the Age of Privateering." *Understanding Cyber Conflict: Fourteen Analogies. Georgetown University Press: Washington, DC* (2017): 231-247.
[198] See for example the following important works discussing international law with respect to cyberspace: Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013; Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017; Tsagourias, Nicholas, and Russell Buchan, eds. *Research Handbook on International Law and Cyberspace*. Cheltenham: Edward Elgar Publishing, 2015.
[199] Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." *American Journal of International Law* 110, no. 3 (2016): 425-479.
[200] Zimmermann, Lisbeth, Nicole Deitelhoff, and Max Lesch. "Unlocking the agency of the governed: contestation and norm dynamics." *Third World Thematics: A TWQ Journal* 2, no. 5 (2017): 691-708.
[201] Wiener, Antje. "Agency of the governed in global international relations: access to norm validation." *Third World Thematics: A TWQ Journal* 2, no. 5 (2017): 709-725.
[202] Hall and Taylor have already pointed out, the two are not mutually exclusive, see Hall, Peter A., and Rosemary CR Taylor. "Political science and the three new institutionalisms." *Political Studies* 44, no. 5 (1996): 936-957.
[203] March, James G., and Johan P. Olsen. "The institutional dynamics of international political orders." *International Organization* 52, no. 4 (1998): 951.
[204] Finnemore, Martha, and Kathryn Sikkink. "International norm dynamics and political change." *International Organization* 52, no. 4 (1998): 887-917.
[205] Nakashima, Ellen and Adam Goldman. "In a first, Chinese hackers are arrested at the behest of the U.S. government." *Washington Post.* October 9, 2015. https://www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html.
[206] Noble, Zach. "Report: China has arrested alleged OPM hackers." FCW. December 2, 2015. https://fcw.com/articles/2015/12/02/china-cyber-opm-arrest.aspx.
[207] Hosenball, Mark and Patricia Zengerle. Reuters. "The US isn't going to publicly blame China for the catastrophic hack of the federal government's personnel records." *Business Insider.* July 22, 2015. https://www.businessinsider.com/r-us-unlikely-to-blame-china-publicly-over-opm-data-breach-officials-2015-7.
[208] Segal, Adam and Alex Grigsby. "CFR Cyber Operations Tracker." Council on Foreign Relations. Accessed August 27, 2019. https://www.cfr.org/interactive/cyber-operations; Lewis, James Andrew. "Significant cyber incidents since 2006." Center for Strategic and International

Studies. Accessed August 27, 2019. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents; Valeriano, Brandon, and Ryan C. Maness. "The dynamics of cyber conflict between rival antagonists, 2001–11." *Journal of Peace Research* 51, no. 3 (2014): 347-360; Whyte, Christopher, Brandon Valeriano, Benjamin Jensen, and Ryan Maness. "Rethinking the data wheel: Automating open-access, public data on cyber conflict." In *2018 10th International Conference on Cyber Conflict (CyCon)*. IEEE, 2018: 9-30; Valeriano, Brandon and Ryan Maness. "Coding Cyber Security Incident Data." *RelationsInternational* (blog). November 8, 2017. http://relationsinternational.com/coding-cyber-security-incident-data/.

[209] Egloff, Florian. "New Players Join Race for Offensive Cyber Abilities." Daily Brief. Oxford Analytica. August 20, 2018. https://css.ethz.ch/publikationen/suche-und-bestellung/details.html?id=n/e/w/p/new_players_join_race_for_offensive_cybe.

[210] Perlroth, Nicole and Quentin Hardy. "Bank Hacking Was the Work of Iranians, Officials Say." *New York Times*. January 8, 2013. https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html; Fisher, Max. "South Korea under cyber attack: Is North Korea secretly awesome at hacking?" WorldViews. *Washington Post.* March 20, 2013. https://www.washingtonpost.com/news/worldviews/wp/2013/03/20/south-korea-under-cyber-attack-is-north-korea-secretly-awesome-at-hacking/.

[211] U.S. Office of the Director of National Intelligence, U.S. Department of Defense, U.S. National Security Agency. *Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States*, by James R. Clapper, Marcel Lettre, and Michael S. Rogers. Washington, DC, 2017. https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

[212] Gerring, John. "The Case Study: What it is and What It Does." In *The Oxford Handbook of Comparative Politics*, edited by Carles Boix and Susan C. Stokes. New York: Oxford University Press, 2009: 10, 26.

[213] Gerring, John. "The Case Study: What it is and What It Does." In *The Oxford Handbook of Comparative Politics*, edited by Carles Boix and Susan C. Stokes. New York: Oxford University Press, 2009: 26.

[214] Gerring, John. "The Case Study: What it is and What It Does." In *The Oxford Handbook of Comparative Politics*, edited by Carles Boix and Susan C. Stokes. New York: Oxford University Press, 2009: 10.

[215] Levy, Jack S. "Case Studies: Types, Designs, and Logics of Inference." *Conflict Management and Peace Science* 25 (2008): 6.

[216] Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 25.

[217] Sil, Rudra, and Peter J. Katzenstein. "Analytic eclecticism in the study of world politics: Reconfiguring problems and mechanisms across research traditions." *Perspectives on Politics* 8, no. 2 (2010): 415.

[218] Sil, Rudra, and Peter J. Katzenstein. "Analytic eclecticism in the study of world politics: Reconfiguring problems and mechanisms across research traditions." *Perspectives on Politics* 8, no. 2 (2010): 411.

[219] Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Electronic Frontiers Foundation. February 8, 1996. https://www.eff.org/cyberspace-independence.

[220] Parent, Joseph M., and Sebastian Rosato. "Balancing in neorealism." *International Security* 40, no. 2 (2015): 54-55.
[221] Goldsmith, Jack and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press, 2006.
[222] Spencer, Keith. "How the 'Great Firewall' extends beyond China." *Salon*. March 25, 2019. https://www.salon.com/2019/03/25/how-chinas-internet-censorship-system-is-leaking-into-the-rest-of-the-world/.
[223] VandeHei, Jim and Mike Allen. "The great global decoupling." *Axios.* August 13, 2019. https://www.axios.com/china-united-states-relations-new-cold-war-7be11ae3-a62f-4b0e-89fc-e75beb18903b.html.
[224] Nye Jr, Joseph S. *The Future of Power*. New York: Public Affairs, 2011: 132.
[225] Parent, Joseph M., and Sebastian Rosato. "Balancing in neorealism." *International Security* 40, no. 2 (2015): 54-55.
[226] Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 51.
[227] Keller, Jared. "Evaluating Iran's Twitter Revolution." *The Atlantic.* June 18, 2010. https://www.theatlantic.com/technology/archive/2010/06/evaluating-irans-twitter-revolution/58337/.
[228] Vargas, Jose Antonio. "Spring Awakening." Sunday Book Review. *New York Times.* February 17, 2012. https://www.nytimes.com/2012/02/19/books/review/how-an-egyptian-revolution-began-on-facebook.html.
[229] Buzan, Barry, Ole Wæver, Ole Wæver, and Jaap De Wilde. *Security: A New Framework for Analysis*. Lynne Rienner Publishers, 1998.
[230] Cavelty, Myriam Dunn. *Cyber-security and Threat Politics: US Efforts to Secure the Information Age*. Routledge, 2008; Dunn Cavelty, Myriam. "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse." *International Studies Review* 15, no. 1 (2013): 105-122.
[231] *ISO/IEC 27000:2018 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary.* Definition 3.28: "information security." (Geneva: International Organization for Standardization, approved February 2018). https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.
[232] Maurer, Tim, and Robert Morgus. "'Cybersecurity'and Why Definitions Are Risky." *ISN Blog* (2014).
[233] General Assembly Resolution 54/49. *Developments in the field of information and telecommunications in the context of international security.* A/RES/54/49. December 23, 1999. https://undocs.org/en/A/RES/54/49.
[234] For a more detailed discussion of 'illiberal norms,' see Jose, Betcy. *Norm Contestation: Insights into Non-conformity with Armed Conflict Norms*. Springer, 2017: 14.
[235] Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." *American Journal of International Law* 110, no. 3 (2016): 428.
[236] For an in-depth discussion of the implications of lacking intersubjective agreements and norm ambiguity,' see Jose, Betcy. *Norm Contestation: Insights into Non-conformity with Armed Conflict Norms*. Springer, 2017: 5.

[237] EastWest Institute. “Ilya Rogachev.” EastWest Institute 2015 Global Cyberspace Cooperation Summit. Accessed August 27, 2019. www.cybersummit.info/2015/speakers/rogachev/.
[238] For a more detailed analysis, see McKune, Sarah. “An Analysis of the International Code of Conduct for Information Security.” Citizen Lab. Munk School of Global Affairs. Accessed August 26, 2019. https://openeffect.ca/code-conduct/.
[239] For a more detailed analysis, see Maurer, Tim, and Robert Morgus. "‘Cybersecurity’ and Why Definitions Are Risky." *ISN Blog* (2014).
[240] International Telecommunication Union. “World Conference on International Telecommunications.” Accessed August 27, 2019. https://www.itu.int/en/wcit-12/Pages/default.aspx.
[241] Campbell, Kurt and Jake Sullivan. “Competition Without Catastrophe.” *Foreign Affairs*. September/October 2019. https://www.foreignaffairs.com/articles/china/competition-with-china-without-catastrophe.
[242] Ikenberry, G. John. "The future of the liberal world order: internationalism after America." *Foreign Affairs* (2011): 56-68.
[243] Mueller III, Robert S. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)." (2019).
[244] Goddard, Stacie E. "Embedded revisionism: Networks, institutions, and challenges to world order." *International Organization* 72, no. 4 (2018): 793.
[245] Goddard, Stacie E. "Embedded revisionism: Networks, institutions, and challenges to world order." *International Organization* 72, no. 4 (2018): 763.
[246] See also Friedberg, Aaron L. *A Contest for Supremacy: China, America, and the Struggle for Mastery in Asia*. WW Norton & Company, 2011; Ikenberry, G. John. "The future of the liberal world order: internationalism after America." *Foreign Affairs* (2011): 56-68; Mearsheimer, John J. "Can China rise peacefully?" *The National Interest* 25 (2014): 23-37.
[247] Goddard, Stacie E. "Embedded revisionism: Networks, institutions, and challenges to world order." *International Organization* 72, no. 4 (2018): 764.
[248] Parent, Joseph M., and Sebastian Rosato. "Balancing in neorealism." *International Security* 40, no. 2 (2015): 85.
[249] Parent, Joseph M., and Sebastian Rosato. "Balancing in neorealism." *International Security* 40, no. 2 (2015): 85.
[250] U.S. Office of the Director of National Intelligence, U.S. Department of Defense, U.S. National Security Agency. *Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States*, by James R. Clapper, Marcel Lettre, and Michael S. Rogers. Washington, DC, 2017. https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.
[251] See Maurer, Tim. *Cyber Mercenaries – The State, Hackers, and Power*. Cambridge University Press, 2018: 80.
[252] Witlin. Lauren. "Of Note: Mirror-Imaging and Its Dangers." SAIS Review of International Affairs 28, no. 1 (2008): 89.
[253] Hafner-Burton, Emilie M., Stephan Haggard, David A. Lake, and David G. Victor. "The behavioral revolution and international relations." *International Organization* 71, no. S1 (2017): S4.

[254] Hafner-Burton, Emilie M., Stephan Haggard, David A. Lake, and David G. Victor. "The behavioral revolution and international relations." *International Organization* 71, no. S1 (2017): S14.
[255] Thomas, Daniel C. *The Helsinki Effect: International Norms, Human Rights, and the Demise of Communism*. Princeton University Press, 2001; Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." *American Journal of International Law* 110, no. 3 (2016): 443.
[256] Smith, Raymond A. "On their 40th Anniversary, the Helsinki Accords retain a powerful legacy." *Rightsview* (blog). Institute for the Study of Human Rights. Columbia University. July 28, 2015. https://blogs.cuit.columbia.edu/rightsviews/2015/07/28/1713/.
[257] Börzel, Tanja A., and Thomas Risse. "Governance without a state: Can it work?" *Regulation & Governance* 4, no. 2 (2010): 113-134.
[258] Abbott, Kenneth W., Jessica F. Green, and Robert O. Keohane. "Organizational ecology and institutional change in global governance." *International Organization* 70, no. 2 (2016): 263.
[259] Huawei. "Huawei Joins Paris Call for Trust, Security in Cyberspace." August 1, 2019. https://www.huawei.com/ke/press-events/news/2019/7/huawei-joins-paris-call.
[260] Abbott, Kenneth W., Jessica F. Green, and Robert O. Keohane. "Organizational ecology and institutional change in global governance." *International Organization* 70, no. 2 (2016): 272.
[261] Cooper, Ramesh Chandra Thakur Andrew Fenton, and John English. *International Commissions and the Power of Ideas*. United Nations University Press, 2005.
[262] United Nations. World Commission on Environment and Development. "Report of the World Commission on Environment and Development: Our Common Future." New York: Oxford University Press, 1987. https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf.
[263] Human Rights Watch. "Killer Robots." Accessed August 26, 2019. https://www.hrw.org/topic/arms/killer-robots.
[264] Charlet, Kate. "The New Killer Pathogens: Countering the Coming Bioweapons Threat." *Foreign Affairs* 97 (2018): 178.
[265] Linos, Katerina and Tom Pegram. "The Language of Compromise in International Agreements." *International Organization* 70, no. 3 (June 2016): 587-621.
[266] Carnegie, Allison, and Austin Carson. "The Spotlight's Harsh Glare: Rethinking Publicity and International Order." *International Organization* 72, no. 3 (2018): 627-657.
[267] Nye Jr, Joseph S. "Deterrence and dissuasion in cyberspace." *International Security* 41, no. 3 (2017): 44-71; Lindsay, Jon R. "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack." *Journal of Cybersecurity* 1, no. 1 (September 2015): 53-67.
[268] Fischerkeller, Michael P., and Richard J. Harknett. "Deterrence is not a credible strategy for cyberspace." *Orbis* 61, no. 3 (2017): 381-393.
[269] U.S. Department of State. International Security Advisory Board. *ISAB Report on a Framework for International Cyber Stability.* Washington, DC, 2014. Accessed January 6, 2017. https://www.state.gov/t/avc/isab/229023.htm (site discontinued).
[270] Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38, no. 2 (2013): 7-40.

[271] Nye Jr, Joseph S. *Cyber Power*. Harvard University – Belfer Center for Science and International Affairs, 2010; Klimburg, Alexander. "Mobilising Cyber Power." *Survival* 53, no. 1 (2011): 41-60.
[272] Finnemore, Martha, and Duncan B. Hollis. "Constructing norms for global cybersecurity." *American Journal of International Law* 110, no. 3 (2016): 425-479.
[273] Adams, Michael J. and Megan Reiss. "International Law and Cyberspace: Evolving Views." *Lawfare* (blog). Brookings Institution. March 4, 2018. https://www.lawfareblog.com/international-law-and-cyberspace-evolving-views.
[274] Kanuck, Sean. "Sovereign discourse on cyber conflict under international law." *Tex. L. REv.* 88 (2009): 1571.
[275] Krasner, Stephen D. *Sovereignty: Organized Hypocrisy*. Princeton University Press, 1999; Philpott, Daniel. *Revolutions in Sovereignty: How Ideas Shaped Modern International Relations*. Princeton University Press, 2001.
[276] Demchak, Chris C. and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32-61. https://www.jstor.org/stable/26270509.
[277] Swire, Peter and Kenesa Ahmad. "'Going Dark' Versus a 'Golden Age for Surveillance.'" Center for Democracy and Technology. Accessed January 23, 2012. http://www.cdt.org/blogs/2811going-dark-versus-golden-age-surveillance (site discontinued); Coleman, Michael. "Ex-CIA, NSA Chief Defends U.S. Intelligence Gathering." *The Washington Diplomat*. August 28, 2013. https://washdiplomat.com/index.php?option=com_content&view=article&id=9543&Itemid=414; Morell, Michael. "The Importance of Intelligence." *Real Clear Defense.* August 31, 2016. https://www.realcleardefense.com/articles/2016/08/31/the_importance_of_intelligence_109776.html.
[278] Rozen, Laura. "The golden age of intelligence is before us." *Salon.* September 21, 2001. https://www.salon.com/2001/09/21/kaplan_4/.
[279] Ramsay, Kristopher. "Information, Uncertainty, and War." *Annual Review of Political Science* 20 (2017): 505-527.
[280] Parent, Joseph M., and Sebastian Rosato. "Balancing in neorealism." *International Security* 40, no. 2 (2015): 52.

Recommended Reading Order:

1. Core Article #1:
   - Ebert, Hannes and Tim Maurer. "Contested cyberspace and rising powers." *Third World Quarterly* 34, no. 6 (2013): 1054-1074. https://doi.org/10.1080/01436597.2013.802502.

2. Core Article #2:
   - Maurer, Tim. "'Proxies' and Cyberspace." *Journal of Conflict and Security Law* 21, no. 3 (2016): 383-403. https://doi.org/10.1093/jcsl/krw015.

3. Supplementary Material #1 – Monograph:
   - Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press, 2018. https://doi.org/10.1017/9781316422724.

4. Core Article #3:
   - Maurer, Tim. "A Dose of Realism: The Contestation and Politics of Cyber Norms." *Hague Journal on the Rule of Law* (2019). https://doi.org/10.1007/s40803-019-00129-8.

Background material:

Supplementary Material #2 – Annotated Literature Review:

- Ebert, Hannes and Tim Maurer. "International Relations - Cyber Security." *Oxford Bibliographies - Oxford University Press.* Last modified January 11, 2017. https://doi.org/10.1093/OBO/9780199743292-0196.

APPENDIX I – CORE ARTICLE #1

Ebert, Hannes and Tim Maurer. "Contested cyberspace and rising powers." *Third World Quarterly* 34, no. 6 (2013): 1054-1074. https://doi.org/10.1080/01436597.2013.802502.

APPENDIX II – CORE ARTICLE #2

Maurer, Tim. "'Proxies' and Cyberspace." *Journal of Conflict and Security Law* 21, no. 3 (2016): 383-403. https://doi.org/10.1093/jcsl/krw015.

APPENDIX III – CORE ARTICLE #3

Maurer, Tim. "A Dose of Realism: The Contestation and Politics of Cyber Norms." *Hague Journal on the Rule of Law* (2019). https://doi.org/10.1007/s40803-019-00129-8.

Cyberspace and International Relations: Rising Powers, Proxies, and Norms

Dissertation

zur Erlangung des Grades eines Doktors
Dr. rer. pol. in Politikwissenschaft
am Fachbereich "Politik- und Sozialwissenschaften"
der Freien Universität Berlin

gemäß der Promotionsordnung zum Dr. rer. pol.
vom 23. April 2008 in Verbindung mit der Ersten Ordnung
zur Änderung dieser Promotionsordnung vom 26. Juni 2012

vorgelegt von
Tim Maurer

Berlin 2019

Teil 2 von 2: **Supplementary Material**

APPENDIX IV – SUPPLEMENTARY MATERIAL #1 – MONOGRAPH

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press, 2018. https://doi.org/10.1017/9781316422724.

APPENDIX V – SUPPLEMENTARY MATERIAL #2 – ANNOTATED LITERATURE REVIEW

Ebert, Hannes and Tim Maurer. "International Relations - Cyber Security." *Oxford Bibliographies - Oxford University Press*. Last modified January 11, 2017. http://doi.org/10.1093/OBO/9780199743292-0196.

(The print version of the dissertation ends on page 453. The Oxford Bibliographies website entry "International Relations – Cyber Security" is 33 pages long when printed.)