CYBERATTACKS
IN
INTERNATIONAL RELATIONS

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY IN INTERNATIONAL RELATIONS
IN THE DEPARTMENT OF POLITICS AND
INTERNATIONAL RELATIONS
AT THE UNIVERSITY OF OXFORD

81,627 WORDS

BY

R. DAVID EDELMAN

UNIVERSITY COLLEGE

OXFORD, UNITED KINGDOM

MICHAELMAS TERM 2013

The opinions contained in this work are solely those of the author — not of any international organization, government, or department/agency thereof.

CYBERATTACKS IN INTERNATIONAL RELATIONS
R. David Edelman, University College

Abstract of the thesis submitted for the degree of D.Phil.
in International Relations, Michaelmas 2013

New methods of conflict and coercion can prompt tectonic shifts in the international system, reconfiguring power, institutions, and norms of state behavior. Cyberattacks, coercive acts that disrupt or destroy the digital infrastructure on which states increasingly rely, have the potential to be such a tool — but only if put into practice. This study examines which forces in the international system might restrain state use of cyberattacks, even when they are militarily advantageous. To do so I place this novel technology in the context of existing international regimes, employing an analogical approach that identifies the salient aspects of cyberattacks, and compares them to prior weapons and tactics that share those attributes. Specifically, this study considers three possible restraints on state behavior: rationalist deterrence, the *jus ad bellum* regime governing the resort to force, and incompatibility with the *jus in bello* canon of law defining just conduct in war. First, I demonstrate that cyberattacks frustrate conventional deterrence models, and invite, instead, a novel form of proto-competition I call 'structural deterrence.' Recognizing that states have not yet grounded their sweeping claims about the acceptability of cyberattacks in any formal analysis, I consider evidence from other prohibited uses of force or types of weaponry to defining whether cyberattacks are 'legal' in peacetime or 'usable' in wartime. Whereas previous studies of cyberattacks have focused primarily on policy guidance for a single state or limited analysis of the letter of international law, this study explicitly relates international law to state decision-making and precedent. It draws together previously disparate literature across strategic studies, international law, and diplomatic history to offer conclusions applicable beyond any single technology, and of increasing importance as states' dependence on technology grows.

ACKNOWLEDGMENTS

There are many to whom I owe gratitude in the preparation of this work. First and foremost my advisor, Dr. Sarah Percy, who, despite major transitions, was an inspired navigator, counsel, and motivator over my years of doctoral study. I am particularly appreciative for her continued supervision — a responsibility she was under no obligation to retain — even after departing Oxford. That generosity kept both the momentum and rigor of this project, especially in its final year.

In Oxford, my co-advisor Professor Yuen Foong Khong provided invaluable wisdom, particularly in the concluding months of writing. I am grateful to Professor Rosemary Foot, my supervisor for the M.Phil., whose recommendation that I pursue only the most interesting questions set my course in the M.Phil., the D.Phil., and my career. Professor Jennifer Welsh and Dapo Akande provided incisive commentary during my confirmation process and helped orient the overall study and better narrow its focus. I am also exceptionally appreciative to the Department of Politics and International Relations, University College, and Oxford University Press for the generous Clarendon Scholarship that supported my doctoral study.

In America, the opportunity to serve with and learn from some of the most distinguished practitioners in the field of foreign policy contributed immeasurably to this work. At the State Department, John Merrill and Judith Strotz brought my early thinking and writing on this topic to new levels. Michele Markoff shared more history of the issue with me than any graduate student, let alone practitioner, could dream. At the White House, the late Eric Werner deserves credit as one of the most influential and unsung thinkers in the field; I was fortunate to hear his insights into norms in cyberspace, and his untimely death was a blow to a close-knit community

of practitioners. I am also grateful to Rob Knake, Danny Weitzner, Peter Lord, Sean Kanuck, and Andrew Scott for strengthening my arguments through months of spirited debate, and to Gene Sperling, Jason Furman, and Howard Schmidt for their longtime mentorship.

Finally, to the tireless supporters I am lucky enough to call family — Steve, Sharon, and Joanne — words fail in expressing my gratitude, and so, it is to you that I dedicate this work.

TABLE OF CONTENTS

Introduction

TABLE OF CONTENTS

New methods of conflict can usher in tectonic shifts in the international system, reconfiguring power, institutions, and norms of state behavior. Like the longbow, the warship, the bomber, and the ballistic missile, cyberattacks are a new innovation providing states with a novel way to coerce one another into changing behavior.

Cyberattacks are of increasing importance in international relations. A capability unheard of two decades ago has been thrust to the fore as its disruptive potential grows with every corporation, government service, public utility, and military capability that becomes dependent on computing. Given this increasing pervasiveness, it is perhaps natural that just as when humans mastered maritime navigation and flight, this new medium — the Internet, or cyberspace — is now a venue for competition and coercion between states.[1] It is presently unclear whether they will observe any restraint in using this new tool to gain strategic advantage. The sobering reality is that states are amassing immense capabilities to attack one another in cyberspace, yet cyberattacks have not come under any specific international regulation. It is even unclear whether and which general forces of the international system would be strongest in restraining their use.

Those forces of restraint, and whether they might meaningfully change state interest in using cyberattacks, are the subjects of this study. The question motivating the following chapters is whether any of the forces that have traditionally restrained the aggressive tendencies of threatened states can meaningfully apply to state use of cyberattacks. Sources of such restraint vary. In many instances, a rational calculation that potential losses outstrip gains can prevent a state from waging a certain attack. In others, international law serves as meaningful regulation, either because it forms a regime to punish derogation, or indirectly by assigning opprobrium that would complicate a state's relations with allies and peers. For similar reasons, a state might eschew a particular tactic — even if militarily advantageous — because they view it as 'unusable' or morally suspect. In security decisions large and small, these factors have important and differing degrees of influence on state choices.

[1] Hillary Rodham Clinton, *Remarks at the Launch of the U.S. International Strategy for Cyberspace* (Washington: The White House, 2011).

To date there have been numerous small-scale examples of computer network attacks, suggesting what a large cyberattack might look like. There is not, however, a clear expectation of how states would respond to such an event. It is uncertain whether a cyberattack so-defined could comply with humanitarian principles. And yet the race to develop the tools for those attacks continues, unabated, as does the likelihood they could cause damage that in previous decades would be recognizable only as the product of a shooting war. A study focusing not simply on the damage these weapons might cause, or the policies states should pursue to defend themselves, but on how existing forces of restraint might hold back cyberattacks from general use, is overdue. This study seeks to fill that gap.

1.1 Topic and Scope

This study explores interstate conflict involving cyberattacks, and specifically how current regimes, institutions, and customs of international relations might limit or shape it. Therefore this study seeks to answer the question:

> **Which if any forces in the international system might restrain state use of cyberattacks, even when they might be militarily advantageous?**

The answer has profound implications on two levels. First, it can help articulate the likely impact of cyberattacks on international security dynamics moving forward, as more countries become dependent on digital technologies. Second, it offers a critical referendum on these forces of restraint themselves — since, if those forces and regimes built around them are robust, they should apply with equal strength to new weapons as well as old.

These are questions increasingly central to the future of international security; in the words of the U.S. Homeland Security Advisor, “those of us who are involved with international, national, and homeland security policies as well as with the future of the global economy and human rights and freedom must pay attention to cyber issues and be actively engaged in cyber policy formulation."[2] Yet at the present time, states appear to be relying on generic deterrence statements as well as imperfect and often-contradictory understandings of applicable legal precedent in their defense planning vis-à-vis cyberattacks. This uneasy state seems similar to the period of cautiousness and doctrinal head-scratching that accompanied other advances in weaponry: from the strategic and tactical debates over the use of nuclear weapons, to the legal and normative debates accompanying the development of chemical weapons. Such parallels form both a context and historical basis for this analysis.

International peace and security are increasingly dependent on restraining cyberattacks; therefore, there is an urgency to determining which frameworks and regimes of international relations might influence states' decision not to use them. Ene Ergma, the Speaker of the Estonian Parliament and a nuclear physics expert, argued after his country came under a small-scale cyberattack, "[w]hen I look at a nuclear explosion and the explosion that happened in our country, I see the same thing…like nuclear radiation, cyberwar doesn't make you bleed, but it can destroy everything."[3] The tone is hyperbolic, but hardly unusual. Numerous experts in the United States, Europe, and beyond continue to claim a 'dire' threat in cyberspace. State rivalries increasingly play out through digital incursions, and the reality is that an attack like the one suffered by Estonia could all too easily lead to a shooting war.

[2] John O. Brennan, *Remarks at the Launch of the U.S. International Strategy for Cyberspace* (Washington: The White House, 2011).

[3] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, 21 August 2007.

In 2008, the U.S. administration asked for $7.2 billion to support its cyber-defense initiatives.[4] In the UK, cyber-defense spending was one of the only budget lines that not only escaped massive spending cuts in 2010, but received an increase to £650 million over four years.[5] In 2009, a comprehensive American policy study on the "digital threat" determined that "the loss of information has inflicted unacceptable damage to U.S. national and economic security," and that the nation's response would have to be "comprehensive…using all the tools of U.S. power in a coordinated fashion."[6]

The balance of this study considers three logics of restraint — categories well-known to scholars of international relations but not yet systematically applied to cyberattacks — and asks which if any might lead states to reconsider their use. They include first, the rationalist mode of deterrence; second, the regulative mode of the *jus ad bellum,* or international law regulating recourse to force and self-defense; and third, the more ethical and reputational effects of the *jus in bello,* with its proscriptions on certain types of weaponry and tactics. While the latter two are fundamentally studies of how international law might apply to cyberattacks, as those chapters will explore, the ways in which those canons of law might functionally restrain state behavior may indeed be quite different.

The principal argument of this study is that cyberattacks possess novel attributes, frustrating the applicability of any single regime, but can indeed be

[4] Symantec, "Here Comes the CNCI, and the Era of Proactive IT Security," 28 August 2008.

[5] United Kingdom Cabinet Office, *Keeping the UK Safe in Cyberspace*, ed. Cabinet Office of Cybersecurity (London: The Stationary Office, HMG, 2013).

[6] Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, ed. James Lewis (Washington: CSIS, 2008), Preface, 1.

contextualized within international relations. Existing forces of restraint apply in meaningful ways to states' use of cyberattacks, and in some cases, may already be acting to shape state decision-making. First, I argue states are already pursuing strategies to impose those forces on one another, through deterrence postures or de-legitimization of the use of cyberattacks under international law. However, I argue, states generally lack the customary and legal context in which to meaningfully ground their positions, and are building their positions upon untested customary dynamics and unsubstantiated legal claims. As such, those strategies reflect immediate self-interest, and are limited in what they reveal about the long-term effect of cyberattacks on international security. Far more revealing, then, is whether any of those present strategies are durable under the regime they reference — be it conventional deterrence, the U.N. Charter's limitations on recourse to force, or international humanitarian law. Given the novelty of cyberattacks, the only way to evaluate those claims is with reference to the existing laws and norms that exercise restraint in the international system, and informed by analogy to other means and methods of warfare upon which those regimes have previously operated.

Given the abundance of state policies and postures on cyberattacks, this study focuses on nation-states' use rather than non-state activities — the latter being both less significant, and less applicable to a study of restraint in international relations. In the first instance, this analysis therefore concentrates on states as the locus of cyberattacks that significantly threaten national and international security. It is true that low barriers to entry might allow non-state actors to develop coercive tools, however they typically do not identify with, find themselves bound by, or behave in accordance with the customs, regimes, and norms relevant to this study.[7] Even more importantly at the present time the capabilities of non-state actors alone (excluding when co-opted or sponsored by a state), are simply not commensurate with those of nation-states, and do not merit this level of analysis — at least not as independent phenomena.[8] It is for this reason that, as later chapters will explore in-depth, national policy documents such as the U.S. *International Strategy for Cyberspace* fix their focus primarily if not exclusively on state-based actors.[9]

The explicitly ethical concerns cyberattacks raise are not the focus of this study, however it does engage them indirectly with reference to certain regimes with strong ethical character, such as the *jus in bello*. This study does not lose sight of that broader context, but it is neither a work of comparative ethics nor international normative theory. As a matter of normative framing, this study merely presupposes that cyberattacks can and will — if used — have negative impacts on the 'peaceful' interaction of states, their economies, and their people. As with any instrument capable of causing human suffering, there is arguable ethical value in restraining its use. This is not to say this study regards cyberattacks as ethically inferior (or

[7] This approach is also consistent with Joseph Nye's observation in the broader context of international power dynamics when he writes, "Although a hacker and a government can both create information and exploit the Internet, it matters for many purposes that large governments can deploy tens of thousands of trained people and have vast computing power." Joseph Nye, *The Future of Power* (New York: PublicAffairs, 2011), 117.

[8] 'Cyber-terrorism,' once frequently used to describe terrorist use of cyberattack tools, has all but fallen out of the international lexicon, as will be explored in more depth later in the chapter.

[9] The White House, *The United States International Strategy for Cyberspace* (Washington: U.S. Government Printing Office, 2011). (Hereafter cited as *USISC*.) See in particular 14. The *USISC*, cited at various points throughout this study, is that nation's primary document explaining its positions on foreign policy issues related to cyberspace and cybersecurity.

superior, as some literature does), to traditional conflict.[10] Rather, this study shares a narrower normative orientation with those regimes that simply seek to limit unnecessary employment of destructive acts, and consistent with it, does not regard an exchange of cyberattacks as a 'pacific settlement of disputes.'

Having now outlined the topic and scope of the study, the balance of this introduction will define cyberattacks and illustrate their potential with recent cases, summarize the relevant literature, and outline the methodology and argument of subsequent chapters.

1.2 Defining 'Cyberattacks'

This section defines 'cyberattacks,' the subject of this study. It begins with the technological context that explains their operation and significance, and then offers a formal definition that distinguishes them from other 'lesser' phenomena of cybercrime and cyber-espionage. It concludes by making that definition concrete, outlining an early, small-scale example that played out in Estonia in 2007.

Context: Ubiquitous and Vulnerable Digital Systems

Cyberattacks pose a significant and growing threat to modern economies and societies for two principal reasons: increasing dependence on 'networked information infrastructure' and the vulnerabilities inherent in those systems.

[10] See, for example: George R. Lucas, "Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets," in *Oxford Institute for Ethics, Law and Armed Conflict seminar series* (2011), 7; Neil C. Rowe, "Towards Reversible Cyberattacks," (Consortium for Emerging Technologies, Military Operations, and National Security, 2011).

It is difficult not to notice that in the developed world, these electronic systems enable, facilitate, and regulate innumerable aspects of daily life.[11] From computers to automobiles, mobile phones to traffic signals, advanced avionics to banking, these systems — and the information stored and transmitted in their operation — all employ digital signals. According to the U.S. Secretary of Homeland Security, who since 2011 has cited cybersecurity as the agency's top priority alongside counter-terrorism, "our economies, our healthcare systems, and our transportation networks all depend on secure and resilient cyber networks."[12]

This technological ubiquity and dependence is shared by civilian and defense sectors. As one senior U.S. intelligence official put it, "[c]lose to 98 percent of the nation's most important information is housed on [sites] ending in .com," the vast majority of which share the same underlying protocols.[13] Equally dual-use are the most important cables and switches transmitting both private commercial and highly sensitive government data.[14] Increasingly, public utilities control the flow of water

[11] Technological dependence, and the risks associated with it, has become the cause célèbre of many states' national defense and security strategies over the last several years. See, for example: The White House, *The National Strategy to Secure Cyberspace* (Washington: U.S. Government Printing Office, 2001); *The United States National Security Strategy* (Washington: U.S. Government Printing Office, 2009); Australia Attorney General's Department, *E-Security Review* (Canberra2008). Further, the international community has recognized this dependence in the social and economic spheres at the United Nations in A/RES/64/211 and other resolutions focused on "building a global culture of cyber-security."

[12] Janet Napolitano, *Remarks at the Launch of the U.S. International Strategy for Cyberspace* (Washington: The White House, 2011); Amber Corrin, "Cyber Executive Order Close, Napolitano Says," *Federal Computer Weekly*, 28 September 2012; Janet Napolitano, *Appointment of New Deputy under Secretary for Cybersecurity* (Washington: Department of Homeland Security, 2013).

[13] Donald M. Kerr, *Remarks by the Principal Deputy Director of National Intelligence at the Association for Intelligence Officers Annual Intelligence Symposium* (McLean, VA: United States Office of the Director of National Intelligence, 2008).

[14] The United States Congressional Research Service (CRS) notes that the US military "relies significantly on the civilian information infrastructure." United States Congressional Research Service, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress* (Washington: Congressional Printing Office, 2003), 1.

and electricity remotely, via computers connected to the public Internet.[15] Some military experts have even noted that major armed forces' ability to mobilize would be fundamentally jeopardized by the disruption of shared, public, and unclassified fiber-optic networks used by their logistics command.[16] As summarized by a 2010 United Nations Group of Governmental Experts (GGE), the second such body tasked to examine information technology in the context of information security: "because they are inherently dual-use in nature, the same [technologies] that support robust e-commerce can also be used to threaten international peace and national security."[17]

There are countless components, operating across numerous media, that come together to make these technologies function. While they utilize the electromagnetic spectrum, they often do so by means of man-made appliances that exist in real space. They transmit data in the form of signals, over networks that exist both digitally — in terms of the communication between appliances to exchange those signals — and physically, via cables and switches. Hence, components of the 'electronic' world may not appear to be, at first glance, particularly electronic at all.

Underlying the operation of all these electronics is a category of technology called 'information infrastructure,' hardware and software ubiquitous and increasingly fundamental to modern economies, societies, and militaries.[18] Information

[15] Georgia Tech Information Security Center, *Emerging Cyber Threat Reports, 2011* (Atlanta, GA: Georgia Institute of Technology, 2011), see especially 8-9.

[16] Daniel T. Kuehl, "China and Cybersecurity" (paper presented at the National Security Seminar, Heritage Foundation, 28 April 2010).

[17] United Nations Group of Governmental Experts (2008-9), *Report Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2008-9)* (Geneva: United Nations (UNIDIR), 2010), 6. (Hereafter U.N. GGE 2010.)

[18] Office of Technology Assessment (United States), *Information Security and Privacy in Network Environments* (Washington: Government Printing Office, 1994), 27. This is also the definition favored by noted military/cybersecurity commentator Greg Rattray. His is perhaps the best single volume to

infrastructure can be thought of as the physical infrastructure that enables a computer's operation, or the electronic processes that keep computer networks functioning as digital signals pass from machine to machine to transmit data. In sum, information infrastructure is the shared hardware and software that enable devices to communicate with one another, and thus underlie most day-to-day interaction with technology.

The same attributes that make information infrastructure so versatile — allowing a network router to be as useful to a military planner as it is to an online retailer — also make those networks inherently vulnerable. The Internet was designed with versatility and accessibility in mind — but not necessarily security.[19] Many of the core Internet technologies are trust-based systems; they are designed and continue to operate under principles that maximize interoperability between diverse systems and innovation in their use. In order to be maximally compatible, these networks are designed to accept signals from a range of machines, thus depending on 'open' standards and protocols that pass and accept malicious data often as easily as legitimate data. This 'openness' and 'interoperability' is therefore responsible for both the pace of innovation and the infrastructure's inherent insecurity. That vulnerability is compounded by the fact that not only are the same types of infrastructures vital to the functioning of modern economies and militaries, but often

date on the purely military aspects of the subject. See: Greg Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001).

[19] Fritz E. Froehlich and Allen Kent, *Froehlich/Kent Encyclopedia of Telecommunications*, vol. 15 (New York: Marcel Dekker, 1997), 233; United States General Accounting Office, *Computer Security: Hackers Penetrate DOD Computer Systems* (Washington: GAO, 1991).

the *same infrastructure itself* is shared by them in the form of switches, satellite connections and fiber optic cables.

Information infrastructure can be disabled, with similar effect, by a kinetic (i.e. physical) or non-kinetic (i.e. digital) attack; its critical components can be blown up and network cables severed, or they can be flooded with damaging information and viruses. Fiber optic cables, microwave dishes, routers and hubs that connect that infrastructure are physical, often fragile, and susceptible to destruction. Most Internet traffic routed overseas, for instance, travels through one of only a few hundred commercially owned fiber-optic cable bundles running across the ocean.[20] Several recent episodes of these lines being accidentally severed (by ship's anchors or earthquakes), and the deployment of navies to protect them from pirate attack off the Somali coast, demonstrate the fragility of the system.[21] In a recent case near San Francisco, phone and Internet access was disabled through broad swathes of the world's largest technical hub — California's Silicon Valley — when what is presumed to have been a single disgruntled maintenance technician, armed only with a pair of wire clippers and knowledge of the system, severed some of the region's fiber-optic lines.[22] If coordinated by a state deploying several highly trained operatives, the impact could be much greater — a prospect given voice by senior

[20] Peter Svensson, "Finger-Thin Undersea Cables Tie World Together," *Associated Press*, 31 January 2008.

[21] In 2006, four major fiber optic lines were severely damaged following a major earthquake in Taiwan; subsequent underwater mudslides damaged nine cables laid in the Luzon Strait south of Taiwan, destroying all eastward data routes from Southeast Asia. It took forty-nine days for crews on eleven giant cable-laying ships to fix all of the twenty-one damage points. International Cable Protection Committee, *Subsea Landslide Is Likely Cause of SE Asian Communications Failure* (London: ICPC, 2007); Tahani Karrar, "Third Undersea Cable Reportedly Cut between Sri Lanka, Suez," *Dow Jones Newswire*, 1 February 2008.

[22] Marguerite Reardon, "Vandals Blamed for Phone and Internet Outage," *CNet News*, 9 April 2009.

national security officials including the U.S. Secretary of Defense.[23] Blunter kinetic approaches would also be effective. Several central locations throughout the United States, and only a few throughout the United Kingdom, serve as hubs for routing Internet traffic; the simultaneous destruction of two or more could cause considerable damage to the system. The destruction of a handful of communications satellites would also substantially disrupt information flows — explaining Western concern over China's 2007 anti-satellite weapon test.[24]

The combination of vulnerability of and dependence on these systems for basic societal processes makes cyberattack scenarios increasingly relevant for international security. Consider how critical infrastructure that undergirds modern society is, far more often than appreciated, remotely operated and dependent on Internet-accessible networks. Such Supervisory Control and Data Acquisition (SCADA) systems are responsible for the operation of countless functions like water treatment and distribution, electric power generation (including nuclear power), pipelines, chemical plants, and other industrial processes for manufacturing and production.[25] Similar to countless other technologies, as SCADA systems have

[23] Leon Panetta, *Remarks on Defending the Nation from Cyber Attack (11 October)* (Washington: U.S. Department of Defense, 2012).

[24] Carin Zissis, *Backgrounder: China's Anti-Satellite Test* (New York: Council on Foreign Relations, 2007).

[25] The U.S. Congressional Research Service defines SCADA as referring to "the function of those systems, which are often used to control processes in industrial facilities and to log information about status and conditions. They often communicate electronically with central computer systems that are connected to the Internet." United States Congressional Research Service, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options* (Washington: Congressional Printing Office, 2005), 11.

become more networked and designed for remote use, they have become less secure.[26]

For example, poor network security has created the possibility of a remotely triggered nuclear meltdown or large-scale power-generation disruption. In 2008, the Hatch Nuclear Power Plant in the United States reportedly underwent an emergency shutdown as a result of a software update to its business systems. Subsequent investigation found that those business networks were directly linked to (and able to access) critical SCADA systems responsible for functions like cooling at the plant.[27] Similarly, the Browns Ferry nuclear facility in the United States shut down in 2006 when a network traffic overload locked up pump controls.[28] A targeted virus, such as the one researchers claimed was found sabotaging the Iranian nuclear program, represents a small-scale and targeted version of just such an attack vector.[29] Just as with that so-called *Stuxnet* worm, the consequences of a cyber-enabled SCADA disruption may well be physical, to include widespread blackouts, shutdown, or ignition of energy production or transport facilities such as oil and natural gas pipelines.[30]

[26] Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. (Indianapolis, IN: Wiley & Sons, 2008), 389-414.

[27] United States Department of Homeland Security, *Alert: Increasing Threat to Industrial Control Systems*, ed. Industrial Control Systems Cyber Emergency Response Team (Washington: Department of Homeland Security, 2012).

[28] For actions being taken to close such SCADA security gaps, *see*: Jacob Goodwin, "FERC Seeks to Close Any Cyber-Security 'Gaps' at Nuclear Plants," *Government Security News*, 25 March 2009.

[29] John Markoff, "A Silent Attack, but Not a Subtle One," *New York Times*, 26 September 2010; Robert McMillan, "Siemens: Stuxnet Worm Hit Industrial Systems," *Computerworld*, 14 September 2010.

[30] Joel Brenner, *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World*, Reprint ed. (New York: Penguin, 2013), 99.

This vulnerability has not been lost on countries like the United States and United Kingdom, who see a substantial risk, but also potential advantage. According to one U.S. military official, "as infrastructure becomes modernized and networked in most nations throughout the world, reaching system SCADA on a variety of lucrative targets is quickly becoming a milestone in any military operation."[31]

These attacks could be further exacerbated by the stealth installation of digital 'kill-switches.' Practically undetectable in complex systems once installed, this kind of malicious software is designed to cause disruption, with no more than an activation signal, at any time after its installation.[32] Intelligence and defense officials have specifically noted the likelihood of such an attack. According to a 2009 report, British intelligence chiefs warned that China may have gained the capability to effectively cripple the UK's telecommunications through digital sabotage, which could in turn be used to halt critical services such as power or water supplies.[33]

A final, salient point for the international context is that a cyberattack's effects multiply exponentially with the overall level of the victim state's digitization, or reliance on information infrastructure.[34] An economy or society with a very low level of reliance on networked systems would suffer minimal effect from even a

[31] Centre for the Protection of National Infrastructure (United Kingdom), *Process Control and SCADA Security* (London: CPNI, 2008); Bruce A. Wright, "Remarks before the Defense Colloquium on Information Operations," (1999). (Quoted in William Church, "Information Operations Violates Protocol I," *InfoWar Monitor*, 9 April 1999.)

[32] David A. Fulghum, Amy Butler, and Sally Adee, "Cyber-Combat's First Shot," *Aviation Week*, 26 November 2007; Sally Adee, "The Hunt for the Kill Switch," *IEEE Spectrum*, 1 May 2008.

[33] Mike Harvey, "Chinese Hackers 'Using Ghost Network to Control Embassy Computers'," *The Times (London)*, 30 March 2009.

[34] These effects might be conceived of as the digital equivalent of a bombing-induced 'firestorm'—where an attack of sufficient intensity renders itself broader and more destructive by exploiting feedback the initial damage creates.

sophisticated cyberattack — as was largely the case when Russia launched a digital offensive on computers in Georgia on the eve of its 2008 invasion.[35] In tech-reliant states though — including most Western democracies, Japan, South Korea, and others — a profound and exponential feedback effect exists between large information economies, advanced militaries, and the corresponding levels of daily technology use. The principle of inter-connectedness is not terribly new: studies of globalization and trade often examine how technological and human networks grow and become increasingly reliant on the smooth functioning of the larger system.[36] The same is true with digital systems that underlie the economies, societies, and military of modern states. Not just any disruption of these systems would constitute a national security event, yet given some countries' high levels of dependence on information infrastructure and the increasing interconnection between those systems, new avenues are available for a sophisticated state actor to effect a large-scale, cascading failure. It is this general concept of interconnection and vulnerability that helps frame what a cyberattack means in international relations.

Formal Definition

One can see how this shared infrastructure creates a highly appealing target for the would-be attacker who is seeking to disrupt or otherwise disable a technology-

[35] Alex Kingsbury, "In Georgia, a Parallel War Rages Online," *U.S. News & World Report*, 13 August 2008. Incidentally, the global dimension of these feedback effects—at least with regard to economic externalities (such as disruptions to trade flow)—suggest that less developed, less technology-dependent states might be more likely to conduct a cyber assault against a more developed enemy, seeking to maximize the asymmetry inherent therein.

[36] See, for example, Thomas L. Friedman, *The World Is Flat: A Brief History of the Twenty-First Century*, 1st ed. (New York: Farrar, Straus and Giroux, 2005).

dependent state or subdivision thereof. Using this capability to significant national security effect is the subject of this study:

> **A cyberattack** is a coercive act that exploits the insecurities of networked systems, disrupting or destroying information infrastructure or the critical infrastructure dependent on it, to significant national security effect.

"A coercive act…" First, the act in question must be an intentionally *coercive act*, which is to say designed by an aggressor state to achieve a particular change in behavior from the victim state (ranging from new policy choices to outright surrender).[37] This characteristic distinguishes cyberattacks from cybercrime, which is primarily financial in motivation and carried out by individuals on their own or their syndicate's behalf. It also distinguishes cyberattacks from cyber-espionage, which is by contrast seeking to amass information to inform decision-making or gain strategic advantage.[38] In the cases of cybercrime and cyber-espionage, cyberspace offers only a new venue in which to undertake well-known activities.[39] Digital systems may make these actions easier or possible on a greater scale, but beyond that potential intensification there is little deeply novel from the standpoint of international relations. By contrast, and as the balance of this study will argue, cyberattacks are not straightforwardly dealt with by any single regime of law, and even less so by existing customary state practice.

[37] Throughout, this study favors the use of the phrase 'interstate coercion' to 'conflict,' 'act of war,' 'act of aggression,' or other characterizations of such phenomena. Other phrases would, potentially, presuppose or otherwise prejudice the analysis of later chapters examining whether those legal designations apply.

[38] Some governments refer to this category of 'hacking' as Computer Network Exploitation (CNE), which, along with a few other specialized operations, generally comprises the kind of data exfiltration characteristic of digital espionage.

[39] So-called 'cyber-terrorism' is also excluded from this definition; because of the fundamentally contested (and potentially applicable) nature of concepts of a terrorist act, a section of Chapter 3 briefly explores the applicability of this tactical concept.

"…disrupting or destroying information infrastructure…" What sets cyberattacks apart is the likelihood that they will exploit critical information infrastructure. This is a technologically complex task, and studies of the technical tools of disruption in cyberspace are consistent in the view that states retain preeminence in developing these most sophisticated and effective tools — in other words, those capable of widespread disruption on a national scale.[40] As such, in the strategic cyber-defense literature, there exists a compelling consensus that as *primary* actors, state actors will maintain enduring relevance due to particular resource and organizational advantages.[41] Because states have at their disposal intelligence services, long-term military planning, and vast economic resources, they are most capable of making devastating cyberattacks that target and disrupt critical infrastructure, including information infrastructure.

This is not to say that cybercrime tools or actors might be used, in aggregate, by states seeking to orchestrate a less attributable cyberattack. Talented rogue actors may develop one-off tools capable of significant damage. Hackers for hire, often affiliated with organized crime, offer unsophisticated cyberattack tools at prices within reach of even moderately resourced militaries. Indeed, some organized crime elements are known to have developed cyberattack tools, and may have even amassed

[40] See: Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners* (Oxford: Syngress, 2011), 71; McAffee and Good Harbor Consulting, *Virtual Criminology Report* (Santa Clara, CA: McAfee, 2009); Select Committee on Intelligence, United States Senate, *Annual Threat Assessment of the US Intelligence Community, Unclassified (Testimony of Adm. Dennis C. Blair)*, 2010, 2.

[41] See: United States Air Force, *Air Force Doctrine Document 2-11: Cyberspace Operations* (Washington: LeMay Center for Doctrine Development and Education, 2008).

the kind of rudimentary capability that disabled Estonian information infrastructure.[42] Therefore the technological sophistication of a country may not track to its ability to obtain or deploy cyberattack tools — consider that North Korea has per capita Internet penetration roughly equivalent to the Democratic Republic of the Congo, yet is also believed to have orchestrated a number of disruptive cyberattacks from 2008 to the present.[43] An attacker need not create all cyberattack tools indigenously; military-scale spending can narrow some military asymmetries, as can a willingness to transact with criminal actors.

"…or the critical infrastructure dependent on it…" Cyberattacks of national consequence would target the shared critical infrastructure outlined in the prior section. That infrastructure can take two forms: the information infrastructure itself, which permits digital systems to operate, or a disruption that degrades the functioning of more traditional infrastructure reliant upon it, such as electrical grids. While cyberattacks would in most instances be executed from afar and via electronic signals, they could conceivably include targeted disruption of physical infrastructure. The referent object of this definition is the infrastructure itself, not the method of its disruption. A non-kinetic, 'digital' attack uses computer signals carried over a network to cause effects either to other digital systems, or perhaps as a second-order consequence to the physical assets they control (such as an electrical grid).[44] Even

[42] Iain Thompson, "Russia 'Hired Botnets' for Estonia Cyber-War: Russian Authorities Accused of Collusion with Botnet Owners," *Computing (UK)*, 31 May 2007.

[43] International Telecommunications Union, *World Telecommunication/ICT Indicators Database 2010* (Geneva, 2010); BBC News, "South Korea Blames North for Bank and TV Cyber-Attacks," 10 April 2013; "North Korea Launched Cyber Attacks, Says South," *Associated Press*, 11 July 2009.

[44] What the U.S. government refers to as 'computer network operations' (CNO), falls generally within this area. CNO is a blanket term that includes computer network exploitation (CNE), namely

surgically precise disruption can lead to profound military effects, as Syria learned when, according to media accounts, an Israeli cyberattack disabled some of Damascus' radar systems before an airstrike on a covert nuclear facility.[45] Western defense officials have also made public their specific preparations for such an attack.[46]

"…to significant national security effect." Finally, the act in question must possess a quality of severity in the context of national and international security. This point cannot be overemphasized, given the penchant for hyperbole epidemic among press and other popular accounts of disruptive events in cyberspace. To be sure, unsuccessful attempts by a rogue regime or individual to disrupt information infrastructure of a less favored state does not truly constitute a cyberattack as examined in this study. These types of 'attacks' are common — so common, in fact, that the top United States general tasked with cyberspace defense numbers them in the millions annually.[47]

The issue then is the severity of effect — an attribute impossible to quantify, but the permutations of which will be explored throughout.[48] For the purposes of

reconnaissance and espionage; and computer network attack (CNA), namely sabotage and remote system disablement. Cyberattacks thus include CNA, but not CNE (as will be discussed shortly).

[45] Kingsbury, "In Georgia, a Parallel War Rages Online."; David Fulghum, "Israel Used Electronic Attack in Air Strike against Syrian Mystery Target," *Aviation Week*, 8 October 2007.

[46] For example, the U.S. military encountered just such a case in the "Buckshot Yankee" episode. See: William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010. See also: Julian E. Barnes, "Cyber-Attack on Defense Department Computers Raises Concerns," *Los Angeles Times*, 28 November 2008; Agence France-Presse, "Growing Threat from Cyber Attacks: U.S. General," 7 April 2009.

[47] BBC News, "US Cyber War Defences 'Very Thin', Pentagon Warns," 16 March 2011.

[48] As Chapter 3 explores, the ultimate decision of 'severity' is in the eye of the beholder, and that *policy* judgment is in many cases the determinant of appropriate response. Therefore for analytical purposes, assigning a quantitative or even overly precise 'threshold' to the gravity of an event to

definition, however, such an incident must *cause severe disruption, degradation or destruction of critical systems* — or, put another way, must be of sufficient effect as to be judged by the victim to constitute a real threat to national and economic security and/or social stability. Despite attempts by some policy-focused literature to quantify these threats, this is a qualitative judgment of effect, rather than a quantitative threshold (such as declaring a cyberattack any computer-based event that, for instance, disrupts power to ten million or more homes).[49]

By way of analogy, it may be true that any itinerant bullet whizzing over national borders could be judged an attack. It may further be true that if an identified soldier fired that shot, it too could register as such. Were a civilian struck and killed by that bullet, it may indeed be an attack of some consequence. The ultimate determinant, however, is one of context. If that gunshot were fired today across the Canada-U.S. border, neither Washington nor Ottawa would deem it a meaningful 'attack.' It would not be a national security incident of consequence. If, however, that gunshot crossed the 38th parallel, striking a South Korean guard, the atmosphere of tensions might well create an entirely more explosive effect. As a study within international relations, the notion of an 'attack' is often shorthand, excluding events of minor import and drawing attention to those of national and international consequence. So too does this study, in the case of cyberattacks.

quality as a 'cyberattack' would be counterproductive, missing the point of the real-world question at hand entirely.

[49] See, for example, the metrics developed by U.S. Cyber Consequences Unit. Scott Borg, *The Cyber Defense Revolution: A Synthesis (Presentation of the U.S. Cyber Consequences Unit)* (Tallinn, Estonia: NATO CCD-COE, 2009).

Severity also argues for retaining states as the principal focus of this study. Individually, non-state actors are more likely to pose a nuisance rather than a comprehensive threat to a state's national security, as a part of a coordinated, well-funded cyberattack. Their potential involvement complicates, but does not undermine questions of self-defense — rather, key issues include the extent of state involvement or complicity in such an attack.[50]

Cyberattacks are thus a distinct form of interstate coercion, and one that because of its novelties, eludes comprehensive analogy. The point was well summarized by the 2010 United Nations Group of Governmental Experts (GGE), which concluded that that networked technologies:

> Have unique attributes that make it difficult to address threats that States and other users may face…are ubiquitous and widely available…are neither inherently civil nor military in nature, and the purpose to which they are put depends mainly on the motives of the user. Networks in many cases are owned and operated by the private sector or individuals. Malicious use…can easily be concealed. The origin of a disruption, the identity of the perpetrator or the motivation can be difficult to ascertain. Often, the perpetrators of such activities can only be inferred from the target, the effect or other circumstantial evidence…[t]hese attributes facilitate [their] use for disruptive activities.[51]

Preliminary Evidence: Estonia

The international community has already witnessed a rehearsal for just such an attack, during a coordinated but temporary episode that took place in Estonia in 2007.

On April 27, 2007, Estonian government officials and private citizens alike awoke to discover that their country — among the most wired in Europe — was

[50] Chapter 3 will take up the question of culpability for a 'cyberattack' deemed an act of aggression.

[51] GGE (2010), 3.

suffering from a massive computer network outage.[52] The Minister of Defence was unable to browse the web or check his military email; on the streets, ATM terminals stopped functioning and bank transactions would not clear; online, access to domestic and foreign media outlets was blocked, and information from Europe's leader in 'e-Government' was unavailable.

The computer-based attacks that caused this mass disruption commenced only a few days after the relocation of a Soviet-era memorial from a central square in Estonia's capital of Tallinn (a move that occasioned great protest by Russian nationalists and Kremlin officials).[53] Machines used in the attack were traced to Russian Internet addresses, and claims that the attack was of Russian origin, and had government coordination, appeared throughout online chat rooms and message boards.[54] The sophistication of the attack suggested that a state might have played a role, as did the common knowledge among Internet experts that law enforcement within Russia was notoriously (and perhaps intentionally) lax at prosecuting the online criminals capable of facilitating such an attack.

The intentional disruption of Estonia's networks was unprecedented in its coordination and effectiveness, but far more troubling for policymakers and defense officials were its implications. With so much circumstantial evidence pointing to Russian responsibility, Estonian officials began asking the difficult question: were the events of April 27 tantamount to an armed attack by Russia? If so, how should the

[52] Davis, "Hackers Take Down the Most Wired Country in Europe."

[53] BBC News, "Estonia Hit by 'Moscow Cyber War'," 17 May 2007. Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet Wars," *Georgetown Journal of International Affairs* (2008): 121-26..

[54] Thompson, "Russia 'Hired Botnets' for Estonia Cyber-War: Russian Authorities Accused of Collusion with Botnet Owners."

government respond? Would the international community even recognize the attack as a prohibited use of force, and could Estonia legitimately consider a reprisal of any kind? Even more complicated was the question of whether or not NATO had an obligation to interpret the episode as an "attack against them all," thus activating member states' treaty obligations to respond militarily.[55] The issue was brought to NATO's attention by Estonian officials and has been treated with great seriousness since, meriting a special 'break-out' session on the agenda of the 2008 NATO summit in Bucharest.[56]

The challenge for both Estonia and NATO in defining the event began with the sheer incommensurability of a digital attack and traditional notions of state-based military belligerence. The attack's effects lasted only days, but that was hardly known to the victim government in planning its response. It held a large percentage of the Estonian economy, government, and aspects of its military hostage. There appeared no ready way to identify with any certainty the individual(s) manipulating the thousands of machines used in the attack. Moreover, the attack was not a traditional 'smash-and-grab' operation aimed at stealing sensitive state information (thus relegating it to the sphere of espionage), but instead targeted computer network infrastructure shared by both the civilian and military sectors. Response in-kind was impossible for a number of reasons, yet a military response would be unprecedented. Ultimately, the matter ended in a state of uneasy inaction and hushed debate over the inapplicability of defense plans to this new threat.

[55] *North Atlantic Treaty*, Art. 5.

[56] Sydney Morning Herald, "Estonia Urges Firm EU, NATO Response to New Form of Warfare: Cyber Attacks," 16 May 2007.

NATO’s lack of a clear response revealed uncertainty about how to assess the attack that Estonia had just sustained, as well as serious concerns about the legality of mounting a response. This trepidation was not entirely new. NATO members had already attempted to grapple with these same international legal issues during the 1999 action in Kosovo. After that intervention, unnamed senior defense officials were quoted admitting to the existence of plans to use computer-based attacks against Serbian technology infrastructure, but added that the United States chose not to follow through after legal guidance from the Defense Department Legal Counsel suggested that such tactics might be considered ‘war crimes.’[57] Similar concerns held back cyberattacks contemplated against Saddam Hussein’s interests during the Second Gulf War.[58] What was abandoned then as legally tenuous was brought to the fore in Estonia, with apparently few guiding precedents developed in the intervening years. In the case of Estonia, an even more basic question held NATO back from responding: would the assault just sustained by the Estonians even be considered an illegal use of force under international law?

To this day these questions remain largely unanswered, even as they increase in relevance. As previously noted, in 2008 Russia was again accused of attacks on a nation’s computer systems, this time as part of its overt offensive against Georgia. The cyberattack is on its way to becoming a valuable tool of interstate coercion, but one that many intelligence and defense officials freely admit is poorly understood,

[57] Bradley Graham, "Military Grappling with Guidelines for Cyberwar," *Washington Post*, 8 November 1999.

[58] John Markoff and Thom Shanker, "Halted ’03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *The New York Times*, 1 August 2009.

and the study of which is, outside the domestic law enforcement realm, very much in its intellectual infancy.

1.3 Literature

The literature relevant to this study falls into three broad categories: early doctrine examining 'information warfare' as an abstract concept; more recent accounts focusing on the national cybersecurity threat and policy steps to mitigate it; and a recent but growing literature focusing specifically on cyberattacks in domestic and international law. This section outlines each category to demonstrate there is a significant gap in literature: the paucity of studies applying existing international regimes and customs, responsible for state restraint from other methods of coercion, to this new tool. Even less of the relevant literature is generally applicable within international relations, and is instead aimed at influencing a particular state's policy. Both are notable lacunae this study aims to fill.

Early Literature on 'Information Warfare'

The first direct contribution to the study of cyberattacks can be traced back to military theory and doctrine from the period of the late 1970s through early 1990s. These studies are often neglected, but important in explaining the intellectual origins of present-day state policies regarding cyberattacks.

Such works were products of their historical era in seeking to understand, for the first time, the wartime effects of increased computing power and the reliance on information systems. As a function of that framing, terminology differed, and many works sought to extend well-known concepts of 'information operations' to 'information warfare.' In what was probably the earliest modern use of the term in this context, a researcher for the U.S. Office of Net Assessment used the term 'information warfare' (IW) in the 1970s to describe the competition between competing 'cybernetics,' or control systems.[59] Absent any examples of a state using purely attacks advantage to achieve military aims, the earliest works sought to apply precepts of military theory to a hypothetical environment where information, rather than conventional firepower, might provide a state with superior resources to fight and win a war.[60] Most notable in this literature is the notion of digital capabilities as a discrete concept contributing to military power. This theme, while underdeveloped in the military-focused doctrine of the era, was prescient in considering cyberattacks as a force influencing states' perceptions of power in their international relations.[61]

Bridging this early work and the present topic, consideration of which began in earnest in the mid-1990s and early 2000s, were three key volumes — all by affiliates of the RAND Corporation. These books, for first time, analyzed in the international context the role of a discrete attack originating from computer networks. While still relying upon earlier terminology, Daniel and Julie Ryan paved new ground in defining a concept very much akin to the subject of this study, situating in their work around the notion that "information warfare is, first and foremost, warfare. It is not information terrorism, computer crime, hacking, or commercial or state-sponsored

[59] David Tubbs, Perry G. Luzwick, and Walter Gary Sharp, "Technology and Law: The Evolution of Digital Warfare," in *Computer Network Attack and International Law*, ed. Michael Schmitt and Brian O'Donnell (Newport, RI: Naval War College, 2002), 36. (Hereafter cited as *Naval War College.*) This concept is distinct from the sort of 'information advantage' in warfare present in doctrine from Sun Tzu to Clausewitz; rather than competing for the most information, the present-day form of 'information warfare' envisaged competition of systems for controlling information, what today we would regard as computing power and networking speed.

[60] See, e.g., Davis Alberts and Richard Hayes, *Power to the Edge: Command...Control...In the Information Age* (Washington: DoD Command and Control Research Program, 2005).

[61] These contributions presaged works like Nye's 2011 chapter-long meditation on "cyberpower." See: Nye, *The Future of Power*, Chapter 5.

espionage using networks for access to desirable information."[62] Likewise, Khalilzad and White's edited volume represents the most expansive and topical of these works, supplemented by John Arquilla and David Ronfeldt's volume considering the full range of cyberattack possibilities.[63] While not fully durable in today's analysis, and carrying outdated terminology, both volumes remain markedly forward-looking in considering the full range of disruptive actions, such as early 'hacktivist' website defacements and terrorist use of the Internet.[64]

All three of these works stand out for their relevant focus, while much of the rest of related literature in the 1990s, by scholars like George Stein, John Alger, and Dorothy Denning, had difficulty articulating and forming a discrete program of study, in part due to an approach deeming 'information warfare' nearly every aggressive act utilizing information of any sort.[65] These problems of definition are not unique to the cyber field; in discussions of irregular warfare, one scholar has pointed out, "authors are inclined to lump everything together under a concept to the point where a term describes everything and explains nothing."[66] In this respect, history appears to

[62] Daniel J. Ryan and Julie C. H. Ryan, "Protecting the National Information Infrastruture against Infowar," in *Information Warfare: Chaos on the Electronic Superhighway*, ed. Winn Schwartau (New York: Thunder Mouth Press, 1994), 672.

[63] John Arquilla and David Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica: RAND, 2001). Zalmay Khalilzad and John P. White, eds., *Strategic Appraisal: The Changing Role of Information in Warfare* (Santa Monica: RAND, 1999).

[64] John Arquilla and David Ronfeldt, "Emergence and Influence of the Zapatista Social Netwar," in *Networks and Netwars*, ed. John Arquilla and David Ronfeldt (Santa Monica: RAND, 2001).

[65] George J. Stein, " Information Warfare," *Airpower Journal* 9, no. 1 (1995); John Alger, "Introduction to Information Warfare," in *Information Warfare: Chaos on the Electronic Superhighway*, ed. Winn Schwartau (New York: Thunder Mouth Press, 1994); Dorothy Denning, *Information Warfare and Security* (Reading: Addison-Wesley, 1999).

[66] James Kiras, "Irregular Warfare," in *Understanding Modern Warfare*, ed. David Jordan (Cambridge: Cambridge University Press), 229.

repeat itself: there are meaningful parallels to the over-expansion of the ‘information warfare’ concept in the 1990s to today’s ‘cyberwar’ concept described below.

Threat-Based Literature

A second category of literature on the topic is more recent, but distinguished by its focus on influencing policymaking by documenting the cybersecurity threat as a means to capture the attention of government leaders. This literature is made up primarily of popular monographs, think-tank studies, and some scholarly articles. These works represent the vast majority of publication during the last decade, a proliferation in part attributable to a massive increase in spending by the United States government on cyber-defense since 2004, and even more so following the attacks in Estonia. Emblematic of these works are Clarke and Knake’s 2009 volume *Cyber War,* a popular monograph that vividly illustrates the potential threats of state-based cyberattack, but which suffers from many of the same definitional challenges of early work on ‘information warfare.’[67] Joel Brenner’s *America the Vulnerable* is a more recent, notable contribution in the same canon.[68] Specifically, works like *Cyber War* amplify a tendency in the press and, to some extent, academia to abuse terms of art like ‘warfare’ and ‘attack’ to describe any aggressive cyber activity, including well-understood acts like espionage, when conducted via the Internet. This terminological

[67] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010). Farwell and Rohozinski’s 2012 article is emblematic of academic journals also playing accessory to this blurring of concepts and acceptance of policy focus. See: James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival* 54, no. 4 (2012).

[68] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin, 2011). Emblematically, the book heralds itself as: “An urgent wake-up call that identifies our foes; unveils their methods; and charts the dire consequences for government, business, and individuals.”

confusion persists to this day — with a few notable exceptions, also largely in the policy and think-tank literature, seeking to refute Clarke's prediction of the outbreak of general 'cyber war.'[69] It is notable and appropriate, however, that at least the 'cyber-terrorism' neologism has fallen from the lexicon and the field of primary study, given the general consensus that states remain the primary orchestrators of cyberattacks of international consequence.[70]

Other influential works focus squarely on influencing policymaking, including early think-tank reports by experts like James Lewis, and later several special commissions appointed to examine the threat — the most influential of which was convened under Lewis' supervision.[71] Following those earlier works, dozens of similar documents have proliferated, primarily seeking to contextualize for policymakers the publicly available evidence of states' use of cyberspace (for spying and potentially attacking). The most significant of these policy-focused volumes — works edited by Kristin Lord, David Bentz, Franklin Kramer, and Herb Lin — use the domestic vulnerability as a starting point to examine the implications for foreign policy and national security.[72]

[69] James A. Lewis, *The Cyber War Has Not Begun* (Washington: CSIS, 2010); Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012); *Cyber War Will Not Take Place* (London: C Hurst & Co. Publishers, Ltd., 2013 (forthcoming)).

[70] Amidst works that overemphasized the terrorist threat, Lewis' 2002 review provided an early counterpoint, which would presage a decade's worth of subsequent work to maintain this definitional accuracy and commitment to disaggregating and contextualizing threats. See: James A. Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington: CSIS, 2002).

[71] *Cyber Security: Turning National Solutions into International Cooperation* (Washington: CSIS, 2003). Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*.

[72] Some of the most significant efforts relevant to international relations include: Kristin Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age* (Washington: Center for New American Security, 2011); David J. Betz and Timothy C. Stevens, eds.,

Missing from these particularly numerous works, then, is terminological and methodological grounding, particularly in the history and theory of international relations. The vast majority of this literature is directed not at understanding the impact of cyberattacks on the relations of states, but on one or more nation's immediate national security policy. They are oriented around how a single state should invest and organize given these changes in security practice — but in so doing, tend to orient observations and argument on the nation whose policymakers they seek to influence. These studies offer recommendations worth pursuit and further study — such as Martha Finnemore's extended recommendations on promulgating norms of responsible behavior in cyberspace, or Libicki's on 'cyber-deterrence' — but missing is a comprehensive understanding of how such an approach might bring stability to the space, and upon what precedent such an effort might rely.[73]

Legal Literature

A third and final category of literature is aimed at understanding the appropriate framework to situate cyberattacks in domestic and international law.

The earliest examples of this literature can be found in the early 2000s, when as previously mentioned, military literature began to regard technology not just as an enabler of future military operations, but also as a potential venue for them. Perhaps

Cyberspace and the State: Towards a Strategy for Cyberpower (Adelphi Series) (London: Routledge, 2012); Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington: Potomac Books, Inc., 2009); United States National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, ed. William A. Owens and Kenneth W. Dam (Washington: National Academies Press, 2009).

[73] Martha Finnemore, "Cultivating International Cyber Norms," in *America's Cyber Future: Security and Prosperity in the Information Age*, ed. Kristin and Travis Sharp Lord (Washington: Center for New American Security, 2012). Marin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009).

the most important, but often ignored epoch for the emergence of cyberattack literature was following the Gulf War and NATO intervention in Kosovo, when the first studies considering 'computer network attack' in the context of international law took shape. The latter milestone may have been particularly significant in explaining the legal establishment's early and short-lived interest in the field, as media outlets began reporting that the United States considered using cyberattack tools against the Hussein regime or Serbian targets' financial accounts during the Kosovo intervention.[74] These early works included contributions in international law from those who were first and foremost technical security experts, like Steve Lukasik and Sy Goodman.[75] Similar, individual studies by legal scholars like Walker helped bridge the gap between analysis of 'information warfare' fixated on military doctrine, and the international legal issues such a practice might implicate.[76]

The capstone of this early work was a comprehensive volume that brought together a range of noted international law scholars including Yoram Dinstein, Anthony D'Amato, and Daniel Silver to produce a single comprehensive study of the legal status of the hypothetical threat of 'computer network attacks.'[77] This work, edited by Michael Schmitt and Brian O'Donnell, remains exceptionally relevant,

[74] Elizabeth Becker, "Pentagon Sets Up New Center for Waging Cyberwarfare," *The New York Times*, Oct 8, 1999: A16; John Markoff, "The New York Times," *Military Breaks the Rules of Military Engagement*, Oct 17, 1999: L5.

[75] Greory D. Grove, Seymour Goodman, and Stephen Lukasik, "Cyber-Attacks and International Law," *Survival* 42, no. 3 (2000).

[76] George K. Walker, "Information Warfare and Neutrality," *Vanderbilt Journal of Transnational Law* 33, no. 5 (2000).

[77] See: Yoram Dinstein, "Computer Network Attacks and Self-Defense," in *Computer Network Attack and International Law*, ed. Michael Schmitt and Brian O'Donnell (Newport, RI: Naval War College, 2002); Anthony D'Amato, "International Law, Cybernetics, and Cyberspace," *ibid*. Daniel B. Silver, "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter," *ibid*.

broaching many of the topics challenging lawyers examining cyberattacks today.[78] It did so, however, in the context of that day's technology, with a limited sense of the scale of possible disruption, an over-emphasis on the novelty of terrorist use of the Internet, and lacking any concrete examples (like Estonia) against which to evaluate its theories.[79] Perhaps given this drought of precedent, no comparable contributions to this field of the literature emerged in the years immediately following Schmitt and O'Donnell's work.

Entries in the legal literature have become far more numerous in the last few years, particularly following the growth of policy-focused literature after 2007. Some of the strongest examples include Schmitt's return to the topic, and the entry of other, established scholars of international law such as Oona Hathaway into these reinvigorated debates.[80] These more-recent works are notable for overcoming some of the technological aging and topical meandering of works from the early 2000s, though they rely on largely the same cast of scholars and baseline international law as the prior period. What even these present-day legal works lack, however, are any conclusions about the international legality of the general practice of a cyberattack, or how legality might shape international practice. Instead, most focus either on defining areas for legal consideration, or offering recommendations on how states

[78] Michael Schmitt and Brian O'Donnell, eds., *Computer Network Attack and International Law* (Newport, RI: Naval War College, 2002).

[79] See, e.g., Charles J. Dunlap Jr., "Meeting the Challenge of Cyberterrorism," in *Computer Network Attack and International Law*, ed. Michael Schmitt and Brian O'Donnell (Newport, RI: Naval War College, 2002).

[80] Michael Schmitt, "Cyber Operations and the Jus in Bello: Key Issues," *Naval War College International Law Studies* (2011); Oona Hathaway and Rebecca Croontof, "The Law of Cyber-Attack," *California Law Review*, no. 817 (2012); Herbert Lin, "Cyber Conflict and International Humanitarian Law," *International Review of the Red Cross* 94, no. 886 (2013).

might conduct 'legal' cyberattacks. Indeed, the most recent effort in this space, the *Tallinn Manual* released at the time of writing, is a project designed to provide guidance on the legality of specific cyberattack tactics.[81] In this respect, it offers an important contribution to the overall effort to bring cyberattacks under some international regulation, but begins its analysis from the premise that cyberattacks will be unrestrained, but for specific recommendations of law.

Situating This Study

This study is informed by each of these broad categories of literature, but maintains a distinct orientation and approach, situating cyberattacks within the broader discipline of international relations. Where prior works have focused on explaining to militaries or to policymakers what present-day cyberattacks mean to their efforts, or defining for them the specific parameters of lawful cyberattack tactics, the chapters that follow examine an expansive field of influences on state behavior relative to cyberattacks. Also distinguishing this study is its general applicability to international relations. This analysis is not specific to any one country, its policymakers, or even the present state of technology. Rather, this study contributes to the existing literature an assessment of the variety of forces of restraint in international relations, and the applicability and impact of each on state behavior. Even those approaches most recognizable within international relations, such as Nye's chapter on 'cyber-power' in his 2011 volume, and Schmitt's two articles concluding the need for a more comprehensive normative (*vice* strictly legal) framework to

[81] Michael Schmitt, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge: Cambridge University Press, 2013).

restrain cyberattacks, do not compare multiple forces of restraint, and none have employed a systematically analogical methodology described below.[82] Relative to the existing literature then, this study explores cyberattacks with the stated intent of seeking their restraint, critically evaluating rather than attempting to shape state policies, and does so in the context of existing international regimes and prior international efforts.

1.4 Methodology & Sources

Methodology

Cyberattacks are a new phenomenon in international relations, lacking any specific international regimes devoted to them, and few customs governing their use. Methodologically, the subject of this study is a phenomenon so novel it presents two challenges: the lack of applicable precedent that precludes a focus on case studies and rapid technological changes that could render analysis quickly obsolete. Moreover, with little public material available on how states are arriving at even preliminary decisions regarding cyberattacks and cyber-defense, a process-tracing approach would also be analytically unsatisfying and difficult given its retrospective orientation.[83] Alternative, explicitly predictive approaches run the obvious risk of speculation. They are also ill-suited to a study that, despite its potential implications for future

[82] Nye, *The Future of Power*, Chapter 5; Michael Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1999); "Cyber Operations and the Jus in Bello: Key Issues."

[83] See: Stephen Van Evera, *Guide to Methods for Students of Political Science* (Ithaca: Cornell University Press, 1997), 64.

state practice, probes the applicability of *existing* regimes and practices of restraint to a new phenomenon.

Given these considerations, this study pursues a methodology based on systematic analogy. It elucidates a novel phenomenon by reference to the methods of restraint already in operation in international relations, informed by prior example of those means of coercion (especially weapons) towards which states do presently show restraint. Specifically, each chapter represents a different line of inquiry into how the forces that restrain state behavior might operate on cyberattacks. To do so, it begins by defining both the essential features on which that force acts and the conditions necessary for it to obtain and effectively constrain state behavior. It then examines both the essential qualities of a cyberattack, and of a range of other weapons throughout history on which the force has had effect. The conclusion of each analysis is whether that force in international relations is meaningful in influencing states' decision-making in the choice to conduct a cyberattack.

In so doing, it follows in a robust tradition of analogical reasoning across the physical and social sciences, as well as philosophy and political theory. Analogical method is bound up in its purpose; to understand novel phenomena requires contextualization, connecting the old and familiar. Such was the approach often employed by Plato, where fundamental philosophical phenomena are not intuitively explainable but by reference to more intuitively understood concepts (in this case, those more common to daily experience).[84]

[84] Plato's three most famous analogies, the Form of the Good, the Divided Line, and the Allegory of the Cave, all appear in *The Republic*. Plato, *The Republic*, trans. Francis MacDonald Cornford (Oxford: Oxford University Press, 1964), 217-35.

The adoption of this approach by the physical sciences with respect to novel phenomena offers a detailed and relevant methodology. Mary Hesse's ground-breaking 1963 work on models and analogies in science recognized that novel phenomena often elude existing explanatory theory — specifically, a 'model' in which to situate them. In these instances, Hesse argues for an explicitly analogical approach with two phases: first, developing a list of observable qualities or 'predicates' of a phenomenon and second, of the causal relations they instantiate.[85] By bridging essential qualities of old and new, an analogical approach contextualizes novel phenomena and tests the durability of existing models and systems.[86] The approach here, examining the relationship between certain emblematic qualities of a phenomenon and the system in which it exists approximates Hesse's predicate-relational effect.

Elsewhere in international relations, practical philosophers have also adopted variants of this approach, though primarily as a means to evaluate a philosophical system, rather than to evaluate the fit between the action and various systems. A notable example in the discipline is Michael Walzer's *Just and Unjust Wars*, which in a manner highly recognizable within this study, illustrates the boundaries of a given philosophical system through historical example.[87] For the purposes herein, the term 'analogical reasoning' is preferable to 'historical illustrations' due to the dynamism of

[85] Mary B. Hesse, *Models and Analogies in Science* (London: Sheed & Ward, 1963), Ch. 2.

[86] Max Black further emphasized this interface, noting the ability of this kind of associative reasoning to lend conditions of meaning otherwise impossible by the two subjects independently. See: Max Black, "More About Metaphor," in *Metaphor and Thought*, ed. Andrew Ortony (Cambridge: Cambridge University Press, 1979), 28. See, more generally: *Models and Metaphors* (Ithaca: Cornell University Press, 1962).

[87] Michael Walzer, *Just and Unjust Wars*, 4th ed. (New York: Basic Books, 1977).

some of the norms under discussion, and to avoid the presumption this study was fixed around certain historical cyberattacks.

The methodology I employ is not without challenges. Analogical reasoning's focus on similarities between two phenomena can run the risk of obscuring more profound distinction. This issue is partly mitigated by drawing comparison not just between similar qualities of a proscribed act and a cyberattack, but also between the *effects* of that force of proscription on both. I also endeavor to pay regular attention to qualities of cyberattacks that are truly 'unique' or might undermine the effect of a restraining regime itself, as exists in a few important cases. A second challenge comes in reference to choices made by states, since this approach can also be abused and lead to jettisoning context from a complex set of decisions that influenced particular outcomes, assuming single-factor causation in a multivariate environment. It is for that reason that this study does not rely on any single analogy, or orient itself by extended parallel to any single interstate act (say, a blockade), but rather offers a range of examples across different tactics, technologies, and timeframes. Finally, the predicate need of an analogical approach to define essential qualities of a technological act also creates exposure to obsolescence. This risk is inevitable with any work dealing with high technology, but I accept it as preferable to fixation on particular and imperfect case studies, which would only exacerbate this and the prior two concerns.

Sources

The background knowledge informing this dissertation was developed over my last several years in the field, beginning with the research for the M.Phil. thesis that provided the foundation of this study, and subsequently as a practitioner with the U.S. Department of State and White House. That work was supplemented by attending and delivering papers at dozens of conferences, international symposia, and think-tank discussions integrating government and private sector views on these issues. Additionally, I conducted a series of interviews — carried out independent of any official capacity — on some of the doctrinal and policy questions I address throughout the study. Given that context, it is worth reiterating that the arguments and conclusions in this study are my own, and reflect neither the policy nor preference of any one state, government, or institution.

With respect to formal sourcing, the primary material for this study is, in all instances, drawn from publicly available documents. The first category of sources pertains to recent state activities in cyberspace. Given their contemporary nature, the only historical record comes from newspaper and technical press accounts, which I reference to provide some factual basis for certain key historical events. Supplementing these accounts, the best in-depth data on cyberattack incidents and capabilities come from the reports of technical cybersecurity firms, many of which have invested hundreds of millions of dollars in observing malicious activity online. While some such firms are noted for lacking objectivity, those reports referenced herein are generally regarded among technical and cybersecurity experts as neutral in their presentation.

With the exception of the events of Estonia and to a lesser extent, *Stuxnet*, states have rarely commented on specific cybersecurity incidents in which other states are the suspected perpetrators; as a result, the most meaningful documentation of their positions are more general in nature. Recent years have offered numerous opportunities to observe those reactions: in the United Nations context, they include the construction of annual General Assembly resolutions and the state views the solicit; in negotiations of Groups of Governmental Experts from key players in international security; and in statements of senior officials during U.N.-sponsored events, like the Internet Governance Forum. Third-party venues, some with thinly veiled state sponsorship, also offer important venues for states to articulate their positions on the issue of cyberattacks. In recent years, the London Conference on Cyberspace in 2011 and its successor events in Budapest and Seoul, as well as the annual cybersecurity forum in Garmisch-Partenkirchen, were among the most significant.

Some governments with histories of advocacy in this space have also issued comprehensive documents that provide core documentary evidence of their views. The United States, Australia, United Kingdom, and Russia have produced the greatest number of these documents in the form of military whitepapers and doctrine statements, foreign ministry proclamations, and whole-of-government (White House/Kremlin) cyberspace policies. Dozens of other states have also developed versions of these national strategies, though many focus primarily on domestic vulnerability and governance, and only a few contain sections devoted to international relations.[88] Finally, public bilateral and multilateral agreements between key powers and their allies also provide an important documentary basis for their evolving views.

[88] Particularly useful for a separate, comparative analysis of domestic policies outside the scope of this study, key examples include: Australia Attorney General's Department, *Cyber Security Strategy* (Canberra: 2009); Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa: 2010); Federal Chancellery of the Republic of Austria, *Austrian Cyber Security Strategy* (Vienna: 2013); Germany Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (Berlin: 2011); Finland Secretariat of the Security and Defence Committee, *Finland's Cyber Security Strategy* (Helsinki: 2013); France Agence Nationale de la Sécurité des Systèmes d'Information, *Information Systems Defence and Security: France's Strategy* (Paris: 2011); Japan Information Security Policy Council, *Information Security Strategy for Protecting the Nation* (Tokyo: 2010); Innovation & Employment Ministry of Business, New Zealand, *New Zealand's Cyber Security Strategy* (Wellington: 2011); Reform and Church Affairs Ministry of Government Administration, Norway, *Cyber Security Strategy for Norway* (Oslo: 2012); The Netherlands National Coordinator for Security and Counterterrorism, *National Cyber Security Strategy 2: From Awareness to Capability* (The Hague: 2013); Civil Protection and Sport DDPS Federal Department of Defence, Switzerland, *National Strategy for the Protection of Switzerland against Cyber Risks* (Bern: 2012); Internal Security

Each chapter also has a literature specific to its line of inquiry. Chapter 2's examination of rationalist deterrence is the most straightforward. Absent any formal governing document, the section draws on the rich academic and historical debate about the origin and function of deterrence before, during, and after the Cold War. Chapter 3, which focuses on restraints on the use of force within international law, uses the U.N. Charter as its cornerstone and develops its analysis through key rulings of the International Court of Justice (ICJ) and scholarship on them. Chapter 4 examines the numerous documents that comprise *jus in bello* canon of law, including the Hague and Geneva canons of law, laying their development against the historical record on how, when, and to what end various means and methods of war were deemed 'unusable.' As examples, it draws upon the legal literature on the formation of specific legal regimes against chemical weapons, land mines, and cluster munitions. Finally, the conclusion relies upon the specialized literature within international relations tracing the processes of norm formation to consider the pathways by which a 'cyberattack taboo' might form.

1.5 Outline of Argument

The disruptive and destructive potential of cyberattacks make them powerful and — on some level — potentially transformative instruments of interstate coercion. But, as this study argues, it will not and need not necessarily be so. Several discrete forces in international relations have throughout history restrained states' recourse to

Agency Ministry of Administration and Digitisation, Poland, *Cyberspace Protection Policy of the Republic of Poland* (Warsaw: 2013); Maritime Affairs and Communications Ministry of Transport, Turkey, *National Cyber Security Strategy and 2013-2014 Action Plan* (Ankara: 2013).

force or particular means and methods of war. For instance, familiar fears of retribution might inhibit their use. So too might a regime of international law designed to punish derogation. Finally, states might fear violating international laws against which they are judged by others, or represent a certain baseline of just conduct. All three of these distinct forces — so-called ‘logics of restraint’ — differently influence state choices to use certain capabilities at their disposal. Each has the potential to exercise a powerful force in shaping state’s use and non-use decisions. The argument of this study is that embedded within these logics of restraint are particular conditions essential for them to obtain and have effect, and that cyberattacks meet many of those conditions. The conclusion is not that any single logic will automatically bring restraint to states’ use of cyberattacks, but all are meaningfully relevant, and some are particularly powerful in that effort. The outline of each of the following chapters is as follows:

In Chapter 2, I examine the role conventional deterrence could play in restraining state use of cyberattacks. The chapter begins explaining the rationalist model of state decision-making in terms of perceived gain and loss, and then disaggregates the concept of deterrence to identify what key pieces of information states require for a deterrent relationship to obtain. I argue that cyberattacks’ unique features frustrate conventional deterrence models, denying states the information to make rational calculations, and leaving cyberattacks’ status within international custom deeply unsettled. The chapter then seeks to explain why, if these tools are poor at ‘keeping the peace,’ states are amassing these capabilities and broadcasting this accretion. By adding a dimension to the traditional rationalist view, I argue this behavior is explainable as a process of *structural deterrence*, in which states are seeking to influence whether and how states can respond militarily to a cyberattack, thus influencing the overall deterrence value of such tools.

Chapter 3 turns to regulative norms in international relations, specifically the restraining effect of the *jus ad bellum* canon of international law limiting the recourse to force. It begins by outlining the existing, general prohibition on the "use of force" outlined by the U.N. Charter's Article 2(4), then examines whether and how cyberattacks might be proscribed under that regime. I argue that despite the apparent difference between a cyberattack and conventional arms, cyberattacks appear to qualify as military instruments, and there is a more than ample basis to consider them presumptively illegal under both Article 2(4) and several other articles of the Charter. To conclude analysis of the *jus ad bellum*'s restraining effect, the chapter then examines the prospects for cyberattacks activating that remedial regime, namely states' rights of self-defense under the U.N. Charter's Articles 39 and 51. It argues that despite numerous controversies in the scholarship surrounding self-defense, there exists a strong basis for the claim that a state subject to cyberattack has an inherent right to repel it with force. Ultimately, this regime is promising but nascent, demanding a state to deploy repellent force to a cyberattack to establish its customary operation on this particular tool.

Chapter 4 examines the effect the *jus in bello,* or law governing just conduct in war, might have in restraining states' security choices. This chapter begins with the observation that states have claimed curiously little credit for acts of cyberspace coercion, and considers whether it may be out of concern they violate this powerful force of international law. To test whether such a concern is valid, the core of this chapter begins as the last: examining whether cyberattacks might run afoul of the existing, general legal regime requiring that attacks be proportional and discriminate between civilian and military objects. I argue that there is substantial basis that cyberattacks violate these principles, and in many instances no less so than weapons that have been formally proscribed by the international community. The result may be the basis for a 'cyberattack taboo,' but one that would be too early to trace.

The conclusion draws this analysis together to consider the prospects for restraining state use of cyberattacks, considers some preliminary pathways a norm against cyberattacks might take, and proposes several areas for further study.

Chapter 2:

Cyberattacks and Deterrence

TABLE OF CONTENTS

Of the many reasons a state might restrain its development, deployment, or use of cyberattacks, perhaps the most basic is if doing so brought more risk than reward. This calculation is at the core of rationalist views of international relations and, in turn, the forces of deterrence and dissuasion. Beginning with this familiar frame, this chapter evaluates the potential 'pull' value of acquiring cyberattack capabilities, and the retributive 'push' that might serve as a disincentive to acquiring or using them.

States may seek to acquire certain capabilities as much for their value in keeping the peace as their value in war, reflecting a quality of those capabilities commonly referred to as 'deterrent value.' States may also acquire and demonstrate capabilities with the hopes of preventing an adversary from acquiring or using a particular military capability against it. If successful, the first state is said to have 'deterred' its adversary. Because it holds the potential on the positive side to shape behavior without overt conflict, and perhaps even stabilize tumultuous interstate relationships, deterrence is one of the more powerful forces in international relations.

Given cyberattacks' attractiveness in affording asymmetrical power, is it inevitable that more states will seek to acquire them? Does the potential for a destructive cyberattack make developing those capabilities a strong deterrent (and thus desirable to states seeking to maximize security)? Might it be impossible to deter a state from developing a capability that can be amassed so covertly, thus increasing further the incentives to acquire? In this framing, cyberattacks might proliferate unchecked.

Setting aside the hype related to cyberattacks, one might contrarily ask: do cyberattacks provide real value to the average state seeking to improve its lot in international security? Or are they 'niche' weapons that only a handful will find worth the effort? Is their utility limited to an attack, and at that, one that is largely unrepeatable? And might cyberattacks be kept in check by other states possessing similar capabilities, similar to the mutual deterrence that characterized the Cold War superpowers? Here then, and perhaps counter-intuitively, cyberattacks might not be crucial to the vast majority of states, or might even play a role in keeping the peace.

The answers rest on two fundamental questions that undergird the chapter: whether or not cyberattacks are effective at deterring aggression, and whether they in turn can be meaningfully deterred. Respectively, these questions define the ‘pull towards’ and ‘push against’ acquiring cyberattack capabilities. Understanding whether cyberattack capabilities have deterrent value, and whether states can be deterred from acquiring and using them, provides a rationalist means to explain their uptake among states, or restraint therefrom. If their deterrent value is high, the likelihood that more states will actively seek and acquire them is as well. However, if their deterrent value is low, the reward that accompanies having the capability is substantially depreciated. Likewise, if a state can be easily deterred from acquiring or using them, their value might decline — but, alternatively, if the best way to counter a cyberattack is with another, those capabilities may proliferate even further.

Outline of Argument

This chapter examines the role of deterrence in restraining state use of cyberattacks, both as a general matter and in light of present state practice. It is oriented around three key questions: in seeking to restrain state use of cyberattacks, (1) might states self-restrain if cyberattacks are of limited deterrent value; (2) might states be deterred from acquiring or using cyberattack capabilities by other states doing the same; and (3) might states be deterred from acquiring or using them by other states’ more traditional capabilities?

As the introduction outlined, cyberattacks can be recognizably destructive, but also possess unique characteristics that distinguish them from other aggressive acts. So how does a state deter something that it cannot easily count; that cannot be observed with the naked eye, traditional surveillance, or reconnaissance; and whose effects vary dramatically based on the level of technology in a victim state?

This chapter argues that cyberattacks in and of themselves deprive states of the ability to make meaningful rationalist calculations, rendering those capabilities poor deterrents, but also difficult to deter. Consequently, restraining cyberattacks requires more than simply amassing greater, similar capabilities in the manner of most conventional and nuclear deterrence. Instead, this chapter argues that a different and novel strategy is both necessary and already in use: a strategy of *structural deterrence*, shaping the international environment through alliances and law to favor their strengths within an overall deterrence relationship. In short, we are presently observing a form of 'cyber-deterrence,' but not of the sort upon which military literature narrowly focuses. Rather, the contest in which states are presently engaged to restrain one another's use of cyberattacks is one of rationalist dissuasion through neoliberal means.

In detail, the chapter's argument is as follows. An introductory section defines the notion of deterrence and situates it within the theories of international relations into which it features prominently. The chapter then argues four key points to address these questions. First, it outlines the general criteria required for states to make rational deterrence calculations. Second, laid against those criteria, it argues that cyberattack capabilities meet very few of them given the complex aspects of observing and attributing them, making them poor instruments of deterrence. Third, it argues that there are substantial difficulties in deterring cyberattacks with other cyberattack capabilities (in-kind deterrence), but that — like any other aggressive acts — states might be effectively deterred from using them in other ways (most obviously threat of military reprisal). The credibility of that threat of military reprisal is, I argue, presently contested, leaving states unable to amass the information necessary to make full, rationalist deterrence calculations. Therefore fourth, the chapter argues that in order to shift the deterrent balance in their favor, states are engaging in an unconventional form of competition that I call 'structural deterrence.' In exercising structural deterrence, states seek to shift deterrence calculations by shifting the context of their use — competing not directly for capabilities, but indirectly over cyberattacks' institutional and legal status, in order to invite or deny the use of conventional militaries against them. The chapter concludes by recognizing that far more than rationalist calculations will determine whether cyberattacks can be restrained, even in a mode conventionally referred to as 'rationalist deterrence.'

2.1 Defining Rationalist Deterrence

Situating Deterrence: Concept and Theory

The most accessible, intuitive logic of restraint in interstate conduct is that of *rationalist deterrence.*[1]

Rationalism, or rational choice theory, is a straightforward way of explaining state choices: simply, that state's decisions are based fundamentally on expectations of gain and loss. Formally, a rationalist calculation for a given state action is straightforward: expected gain minus expected loss provides a positive or negative sum. If positive, the action is undertaken, if negative, it is not. This concept is made

[1] As a broad concept in today's literature, rationalist deterrence incorporates two means of affecting adversary choices: the *deterrent* influence of expected retaliation, and the *dissuasive* influence of limited impact/inexpensive recovery. If an attacker were dissuaded from an attack based on an adversary's rapid and inexpensive reconstitution from it, it would not have significant national security effect, and would not be of much relevance to this analysis. Therefore, this concept is largely excluded in the section.

complex (and meaningful in international relations) by problematizing the ‘currency’ of gain and loss — the premise upon which the principal theories of the discipline diverge, and which will be discussed shortly. In the interim however, it is most important to keep in mind this basic rationalist calculation of gain and loss informing decisions to act.

As it was generally understood before and throughout its intellectual heyday during the Cold War, deterrence is — at its core — a rationalist concept. From the standpoint of a would-be aggressor, it explains a condition when the expected loss of a coercive act outweighs the expected gain due to certain anticipated actions or known attributes of the intended victim. A state that carries out an act of coercion is by definition undeterred, implying that its perceptions of relative loss were outstripped by perceptions of gain. Such was the case, for instance, in the United States’ decision to enter the region and repel Iraq during the 1990-1991 Gulf War (the United States was, correctly, undeterred by Saddam Hussein’s army).[2] Likewise, in its far more legally complex strike on a Syrian nuclear reactor in 2007, Israel was undeterred by the likelihood of Syrian air defenses (dissuasion) or counterattack (deterrence).[3] By contrast, a state is effectively deterred when it refuses to take an aggressive action that might otherwise bring it immediate or precedential gain: for instance, both Hussein’s Iraq and Assad’s Syria were deterred from waging a direct counter-attack on their

[2] This example is not to be confused with the more comprehensive point about a shift in U.S. foreign policy that Lawrence Freedman aptly observes regarding the American invasion of Iraq in 2003, where the paradigm of that country’s strategy markedly shifted away from deterrence and towards a pre-emptive doctrine. See: Lawrence Freedman, *Deterrence* (Cambridge: Polity, 2004), 4, 96-105.

[3] See: Erich Follath and Holger Stark, "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Speigel Online International*, 2 November 2009. For a more technical discussion, see: Fulghum, "Israel Used Electronic Attack in Air Strike against Syrian Mystery Target," *Aviation Week,* 8 October 2007 See also: David A. Fulghum, Amy Butler, and Sally Adee, "Cyber-Combat's First Shot," *ibid*., 26 November 2007.

aggressors' territory. Both India and Pakistan, despite over a decade of small-scale war across their border, have mutually deterred one another from both broader outbreak of conflict and the use of nuclear weapons they both possess. Deterrence can describe such monumental security choices as going to war, or more limited ones such as selection of a response to a diplomatic or political slight. The concept is, however, at its clearest in decisions for and against coercion that might reasonably lead to the outbreak of hostilities — a category into which cyberattacks clearly fall.

From the standpoint of more systemic international relations theory, this notion of rational choice is also the basis for *realist* explanatory theories of state action, such as the one popularized by Hans Morgenthau.[4] In this systematic arrangement, as Morgenthau puts it, "politics, like society in general, is governed by objective laws that have their roots in human nature," and that the "main signpost that helps political realism to find its way through the landscape of international politics is the concept of interest defined in terms of power."[5] In these general theories of international relations, the referent object of 'gain' or 'loss' is dynamic: it might be territory, natural resources, valuable populations, or military hardware. But if those qualities of gain and loss are calculated in an abstract zero-sum concept of interstate 'power,' that concept is fixed around international security choices like whether and when to attack one another, and more contemporary international relations theorists systematize those state choices as 'neorealism.'[6] Both of these schools take states as

[4] Hans J. Morgenthau, *Politics among Nations: The Struggle for Power and Peace*, 5th ed. (New York: Knopf).

[5] *Ibid.*, 4-5.

[6] See, most famously: Kenneth N. Waltz, *Theory of International Politics*, Reprint ed. (New York: Waveland, 2010 (first published 1979)).

the primary actor in the international system, and in turn accept two fundamental attributes about them: that they are rational egoists (i.e. interest maximizers in the utilitarian sense); and that that they are prone to conflict (most readings of Waltz suggest almost a Hobbesian state of nature or "*bellum omnium contra omnes*").[7] In reviewing various logics of restraint then, from the rationalist vantage of international relations, deterrence has substantial explanatory value, as it acts to restrain states by the finite and limited capacity for gain from those conflicts. In a rationalist mode the most meaningful check on states using every means of coercion at their disposal is the potential for relative loss — unless they are, in other words, deterred.

Deterrence is also an important *practical* force in the realist mode of international relations; it is, in many ways, a particularly resource-efficient way to project power. Consider that to directly coerce an opponent, a state must first incur the material cost of acquiring that weapon, then material and reputational costs of using it, then the costs of any retributive consequence from so-doing (e.g. a counterattack). If, however, the mere investment in that capability carried with it the ability to avert attack *and* coerce by threat, the cost of deterring is far less than the cost of using. Therefore as a strategy, deterring has its appeal to both potential aggressor (because it is cheaper) and defender (because it reduces the chances of being victimized).

Mutual deterrence should not be confused with stability. A kind of post-Cold War celebratory amnesia seems to have gripped contemporary accounts of how the two superpowers averted conflict, but in so doing, obscured that mutual deterrence is

[7] Variously translated as a 'war of all against all,' or 'of every man versus every man.' Thomas Hobbes, *Leviathan (with Selected Variants from the Latin Edition of 1668)*, ed. Edwin Curley (Indianapolis, IN: Hackett, 1994 (first published 1668)), 76.

not a harmonious condition. While the United States and the Soviet Union deterred one another and successfully avoided outright full-scale conflict during the Cold War, those decades were hugely expensive, the peace fragile, and outbreak of humanitarianly disastrous 'side' conflicts numerous. Nonetheless, deterrent effects quite indisputably played an important role in restraining the use of (at the very least) nuclear weapons in the mid-to-early Cold War, and for similar reasons, those effects are worth studying in the context of cyberattacks as well.[8]

It is undeniable that deterrence can be both effective at restraining a state's use of particular capabilities, and may offer a resource-efficient way to do so. Given that potential, the balance of this section more carefully defines what conditions are necessary for a deterrent situation to take shape, and to lay the foundation for the next section's analysis of how cyberattacks fit within (and in some cases challenge) that basic dynamic.

Narrowing the Concept of Deterrence

Before examining the compatibility of deterrence to cyberattacks, it is important to note that deterrence describes not a unitary concept, but a plurality of concepts once hotly debated, though admittedly less so with the waning of the Cold

[8] Tannenwald makes a compelling case, examined in the final section of this study, that normative effects played at least as important a role in the decisions not to use nuclear weapons during the mid-to-late Cold War, and on the American side, in earlier spats like the Quemoy-Matsu crisis and Korean War. Nonetheless, her examination is limited to American calculations (not Soviet decision-making), and arguments are strongest when they relate to the later period in which the norm she defines has taken stronger root. Particularly given the power-dynamics and decision-making of the Soviet military in the post-WWII era, it seems impossible to discount the role of rationalist calculations and mutual deterrence in preventing both the outbreak of generalized conflict and, inextricably, the use of nuclear weapons. See: Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945* (Cambridge: Cambridge University Press, 2007).

War.[9] Most systemic views on interstate deterrence share an orientation around the state and a basic understanding of rational egoism. For the time being, this chapter's analysis accepts that framing as well. Beyond that, however, there are multiple definitions of deterrence at varying levels of political and temporal specificity; this section narrows the field to the specific type of deterrence relevant to this study, and outlines the recognizable features thereof.

With respect to the political scope or kind of activity being restrained, perhaps the broadest condition would be the one described by George and Smoke, who regard deterrence as "persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits."[10] Mearsheimer offers a similar view, regarding deterrence "in its broadest sense" to be "persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks."[11] Mueller marginally narrows the reference sphere of influence to the military space, but implies an almost Hobbesian realism, noting that given "the absence of war between two countries…it is reasonable to conclude that each is

[9] Central works shaping in this debate include: Bernard Brodie, *Strategy in the Missile Age* (Princeton, NJ: Princeton University Press, 1959); Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960); Glynn Snyder, *Deterrence and Defense: Towards a Theory of National Security* (Princeton, NJ: Princeton University Press, 1961); Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966); George Questor, *Deterrence before Hiroshima* (New York: John Wiley, 1966); Stephen Maxwell, *Rationality in Deterrence*, vol. 50, Adelphi Papers (London: International Institute of Strategic Studies, 1968); Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974); Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976); "Deterrence Theory Reconsidered," *World Politics* 39 (1979); Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: St. Martin's Press, 1981); George Questor, *The Future of Nuclear Deterrence* (Lexington, MA: Lexington Books, 1986); Richard Ned Lebow and Janice Gross Stein, "Rational Deterrence Theory: I Think, Therefore I Deter," *World Politics* 41, no. 2 (1989); Robert Powell, *Nuclear Deterrence Theory: The Search for Credibility* (Cambridge: Cambridge University Press, 1990); Patrick Morgan, *Deterrence Now* (Cambridge: Cambridge University Press, 2003); Freedman, *Deterrence*.

[10] George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice*, 11.

[11] John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983), 14.

currently being deterred from attacking the other."[12] In Mueller's definition, any non-war condition is a function of deterrence — defensible but (as Morgan notes) also "not rewarding analytically" for purposes such as this study of a specific kind of disruptive and potentially destructive attack.[13]

Looking back historically, early Cold War literature offers a more precise concept related to military aggression, and one that seems more properly tailored to the purposes here. Glenn Snyder's seminal work, for instance, defines deterrence as "discouraging the enemy from taking military action by posing for him the prospect of cost and risk outweighing the prospective gain."[14] Such a definition, favored by contemporary deterrence theorists like Morgan, also seems to have the best durability in the practical literature.[15] Thus, the U.S. Department of Defense's Dictionary defines deterrence as "The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction."[16]

Having limited the kind of deterrence under discussion to activity known to be coercive, if not overtly military in character, it is also worth defining the timescale of deterrence under discussion. If deterrence informs a would-be attacker's decision

[12] John Mueller, *Retreat from Doomsday: The Obsolescence of Major War* (New York: Basic Books), 70.

[13] Morgan, *Deterrence Now*, 2.

[14] Snyder, *Deterrence and Defense: Towards a Theory of National Security*, 35.

[15] Yet another, 'compellence,' focuses on the use of threat to get another party to engage in positive activity it otherwise would not. Morgan refers to deterrence and compellence in concert as "coercive diplomacy" — a compelling concept, but one that conceptually strays beyond the direct focus of this study. For a comparison, see: Morgan, *Deterrence Now*, 3. For an in-depth treatment, see: Lawrence Freedman, ed. *Strategic Coercion: Concepts and Cases* (Oxford: Oxford University Press, 1998).

[16] United States Joint Chiefs of Staff, *Jp1-02: Department of Defense Dictionary of Military and Associated Terms* (Washington: U.S. Department of Defense, 2001).

space and, when successful, results in forbearance, one can envision this force acting across two general timescales. In the first, relations between a dyad of states are such that “at least one would consider attacking if a suitable occasion arose,” and in which “the other maintains forces and offers warnings” such that “the first party never goes beyond preliminary consideration of attacking because of the threat from the second party.”[17] This is deterrence played out on a long timescale, a concept that Huth and Russett note (and Morgan argues) is “among the most important and least systematically studied phenomena of international politics.”[18] This is *general deterrence*, and it refers to a particular interstate condition of conflict or non-conflict, rather than use of a particular opportunity. It is a kind of overarching deterrence *theory,* having “to do with anticipating possible or potential threats, often hypothetical and from an unspecified attacker, and adopting a posture designed to deter other actors form ever beginning to think about launching an attack” — of any kind.[19] It is not necessarily tied to a specific challenge, to a single assessment of capabilities, and is thus far more prone to include considerations broader than simply retributive capability. It is, for that reason, not methodologically ideal to frame a study focused on the decision set related to a specific method of coercion, in this case a cyberattack.

Focus on a larger timescale is important to avoiding the practical shortcomings, and concomitant criticism leveled against the subfield of general deterrence. General deterrence’s utility, at least in the form it dominated international relations analysis in the 1970s and 1980s has come under criticism for disconnection

[17] Morgan, *Deterrence Now*, 80.

[18] Paul Huth and Bruce Russett, "General Deterrence between Enduring Rivals: Testing Three Competing Models," *American Political Science Review* 87, no. 1 (1993).

[19] Morgan, *Deterrence Now*, xvi.

from the practice of states.[20] As Kissinger laments, "the nuclear age turned strategy into deterrence, and deterrence into an esoteric intellectual exercise," in other words, that the study of war's potential outbreak seemed almost detached from the geopolitical realities and even a broader security context.[21] This study instead focuses on a narrower concept and timescale. In studying one particular aggressive act, as this study does, a tauter focus on single-point security decisions rather than entire bilateral security dynamic in a relational context is both more rigorous and more conclusive.

Instead, the notion of *immediate deterrence* is more relevant to a study focused on the use/non-use of a particular method of coercion.[22] Best defined retrospectively but helpfully by Morgan in his review of the discipline's many strains, immediate deterrence relates to the circumstances of preparation for/reaction to *impending* attack by a known adversary — "linked to specific military capabilities and the threats built on them," rather than "overall military posture and the broad image it conveys."[23] When describing the relationship between potential (e.g. nuclear) adversaries, the immediate deterrent relationship focuses primarily on pre-conditioned markers of behavior and known prospects of retaliation. The difference might be considered thusly: the mutual success of immediate deterrence is more a

[20] Freedman (2004) takes perhaps less umbrage with the prior era's analytical approach, but challenges the same orthodoxy by demonstrating a coherent norms-based approach to understanding of deterrence. Sharing those concerns about the limitations of a purely interest-based approach, the chapter will examine a more norms-focused approach to deterrence in the final two sections. Freedman, *Deterrence*.

[21] Henry Kissinger, *Diplomacy* (New York: Simon and Schuster, 1994), 208.

[22] Patrick Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, CA: Sage Publications, 1997), 28.

[23] *Deterrence Now*, 81-5.

matter of survival, whereas the success of general deterrence might result in a state thriving.

For these purposes, immediate deterrence refers to the particular use/non-use choices to engage in particular kinds of coercion; likewise, it refers to a particular decision set. Distinctly, general deterrence refers in this study to the establishment of regularized deterrent situations across numerous immediate events, resulting in a more robust equilibrium. It can also be said, and is worth noting for future study, that general deterrence is the broader construct of habituated, predictable immediate deterrence episodes — but meaningful only in an historical, normative context beyond the framing of this chapter.

At present, an examination of only immediate deterrence is appropriate given the lack of habituation of states' use/non-use decisions vis-à-vis cyberattacks. Moreover, such an approach lends itself to more durable study and may perhaps serve as a useful starting point to other analyses of general cyber-deterrence when the phenomenon has more evidence in state practice.

General Features of Immediate Deterrence

Immediate deterrence, regardless of the particular coercive tactic in question, shares certain general requirements to obtain. This section traces those generic features, setting the stage for their application to cyberattacks.

Considering the dynamic between two states, would-be aggressor Asgard and defender Babel, Babel successfully deterring Asgard requires a number of factors be known to each. These might be called *preconditions* of immediate deterrence, since without any one, it would be impossible for one to successfully exert deterrent influence over the other.

The first preconditions, worth mentioning only briefly, are strictly relational. In a bilateral dynamic, Babel must believe or know that Asgard, or a similarly positioned actor, poses a threat to it — in essence, a reason to pursue a strategy of deterrence. If that threat is imagined but not real, Babel might pursue such a strategy, but any success the former attributes to it would be irrelevant and misleading to precedent. Thus, this chapter takes as basic premises that Asgard and Babel are geopolitical foes in which the former perceives material gain from an attack on the latter, and that Babel recognizes the potential for Asgard to do it harm. Thus, actions and reactions in immediate deterrence are based thereupon, rather than grounded in misperception or utter anomaly.[24]

With those basic premises in mind, the most analytically important preconditions are *recognition* (of a weapon) and *attribution* (of its owner/controller).

Recognition. In assessing the decision to attack, Asgard must first be able to *recognize* the material (presumably military) forces that Babel might bring against it in the event of aggression. Recognition, in turn, has two constituent factors: *instrument recognition* and *effect recognition*. The first is an act of identification: literally, knowing upon observation the weaponry that might be deployed in retaliation to an attack. The second is an act of contextualization*:* knowing how the deployment of those retaliatory forces would adversely impact the attacking state.

Instrument recognition has taken many forms throughout the years, usually via what we now call reconnaissance. It has been aided by factors like night-vision,

[24] Misperception can in some security contexts be worthy of analysis for its spiraling of bilateral/multilateral deterrent relationships, but principally in the mode of general rather than immediate deterrence, and thus not appropriate for these purposes. A template for that separate study might begin with: Jervis, *Perception and Misperception in International Politics*, 67-82.

thermal imaging, and satellite observation. It has been obscured by covert development, as well as by deception tactics as simple as canopies over inactive fighters, or as sophisticated as the hundred-mile network of underground tunnels connecting various fortified installations underneath Pyongyang.[25] In each case though, forces were in some way (either directly, or via the plans leading to their manufacture), *observable* to the would-be aggressor. Were they not, they would serve only coercive, rather than deterrent effect, and thus would be of utility only during the outbreak of conflict itself.

Effect recognition, by contrast, is an understanding of the likely damage that deployment of the aforementioned instrument(s) would incur. The two are related but distinct. A landlocked country might be far less deterred when recognizing a massive naval fleet belonging to its adversary. Thus instrument informs, but does not dictate, effect. Even with less obvious examples, it would be tempting but incorrect to assume that many categories of weaponry render this distinction between instrument and effect meaningless. A nuclear blast is a devastating occurrence, but not in all circumstances a state-terminating one.[26] As strategic literature developed during the Cold War pointed out, even the deployment of a half-dozen nuclear weapons was viewed as a differently 'survivable' situation for the Eastern seaboard of the United

[25] Bradley K. Martin, *Under the Loving Care of the Fatherly Leader: North Korea and the Kim Dynasty* (New York: St. Martin's Griffin, 2004), 85, 563.

[26] This is not to say that nuclear weapons did not take on the reputation for such a consequence in the popular and military consciousness — an issue Chapter 4 will explore in the context of international law governing the conduct of war.

States and Western half of the Soviet Union — particularly given different population densities between the two.[27]

So a crucial precursor to Babel deterring Asgard from an attack would be the latter's recognition of the weaponry the former might bring to bear, and its specific destructive effect should it do so.

Attribution. All of this is reasonably straightforward, so long as Babel's flag is neatly painted on the outside of every missile, rifle, and ship it possesses, and visible for Asgard to see. Thus particularly in a world of global power projection, where military capabilities might reside within the borders of allies or in international waters, the matter of attribution is crucial as well.

A would-be aggressor must be able to *attribute* material forces that might be brought to bear against it; in other words, Asgard must believe certain capabilities belong to Babel and not, say, Camelot. Knowing "whose guns are whose" is essential to assessing the loss likely to be incurred in any attack, and is rapidly made complex by global alliances and defense relations both overt and otherwise.

One or more of three methods can yield positive attribution: knowing identity; conducting elimination; and ascertaining monopoly. These are deductive qualities to knowing the possessor of a particular capability or perpetrator of a particular act. Identity answers the question of "who *did."* Elimination focuses on "who *therefore did not.*" Monopoly strives at "who *else* could." Conclusive evidence of the first renders the latter two moot, but for many capabilities, the calculation is not so simple.

[27] See, for example, the deterrence posture enshrined on the United States' Single Integrated Operations Plan (SIOP) developed in the early 1960s. McGeorge Bundy, *Danger and Survival: Choices About the Bomb in the First Fifty Years* (New York: Random House, 1988), 322.

This section will describe each in turn, given the relevance of all three in confronting a cyberattack.

Identity attribution can, even in international politics, take the form of a ‘smoking gun.’ A country’s uniformed soldiers, visible from their home territory in the direction of another’s, might be the simplest example. Likewise, a squadron of fighter jets on the tarmac at a known state airfield would, if visible from a satellite, provide relatively simple attribution in the form of identity.

Elimination can play an important role when identity is not obvious. The presence of a few grounded fighters in a contested region such as Kashmir might yield little specific knowledge of their attribution. Absent distinct markings (required under the *jus in bello* but not always visible) on the planes and knowledge of which country favors a particular landing site, identity might not be immediately obvious.[28] However a particular class of sophisticated fighter might only be used by one of the three claimants to the disputed region. Thus, as a logical matter, knowing that for instance China possesses a kind of jet that its neighbors Pakistan and India do not would provide semblance of attribution via elimination.

Monopoly helps further inform attribution in deterrence by answering whether a particular capability can be developed or deployed by additional actors beyond a classic deterrent dyad of two states. With respect to development, knowing whether a particular capability’s production, acquisition, and possession remains sufficiently complex, expansive, or risky as to remain the sole provenance of states can eliminate an entire layer of complexity in a deterrent relationship. Many of the most powerful,

[28] See Chapter 4 for an extended discussion of these *jus in bello* requirements and their potential effect on cyberattacks.

highly sophisticated military capabilities fall in this category: aircraft carriers, advanced jets, modern tanks, and (to date, thankfully and in all but the most marginal pre-deployment cases), the tools for nuclear and large-scale chemical weapon deployment.[29] Other capabilities, however, have proliferated substantially to non-state actors, including terrorists and organized crime — these include small arms, rocket-propelled grenades, small submarines/submersibles, and mid-size naval vessels. Thus, knowing that states maintain a development and/or deployment monopoly on a particular capability can help positively identify it as belonging to a would-be attacker or defender.[30]

These three general methods of attribution are important to some of the most complex and important conditions of immediate deterrence. Consider, for example, the question of attribution vis-à-vis an intercontinental ballistic missile (ICBM). Today, its in-flight attribution has become knowable thanks to sophisticated telemetry. It was not always so.[31] ICBMs offer a helpful illustration of both distinction and monopoly. Given that only two states possessed the weapons early in their advent, the Soviet Union could generally know that an incoming missile was not their own; therefore, by elimination attribution, any inbound ordnance of that sort was

[29] With very limited exceptions, individuals have played only an intermediary brokering role in states' acquisition of these capabilities, lacking the capability to deploy them directly. The A.Q. Khan network represents perhaps the most famous of this former category. Perhaps the most notable exception in the case of chemical weapons the Aum Shinrikyo cult's possession and use of chemical weapons in their 1995 Tokyo subway attack, though to reinforce the point, the group lacked any sophisticated deployment system for those weapons.

[30] Less salient for this study, but worth noting parenthetically, is the question of whether a capability is available to third parties; i.e. if a weapon developed and deployed by Asgard, aimed at Babel, might be used by Camelot without the others' express permission. Such a capability might then be considered *available* to Camelot and Asgard, enhancing the deterrent posture of both.

[31] Bundy, *Danger and Survival*, 471.

American-origin.[32] Likewise, the ICBM was (and remains) the sole provenance of states in their development and deployment, therefore, monopoly attribution was simple: there was little to no risk that such a weapon came from a non-state source. Before the tracking of ICBM capabilities and regular testing became a feature of the nuclear era, these two features — elimination and monopoly — were more salient mechanisms for assessing and acting upon the origin of a potential ICBM attack than identity attribution itself.[33] The same logic applies for deterrence purposes to the possession and deployment of ICBMs; elimination narrows the field of potential actors (including third-party allies that might maintain deployments of others' weapons, such as in Europe), producing a dynamic of immediate deterrence even absent obvious identity of a capability.

To recap: for the purposes of this analysis, the most helpful framing of the question is immediate deterrence, or the information and choices leading to a single decision to execute or hold back from an attack. However, for Babel to deter Asgard from attacking it, Babel's weapons need to be recognizable (both observable and with known effect) and must be reliably attributable to it and/or available for its use. Together, recognizable and attributable capabilities provide the two necessary inputs for the rational calculations of immediate deterrence between two states.

[32] Of course, the stationing of ICBMs in third-party allies offers precisely the kind of complexity that this chapter explores later in the context of cyberattacks.

[33] For example, the 1955 U.S. defense report *Meeting the Threat of Surprise Attack,* which Bundy regards as "one of the most influential in the history of American nuclear policy," was straightforward about these assumptions. Science Advisory Committee Technological Capabilities Panel, United States, "Meeting the Threat of Surprise Attack," (The White House, 1955). See also: Bundy, *Danger and Survival*, 325-8.

2.2 Cyberattack Capabilities as a Deterrent

For the state considering its defensive options, is developing cyberattack capabilities a safe bet in seeking to deter other cyberattacks, or attacks more generally? More specifically, can cyberattack capabilities effectively deter would-be attackers engaging in rationalist calculations? This section uses the methodology just outlined to examine whether cyberattacks are a powerful (and thus attractive) tool for deterring aggression. It argues a novel thesis: that despite attention to them in recent years, cyberattacks are an almost uniquely poor deterrent, due to particular qualities that deeply frustrate traditional rationalist deterrence models. Thus, futuristic prospects of a wholesale military shift to cyber capabilities or a kind of mutual "cyber-deterrence" are largely dashed.[34] Therein lies, this section argues, some cause for optimism: once their novelty wears off, states might not find the deterrent value sufficient to merit the investment.

The prior section outlined the details of how rationalist deterrence operates as a generic, if not systemic, theory of state behavior given a particular security threat. Its maxims, in that respect, function regardless of the means of aggression; otherwise, the theory would be of little explanatory value, calling into question why it might be the subject of so many fine studies. Indeed, the prior analysis confirms much of that account: principles of deterrence work well informing state behavior relative to both traditional coercive means like troop movements, and more novel ones like ICBMs.

Yet cyberattacks pose some significant challenges to rationalist deterrence, and approaches that might make rationalist deterrence powerfully explanatory in

[34] See, as discussed throughout: Libicki, *Cyberdeterrence and Cyberwar*.

international relations falter in explaining state choices to develop or use cyberattack capabilities. The reason, as this section argues, is that these capabilities themselves offer little as a reliable deterrent against aggression.

Disaggregating Cyberattack Capabilities

Deterrence is an information-dependent phenomenon; a state must know enough about the capabilities of its adversary to make a rational choice. As this section argues, a would-be attacker's knowledge of specific components of an opponent's capability — whether gleaned covertly or advertised by the defender — can have vastly different effects on deterrence calculations.

For this reason, this section disaggregates cyberattacks into the constituent technologies that are needed to develop, deploy, and use them against another state. Some rationalist studies have sought to consider the elements of a cyberattack as a single capability, but do so at considerable analytical peril.[35] Reducing cyberattacks to a single capability, for the purposes of studying a deterrent effect so deeply tied to another state's specific knowledge of that capability, would be equivalent to regarding all airborne forces as equal in makeup and deterrent implications. Just as now the status of an air force's readiness and specific tools matters tremendously for deterrence, so too does knowing the specific status of a cyberattack capability. It is particularly important because an aggressor might have insights into only one of these elements, substantially changing its deterrent value — just as finding a large airfield is not proof positive of a substantial air force, but seeing a squadron of mobilizing bombers yields more reliable information. Therefore this section embarks on a more

[35] For example Libicki's military-focused volume on "cyber-deterrence" tends to take this kind of monolithic approach, except to distinguish cyberattacks from certain kinds of spying activity.

detailed analysis that is essential to evaluate whether and how those discrete capabilities — individually or combined — provide meaningful deterrent value to their possessor.

Cyberattack capabilities then, for the purposes of informing deterrence, can be thought of as three distinct elements: *development infrastructure*; *deployment network(s);* and *execution tool(s).*[36] Recalling that for effective immediate deterrence, the would-be attacker first needs to have recognition (of instrument and effect), second, a means of attribution (either direct identity attribution, or via ancillary deductive means like actor elimination and status of a force monopoly) of the target state's retributive force. Given those inputs, this section now considers the development, deployment, and execution components of a cyberattack to critically examine their deterrent value — specifically, to determine whether states are likely to receive the necessary inputs to make deterrent calculations.[37]

Development environment. Cyberattack capabilities' development environment is composed of, essentially, the hardware and software tools needed to create (but neither deploy nor execute) its 'ordnance' — typically malicious software.[38] Developing the malicious software (often called 'malware') is a mundane

[36] Excepting, for the moment, the simpler case of physical attacks on digital infrastructure.

[37] Again, this section does not explore the question of *dissuasion*, since the likelihood of an attack's success is largely case-specific and more significant for general deterrence relationships.

[38] The most common cyberattack capabilities are, as discussed in the prior chapter, software-based. They function by disrupting the normal operation of software ('code') on computers upon which an increasingly large fraction of daily lives in developed countries and their economies rely. This analysis holds, however, when considering a hardware-enabled cyberattack (say, one in which the destructive feature is incipient within the computers/devices put into place by the victim state). The demonstrate case of malicious software is however more widely known, and therefore a more accessible use case.

affair difficult to detect or observe. Therein lies the first manner in which it frustrates deterrence models.

Development of the malware itself — the first stage in the lifecycle and well before its deployment or use — can take place by an individual or a team working on one or multiple general-purpose computers. Unlike the specialized manufacturing facilities for aeronautics, or enrichment equipment required for certain nuclear weapons, the computers used to develop malware require few if any special characteristics.[39] Development can take place on most any off-the-shelf, dual-use computer, while even testing of sophisticated attack capabilities against esoteric infrastructure (like a certain kind of electrical transformer or water pump) would require little more than a single example of such a victim device. So when considering what constitutes a cyberattack 'capability,' it is essential to bear in mind that those capabilities commonly begin on commercial technology distinguishable only by contents and use, not design.

Is either part of this development environment, either the infrastructure or code itself, helpful in assessing a state's cyberattack capabilities, and in turn, its deterrent value? Here the general criteria of instrument recognition, effect recognition, and attribution offer clues.

The infrastructure that constitutes the development environment, at its most generic, provides no meaningful instrument or effect recognition to an adversary. Substantial computing centers filled with servers generating significant heat and connected to thick fiber-optic lines are one kind of infrastructure often associated with

[39] For example, none of the attacks described in Anderson's comprehensive work on security engineering necessarily require military-grade technologies. See: Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 633-52.

cyberattack capabilities. In reality, however, they only indicate a state's level of investment in digital technology. Thus, a state's development of new data centers or dedication of computing facilities to the military — touted by the American, Korean, and Russian militaries as evidence of their cybersecurity prowess — is not tantamount to specific cyberattack capabilities.[40] With respect to attribution, it is plausible that large-scale computing centers might be positively identified as belonging to an adversary, but offer little aid in assessing capability, for the reasons above. This sort of ancillary infrastructure is not a reliable metric of attack capability, and is even less useful in the assessment of those tools' effects.

The other feature of the development environment — the malicious code itself — does offer some more valuable information in making deterrence calculations. Locating such code while in development might reveal clues as to a would-be attacker's designs and sophistication, providing rough instrument recognition. However, the majority of malicious software targets vulnerabilities in common commercial technologies — say, an operating system — and is rarely coded to a single particularly sensitive or important machine. For example, malicious software that is designed to disrupt all but the most specific infrastructure (such as a particular brand of power transformer), or the rare piece of software with its targets 'hard-coded' into it (akin to finding a missile's targets written on its exterior when aerially

[40] Henry Kenyon, "Work Commences on $1b NSA 'Spy' Center," *Defense Systems*, 7 January 2011; Yonhap News Agency, "S. Korea to Launch Cyber Command Next Week," 8 January 2010; David Talbot, "Russia's Cyber Security Plans: As Washington Airs Plans for a New 'Cyber Command,' a Top Russian Official Discusses the Threat of Cyberweapons," *MIT Technology Review*; Vasudevan Sridharan, "Russia Setting up Cyber Warfare Unit under Military," *International Business Times,* 20 August 2013.

photographed) would remain largely enigmatic until it is deployed on networks.[41] In other words, observing even the software in development might not reveal its target, and thus, without observing deployment, a state could glean little about its likely effects.

Compounding this recognition challenge is another practical obstacle: the fundamental need for secrecy combined with the difficulty of witnessing code in development. Consider first that unlike explosives or other capabilities routinely exercised by the military, software-based tools that make up an effective cyberattack are often single-use because they exploit vulnerabilities that can be directly mitigated, if known. Thus, as this chapter will explore in-depth in later sections, maintaining secrecy in development is not just preferable but essential for an effective capability. In this respect, efficacy and deterrent value can be in direct opposition — a feature whose implications are discussed in-depth in subsequent pages. In order to maintain secrecy, the development infrastructure might not be connected to the public Internet until work was complete and the code was ready for deployment. The result is a development environment that is necessarily obfuscated and producing tools that are perennially novel — at least in their method of operation. The investment therefore required to find the particular machine on which development of malicious code is taking place represents a considerable if not insurmountable intelligence and surveillance challenge.

[41] *Stuxnet* was reportedly a rare example of such malware, apparently specifically designed to activate only in the presence of a single type of infrastructure believed to be associated with the Iranian nuclear program. As the next paragraph outlines, this case illustrates the tension between credible (i.e. demonstrable) deterrent effect and efficacy of the attack itself.

Attribution of malicious code in development is notably difficult for three reasons: the almost categorical lack of state identity, the imprecision of elimination, and the typical absence of monopoly. While not excepting that states have engaged in this activity, to date no state has to date publicly and positively claimed credit for a piece of malicious software in development, and only a handful of massively disruptive viruses have had their author unmasked.[42] Even after the fact, states have not attributed to themselves disruptive cyberattacks widely considered their handiwork — a crucial and puzzling fact explored throughout, and especially in Chapter 4.[43] Barring public acknowledgment, elimination can be helpful in refining the sophistication of an actor responsible for malicious code, but little else.[44] Security researchers have generally been effective in distinguishing 'run of the mill' viruses from sophisticated tools intended for deployment against another state's national security, though the line between the tools of organized crime and sophisticated nation-states remains blurry.[45] Regardless, that information would be of little comfort

[42] See, for example: Phil Stewart, "Old Worm Won't Die after 2008 Attack on Military," *Reuters*, 16 June 2011. As of this writing, even physical attacks on digital infrastructure, such as the event that disabled much of San Francisco's Internet connectivity for a period of several hours, remains unsolved.

[43] See, for example, coverage of the Russia-Georgia attacks, Operation Orchard, and *Stuxnet*, all *op cit.*

[44] Were a state to locate the precise machine(s) on which malicious code development was taking place, identity attribution would be possible; however for the reasons mentioned above, it would be unrealistic to rely upon it to inform immediate deterrence calculations.

[45] For example, comprehensive reports of many of the highest-profile incidents of cyberattack and cyber-espionage in recent years have noted the potential for criminal involvement.

See generally: McAffee and Good Harbor Consulting, *Virtual Criminology*; Select Committee on Intelligence, United States Senate, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community*, 31 January 2012, 7.

For specific cases noting this blurring, see: McAfee, *Protecting Your Critical Assets: Lessons Learned from 'Operation Aurora'* (Santa Clara, CA: McAfee, 2010); *Global Energy Cyberattacks: 'Night Dragon'* (Santa Clara, CA: McAfee, 2011); Kaspersky Lab, *Kaspersky Lab Identifies Operation 'Red October,' an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions* to any state with two technologically sophisticated adversaries. Moreover, it is difficult to eliminate the potential for proliferation of even a state-developed tool itself (to say nothing of the accesses that led to it), as transferring code from one developer to another is as simple as sending an attachment to an email or physically handing off a thumb-sized flash drive. Therefore elimination might be sporadically informative but, given the increasing list of states deemed 'capable' in this space, is far from conclusive. The same frustrations apply to monopoly, perhaps the least-informative criteria with respect to malicious code development. Generally speaking, the development infrastructure for most cyberattacks is generic. Destructive code might be written (i.e. developed) as easily on a home laptop as on a government-issued performance computer — and without monopoly, greatly expanding the universe of attribution. Thus, cyberattack development stands in stark contrast to most sophisticated weapons, which require dedicated facilities, equipment, and supply chains.

The result is that easily observed cyberattack infrastructure yields little knowledge about specific cyberattack capabilities, while the exceptionally difficult-to-observe development of code yields different information, but is still incomplete. Even together, knowing the details of an adversary's development environment is not enough for a state's cyberattack capabilities to render effective deterrent value to a would-be adversary, as Table 2.1 summarizes.

Worldwide (Moscow: Kaspersky Lab, 2013); SecDev Group, "Tracking Ghostnet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, 29 March 2009.

Table 2.1: How Development Environment Informs Deterrence Calculations

	Recognition		*Attribution*		
	Instrument	**Effect**	**Identity**	**Elimination**	**Monopoly**
Development Infrastructure	?	X	√	√	√
Code in Development	√	?	X	?	X

√ = Meaningful contribution *? = Indeterminate* *X = No contribution*

Deployment Network. In their second phase — the deployment networks that house or deliver malicious software — cyberattack capabilities are more easily recognizable, but far more challenging to attribute.

A deployment network is, for this simple case, the network of machines and/or communications pathways that deliver the 'payload' of malicious software to their target computers. For example, in the kind of disruption experienced by Estonia, the victim could theoretically have known about the existence of disruptive network of computers awaiting orders prior to the event. This provides a more accessible means to instrument recognition, i.e. to understand the nature of a potential attack. Likewise, technical surveys of the size of various 'botnets' or other deployment networks for cyberattack capabilities are possible and precise.[46] Thus a state might roughly scale the nature of the threat that could be brought to bear against it.

[46] Amit Kumar Tiyagi and G. Aghila, "A Wide Scale Survey on Botnet," *International Journal of Computer Applications* 34, no. 9 (2011); Hossein Rouhani Zeidanloo, Farhoud Hosseinpour, and Farhood Farid Etemad, "New Approach for Detection of IRC and P2P Botnets," *International Journal of Computer and Electrical Engineering* 2, no. 6 (2010).

Nonetheless, deployment is not the same as use, and not always indicative of the probable effect of an attack. Therefore, absent an execution order with final instructions on the networks to attack, it might not be possible to know much about the scale of capabilities. Even less would be known about the effects (already highly variable given that no state possesses full knowledge of how system outages might cascade and cause damage across their society).

In this scenario, since infrastructure would be distributed across civilian and government, public and private networks, it nearly defines the absence of identity, inability to eliminate, and loss of force monopoly. Moreover, cyberattack deployment networks invoke the other complicating aspect of force monopoly — third-party availability. For example, the network of machines that attacked Estonia, each infected with a virus developed by a source unknown, was later reported to be available for hire to the highest bidder.[47] In fact, many small-scale disruptive networks featuring into a cyberattack are available for hire for as little as a few hundred dollars.[48]

With respect to attribution, one might roughly analogize the deployment network to a squadron of incoming aircraft over international waters — visible on radar, but only in their direction, formation, rough size, and quantity. Such networks offer a better sense of the scale of an imminent cyberattack, but still frustrate meaningful assessment by denying any meaningful and direct information about attribution. As such, these cyberattack capabilities offer far less information than

[47] John Markoff and Mark Lander, "Digital Fears Emerge after Data Siege in Estonia," *The New York Times*, 29 May 2007.

[48] Trend Micro, "Russian Underground 101," (Cupertino, CA: Trend Micro, 2012), 3,6.

would be necessary for them to provide their controlling state with a strong and recognizable deterrent when discovered by an adversary. Table 2.2 summarizes these conclusions.

Table 2.2: How Deployment Network Informs Deterrence Calculations

	Recognition		*Attribution*		
	Instrument	**Effect**	**Identity**	**Elimination**	**Monopoly**
Deployment Network	√	?	X	?	X

√ = Meaningful contribution *? = Indeterminate* *X = No contribution*

Execution tools. A third category of cyberattack capability, the *execution tool(s)*, are the most imminent and forward-deployed component of an attack — and, of the three, constitute the most promising candidate to inform immediate deterrence.

Execution tools can be thought of as the command-and-control infrastructure for hardware- or software-based cyberattack. They represent the final phase in the lifecycle of planning a cyberattack, well after development on the attacker's own networks/machines and deployment that would normally transit third-party networks. Execution tools, by contrast, would be found in two places: either on the victim's networks (such as a power grid network or other critical infrastructure) awaiting the command to execute, or on an attacker's networks, waiting to issue that command. Thus, with respect to recognition and attribution, locating execution tools could provide much of the requisite information for a state to assess the nature of a potential attack — though doing so would indeed prove highly difficult.

In the case of tools known to be on a victim's network, instrument recognition seems highly probable (by their very presence), as would be the effect (by examining their intended purpose on that machine). This potentially powerful message is blunted by two facts. The first, already outlined, is that knowledge of the presence of these tools on a victim's networks invites their rapid inoculation — making cyberattack capabilities difficult to 'exercise.' Second, attribution of such tools located on a victim network is likely to be fleeting. An attacker seeking deniability (as all appear to have to date) would take measures to obscure the identity of the responsible machine.[49] Looking ahead, this condition seems likely to persist. As a general matter, failure to execute the desired cyberattack would jeopardize the credibility of the deterrent. Moreover, discovery of a capability may unduly escalate tensions at a time different from the would-be attacker's preferred moment. Therefore, deniability remains an important asset for cyberattack capabilities, and 'self-advertising' seems unlikely. Frustrating attribution appears practically important, but also deeply undermines cyberattacks' value as a credible deterrent.

Were the means of execution discovered on a would-be attacker's networks — including, for example, if the tools needed to activate malware were already installed on the victim network — the deterrent effect would be perhaps most significant. Here, attribution speaks for itself: in this simplified example, the location of that

[49] Were the attack both sophisticated and on the scale under principal discussion in this study, opportunities for attribution by elimination might present themselves, by narrowing the field to those with sufficient capability and reasonable intent. Still, though, a state with two such adversaries might be left with crucial uncertainty. Moreover, a modicum of certainty on force monopoly in the case of the final execution tools (reserved for a single actor to execute, and sophisticated enough to be of national security concern to a nation-state) offer some additional potential in providing attribution.

execution tool is known to be an adversary's machine.[50] Recognition is also possible at least by half-measure; one can easily connect execution tools' controlling mechanisms to the tools they manage, however it is less likely that the full scale (effect) of the tool would be identified in this way.

As the Table 2.3 below demonstrates, a combination of the two (linking execution tools on both the attackers' networks and victim networks) would provide all necessary inputs to inform immediate deterrence.

Table 2.3: How Execution Tools (at Various Locations) Inform Deterrence Calculations

	Recognition		*Attribution*		
	Instrument	**Effect**	**Identity**	**Elimination**	**Monopoly**
Execution Tools (Victim network)	√	√	X	?	?
Execution Tools (Attacker's network)	√	X	√	√	√
Combined	√	√	√	√	√

√ = Meaningful contribution *? = Indeterminate* *X = No contribution*

[50] While simplified this scenario is not far-fetched; the attacker-side execution tool is likely to remain on computers owned and operated by the state in question for the same reasons of trust that launch codes and sensitive radar systems remain in capitals and not on allies' territory.

Therefore in the abstract, a state could rely on others' knowledge of its cyberattack execution tools — their location, likely effect, and attribution — to meaningfully inform its adversaries' deterrence calculations. This deterrence information should not be confused with full attribution of the sort necessary for criminal prosecution or assessment of individual responsibility.

This latter point has, perhaps unduly, frustrated much of the literature on the international response to cyberattacks. While later chapters will address this question of state responsibility as a matter of international law, as a preliminary matter in the rationalist framing, states' first preoccupation post-attack is unlikely to be assessment of the *individual* responsible. By analogy the identity of who flipped the switch launching the missile, flew the airplane, or even who in the military chain of command issued the order is for the most part militarily, diplomatically, and politically irrelevant. Salient instead is only whether those individuals were part of the organized defense forces, or directly controlled by them. On the scale of attacks under discussion in this study, that kind of broad-brush attribution is eminently possible. With the right inputs then, it is conceivable that states might be able to form deterrence calculations — but, as the following sections will discuss, exceedingly practically difficult.

The Specificity Paradox

One further technical reality sets cyberattacks apart, and deeply frustrates their use as a credible deterrent: the uniquely strong relationship between knowledge of an attack vector's specifics and defense against it. Many of the tools of cyberattacks are (as mentioned earlier) single-use; they exploit previously unknown vulnerabilities in the millions of lines of code that make up modern digital systems. Once their method of attack is known, it can in most cases be trivially 'patched' — in essence, correcting the flaws in the system that were vulnerable to exploitation. Such patches are often distributed, like inoculations, across the entire population of machines, rendering the attacking virus inert.[51] This is what might be called the *specificity paradox*, which has substantial implications for cyberattack capabilities' deterrent value.

While more information released about a given state's cyberattack capabilities might provide it additional deterrence value, that value is not positive and linear. Once a certain level of specificity is known, defense against it becomes accessible, and its deterrence value goes to almost zero.[52] Consider, by contrast, nuclear weapons: detailed knowledge of how a weapon works does not provide meaningful defense against its destructive power. Likewise with advanced missiles, artillery, or submarines, knowledge of their technical workings might at best provide means of sabotage, but not direct defense against their offensive capabilities.

When cyberattacks are introduced into an international security environment, so too is a kind of heterogeneity in the potential threats, and in turn, a pervasive opacity as to the kind of deterrent those capabilities might provide. If a state's threats of cyberattack are specific enough to be credible to their adversary, they may consequently be simultaneously self-defeating.[53]

[51] Such 'patching' happens, in the case of a consumer personal computer, weekly if not more — sometimes with several hundred or more 'inoculations' per cycle.

[52] This feature may be one of the present moment and the present state of technology, and as with all such things difficult to consider fixed. However, lacking any contrary evidence with today's technology, this damning prospect for a cyberattack capability's deterrent effect must undergird study of it.

[53] This same phenomenon explains why general (*vice* immediate) deterrence against cyberattacks is less than promising: since attacks are so inherently 'perishable,' it would be difficult for much habituation of action and reaction, or understanding of escalation thresholds, to obtain.

Conclusions and Implications for Cyberattack Capabilities' Proliferation

There exists a certain paradox in studying deterrence of cyberattacks. In the abstract, deterrence might obtain, but to do so would produce the kind of study Kissinger rightly relegated to an 'esoteric intellectual exercise.' A study with more practical implications for international politics must necessarily accept imperfect and incomplete information. As just argued though, certain types of information are essential to a state making any approximation of a rational choice on that basis. Within the lifecycle of cyberattack capabilities' development, deployment, and final use, only knowledge of the latter — and at that, the fortuitous triangulation of attacker and victim network — is likely to provide the necessary information to meaningfully deter an adversary.

In short, states will favor cyberattack tools for offense over defense, and for use over threat. Cyberattack tools are difficult to observe and hard to locate while in development, easy to obfuscate during deployment, and generally single-use. A would-be attacker is unlikely to be deterred from aggression by a state's cyberattack capabilities alone. So even if Asgard and Babel are two countries with similar vulnerability to a generic cyberattack, Babel's development, deployment, and all but the sloppiest or most disposable preparation to execute cyberattack capabilities are poorly suited to meaningfully inform Asgard's rational choice to attack.[54] Moreover, if Asgard's information about Babel's cyberattack capabilities is credibly specific, the former's ability to defend against a counterattack increases substantially. It seems implausible that cyberattack capabilities represent a sound investment for Babel if it is

[54] Japan and South Korea would be examples of such countries, falling into a similarly high level of digital dependency.

strictly seeking to deter its aggressor. Table 2.4 summarizes the conclusions of the prior sections and provides a comprehensive overview of the information states might use to inform their deterrence calculations against cyberattack capabilities.

Table 2.4: Overview: How Cyberattack Capabilities Inform Deterrence Calculations

	Recognition		*Attribution*		
	Instrument	**Effect**	**Identity**	**Elimination**	**Monopoly**
Development Infrastructure	?	X	√	√	√
Code in Development	√	?	X	?	X
Deployment Network	√	?	X	X	X
Execution Tools (Victim)	√	√	X	?	?
Execution Tools (Attacker)	√	X	√	√	√

√ = Meaningful contribution *? = Indeterminate* *X = No contribution*

There are indeed a few exceptions to this general conclusion. A state with only one plausible, capable adversary and exceptional reconnaissance might be informed of the threat and origin, and find itself deterred from aggression generally. Another case would find Asgard highly dependent on technology and Babel not, in which the former's discovery of the latter's sophisticated cyberattack program may more effectively deter aggression than might otherwise be the case.[55] Beyond these

[55] Another might be a state's sloppy preparation or public demonstration of cyberattack capabilities, but doing so would likely lower the efficacy of that attack to the point of insignificance.

narrow cases however, cyberattack capabilities appear to offer little direct deterrent value in a rationalist decision-making space.

Given that cyberattacks offer little to a state seeking to deter aggression, there are two substantial implications for international politics, both suggesting as a preliminary matter that their limited value in this context may provide some counterweight to their proliferation.

First, as information about their real capabilities and limitations grows, the long-term 'pull' to acquire cyberattacks seems far weaker than journalism and popular literature suggests. Cyberattacks are not, from the standpoint of rationalist deterrence, a sound investment for a state seeking a peacetime deterrent. In the rationalist mode, states make investments in their security on the basis of perceived threat and perceived vulnerability weighed against the value of the strategic investment. Vulnerability and threat may both be high, but the deterrent value of investing in such difficult-to-demonstrate cyberattack capabilities render them a less attractive investment than more conventional, credible attack vectors. Therefore, though cyberattacks possess a substantial and growing disruptive threat to states, they are not the *sine qua non* of maintaining international security.

This conclusion may appear at first blush to be at odds with present state practice. After all, if these tools are of so little deterrent value, why are so many states clamoring to acquire them and advertise their capabilities? It is important not to lose sight of the fact that limited deterrent value does not equate to limited offensive value. Indeed, for states pondering full-scale conflict against an adversary, a cyberattack can for all the reasons outlined in the prior chapter shift the balance of conflict. The fact also remains that while information about cyberattacks may be limited for strictly rationalist calculations, apprehension of them (and hyperbole about their destructive power) is at present quite high. Thus when top Russian officials warn of "the huge potential [for] information-computer technologies [to] be used to ensure military-political domination, the use of force and blackmail to open doors to new trends of arms race," and American officials worry that "the next Pearl Harbor we confront could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems," it may create a (potentially irrational) pull on policymakers.[56] This pull, while defying the cold calculations upon which most deterrence theories are based, is both meaningful and instructive at this particular historical moment.

Some states may be acquiring those capabilities for deterrent potential more than proven deterrent value. Consider, for instance, that the United States, Germany, Russia, the United Kingdom, South Korea, and North Korea all publicly claim to be developing some sort of cyberattack or 'cyber-warfare' capability.[57] One might assume that states are clearly *claiming* development of cyberattack capabilities, and that in so doing they are attempting a sort of in-kind deterrence. As a political matter, which is to say one of national reputation, there may indeed be signaling value in broadcasting such developments. As a rational deterrence matter though, there is

[56] Andrey Krutskikh, "Information Challenges to Security (1999)," in *International Information Security: The Diplomacy of Peace*, ed. Sergei Komov (Moscow: Russian Federation Official Publications), 7; Armed Service Committee, United States Senate, *Hearing to Consider the Nomination of Hon. Leon E. Panetta to Be Secretary of Defense*, 2011.

[57] Committee on Armed Services, United States House of Representatives, *Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force, Hearing before the Subcommittee on Intelligence, Emerging Threats and Capabilities*, 14 March 2013; Federal Ministry of the Interior, *Cyber Security Strategy for Germany*; Talbot, "Russia's Cyber Security Plans: As Washington Airs Plans for a New 'Cyber Command,' a Top Russian Official Discusses the Threat of Cyberweapons"; BBC News, "Interview with Prime Minister Gordon Brown: 'We Must Not Be Victims'," 25 June 2009; Kwan-jin Kim, "Remarks at the 11th Defense Information Security Conference," news release, 2011; "N. Korea 'Confident' in Cyber Warfare Capabilities," *Chosun Ilbo*, 8 April 2013.

little to be gleaned from such a claim. Far more salient is the fact that even among those with ‘declared’ dedicated cyberattack capabilities, none has yet claimed responsibility for any single cyberattack-like event — nor, crucially, demonstrated those capabilities for would-be aggressors to see and assess. Assumptions may be the currency of deterrence in the absence of solid intelligence, but even those countries who directly connect their dedicated cyberattack apparatus to network defense have yet to publicize a successful thwarting of a cyberattack. In the context of this analysis those states may also be disappointed as the short-term decisions of policymakers run up against the underlying realities of immediate deterrence.

The second and perhaps even more significant conclusion of this section is that a state with cyberattack capabilities must principally rely on its other strengths and capabilities to deter adversaries. There is already some evidence of this fact. For instance, those states publicly known to have an overwhelming cyberattack capability have not seen the peacetime balance of power swing tectonically in their favor. Nor, for that matter, have any states realigned their military posture or drawn down traditional forces in preference of cyberattack capabilities (as was often the case with nuclear weapons).[58] The former is particularly notable if it remains true that states with reportedly strong cyberattack capabilities, like Israel and Australia, fail to gain visible concessions from adversaries seeking to avoid become victims of those tools. As states develop a greater understanding of the tactic, even as their susceptibility to it may increase with their technological dependence, from this analysis it seems unlikely that cyberattack capabilities will form the core of a state’s deterrent posture.

[58] For several other examples of tectonic shifts in technology shifting reliance on previously preponderant forces, see: Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, NJ: Princeton University Press, 2004), 77.

Both of these conclusions suggest a limited role for cyberattacks in deterring aggression generally, given their inherent attributes. In this respect, the drive to acquire cyberattack capabilities may be self-limiting. However, it is not overwhelmingly so, as some states claim to be acquiring these capabilities, and there is some evidence that several more are doing so without such a public profile. So how might states with such ambitions be directly *discouraged* from developing cyberattack capabilities under rationalist logic? Might a state be able to deter that cyberattack aspirant from acquiring or using those capabilities? That is the question to which this chapter now turns.

2.3 Deterring Cyberattacks

Cognizant of cyberattacks' limited role deterring aggression generally, this section examines the flipside: how states might go about deterring cyberattacks *aimed at them*.

This section first extends the conclusions of the last — that cyberattacks offer poor tools to deter general aggression — to examine whether states might effectively 'fight fire with fire,' deterring the threat of cyberattack with similar in-kind capabilities. After concluding that cyberattacks play an even more limited role in the maintenance of peacetime international security, and that prospects for a specialized 'cyber-deterrence' seem dim, it highlights an under-acknowledged reality: like any other aggressive state action, cyberattacks can most reliably be deterred by an adversary's overwhelming military or other retaliatory arsenal.

Deterring Cyberattacks In-Kind

Because they are poor deterrents and serve little defensive value against similar capabilities, a state seeking to deter a cyberattack from its adversary would do well to look beyond developing its own capabilities in-kind. The principal reason, the difficulty of signaling and assessing in order to make a meaningful deterrent calculation, does not require recapitulation. However some distinct strategic characteristics of cyberattacks explain why one should not expect in-kind capabilities to meaningfully deter an attack.

As previously noted, cyber-defense and cyber-offense are largely incommensurate. Offensive cyberattack tools do not, by their nature, have inherent defensive value, as might for instance fighter jets, tanks, destroyers, or aircraft carriers. The sorts of tools outlined in the previous section, such as malware, are purpose-built to disrupt, but (at least at present) are not adaptable to defend.

The one exception to this claim would be the potential for pre-emptive or retaliatory disarmament of an aggressor: using cyberattack tools to cripple a would-be aggressor's own capabilities. In this scenario, one could envision such malware being deployed to disable either the delivery network or execution tools of an adversary. While theoretically attractive and perhaps relevant to a later state of technology (and indeed the subject of some cybersecurity officials' futuristic musings), doing so would be at present impractical due to the overwhelming reconnaissance needs and potential for significant collateral effects.[59] Moreover, non-software-based

[59] See, for example, the United States' top military cybersecurity official's repeated calls for defense at 'network speed,' capable of anticipating and responding to attacks without human intervention. Committee on Armed Services, United States House of Representatives, *Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force, Hearing before the Subcommittee on Intelligence, Emerging Threats and Capabilities*, 14 March 2013, 9, 14.

cyberattacks, including destroying information infrastructure or disabling other critical hardware, again have no meaningful defensive use. Today's cyberattack capabilities, in other words, have little *counter-force* value.

The result is that in deterring cyberattacks, those same cyberattack capabilities have at best *counterattack* value — which is of course still limited by the difficulty signaling it, as outlined in the prior section. Nonetheless, if analogies are to be drawn, cyberattacks in this context bear closer resemblance to intercontinental ballistic missiles, artillery, and other tools useful for offense both initial and retaliatory, but not immediate defense itself. Put differently, cyberattack capabilities do little to *dissuade*, which is to dampen or nullify the success of an incoming attack.[60] Given this technical nature, the likely outcome of a dyad of states each developing cyberattack capabilities for use is *not* mutual restraint to limit potential damage, but build-up. In this respect as well, strategic planning for the use of a cyberattack bears some resemblance to the dynamic of nuclear stockpiling and ballistic missile rivalry during the Cold War.[61]

Dim Prospects for 'Cyber-Deterrence'

'Cyber-deterrence,' it seems, may simply be interstate deterrence as we have always known it — only complicated by a technology that eludes much of the foreknowledge that helps states maintain peace. The prior section explained in detail why, as a general matter, cyberattack capabilities are poor investments for deterring

[60] Notably, some national cyber-defense strategies appear to recognize this distinction and specifically note it, including both the U.S. *International Strategy* and *Defense Strategy for Operating in Cyberspace*.

[61] Such a study would fall outside the scope of this dissertation and without much history behind it, may be better suited to military science than international relations. It may however be fruitful for subsequent scholars to examine in-depth in such a context.

aggression due to their unique characteristics. As states develop these capabilities, meaningful in-kind deterrence is unlikely to limit them; if anything, the perceived threat of cyberattack by an adversary would more likely result in a build-up, rather than drawdown of those capabilities.

The conclusion here is that attempts to define and rely upon a discrete and self-contained notion of 'cyber-deterrence' — that is to say deterrence defined solely by the contribution of cyberattack capabilities — are misguided. A cyberattack cannot be meaningfully deterred by another cyberattack. Instead, the only realistic prospects for deterring it appear to be through the full scope of state powers that would be brought to bear to deter any other aggressive state action, whether diplomatic, economic, or military. It is with this in mind that UK Defence Minister Nick Harvey pointed out from a doctrinal standpoint, "cyberspace adds a new dimension, but its use in warfare should be subject to the same strategic and tactical thought as existing means."[62]

If deterring a cyberattack is not well done via a defender's own similar capabilities, might the natural solution be to deter via traditional (i.e. non-cyber) means? Certainly, a state with an overwhelming traditional military presence would hope so. And indeed, were cyberattacks simply another addition to any conventional military arsenal, the answer would almost certainly be 'yes.' After all, while in some cases similar capabilities might dissuade (such as naval ships), other types of aggression are best deterred by different compelling capabilities (say, a nuclear

[62] Nick Harvey, *Armed Forces Minister - Responding to Cyber War*, ed. UK Ministry of Defence (London: The Stationary Office, HMG, 2011).

deterrent to conventional invasion). The latter is particularly true of weapons that favor offense, like cyberattacks.

There is only one concern, trivial to military planning but vital to the international relations of cyberattacks: these kinds of capabilities are not universally regarded as weaponry in the traditional sense. A cyberattack is not necessarily considered, by all states at the present time, an incident that invokes the same kind of comparative military force analysis that defines the prototypical immediate deterrence calculation. Therefore, in weighing the gains and losses of a cyberattack, it is decidedly unclear whether or not military retaliation is on the table. Knowing so would be of fundamental importance to deterring a cyberattack. After all, if states were to universally acknowledge that their conventional forces are off limits in retaliation, it would dramatically skew a would-be attacker's calculations about undertaking one — particularly against a well-armed adversary. Or, perversely, the absence of likely armed retaliation might incentivize the use of cyberattacks relative to other forms of interstate coercion. So today cyberattacks occupy a kind of purgatory — where states are unable to make rationalist decisions about them until certain decidedly normative debates are resolved about their lawful and practical status.

The next section argues that this very debate, with fundamental implications for whether and how cyberattacks might be deterred, is presently playing out on the world stage. Underlying it is the reality that cyberattacks' status within customary practice (of states and their militaries) is unsettled. For this and the reasons articulated prior, it is impossible for states to undertake purely rationalist deterrence calculations. Consequently, states are in the midst of deploying variants of a similar strategy to deter one another from using cyberattacks by linking them to or decoupling them from conventional military arsenals.

2.4 An Alternative Approach: Structural Deterrence

Most discussions of deterrence take as a given the universe of potential responses available to an attacker or defender. Without that basic knowledge, it is difficult if not impossible for a state to rationally assess gain and loss. If that is true, then there would be no way a for state to *predictably* deter cyberattacks by another, and prospects for international stability amidst states possessing them might be fleeting. Purely rationalist analysis, if it takes state response options as determined and static, would relegate the question to a policy matter, and await evidence of when states have been effectively restrained from an overwhelming interest in executing a cyberattack. In short, it would provide little insight to the present-day scholar.

In this present state of affairs, it is impossible for traditional deterrence relationships explain state behavior relative to cyberattack capabilities. Since cyberattacks occupy a kind of 'deterrence purgatory,' where insufficient information exists to inform a deterrent relationship, states are uncertain about the proper or acceptable response to a cyberattack. In particular, they are unclear whether that response is military in nature. I argue that states are aware of this ambiguity, and are seeking, in a novel sort of interstate competition, to set the parameters for future deterrence of cyberattacks.

The section argues that a more nuanced notion of rationalist deterrence is needed to explain both conceptually how cyberattacks might be deterred and how states *are presently* seeking to do so. It starts from the basic premise that the only way to meaningfully deter cyberattacks is by tying them to a conventional arsenal that is, itself, viewed as overwhelmingly deterrent and available for use in response. This method of deterrence is premised not directly on amassing one capability or the other, but primarily on shaping the customary environment for its use to swing rationalist deterrent calculations to one's own advantage, which I call *structural deterrence.*[63]

This section first defines the notion of structural deterrence and provides some rough historical parallels. Next it argues that states are already making use of this strategy vis-à-vis cyberattacks, and documents some of the most important examples thereof. Finally, it concludes by asking which side of this particular structural deterrence debate is likely to succeed: those who would link cyberattacks to their traditional military deterrent, or those who would assert that cyberattacks ought not be countered by conventional military means.

Defining Structural Deterrence

Structural deterrence adds a third dimension to the conventional rationalist calculation by recognizing that states must shape the acceptable universe of 'inputs' others use in calculating the advantage of using novel capabilities. It exists in the same analytical framework of rationalism — taking state interests as given and actions reflecting normative and institutional preferences as in service of that abiding interest — but it does not treat the context of their use as static. This more textured deterrence is one in which states strive to achieve outcomes in a rationalist environment by neoliberal means.

[63] This argument is one with fundamentally rationalist calculations in mind: namely, states in immediate deterrence situations will assess the full scope of possible response, and that whether that response is strictly in-kind, or leveraging other more conventional weaponry, will be essential to the decision to execute a cyberattack. Thus, a decidedly neoliberal and even constitutive argument playing out on the world stage also has substantial implications for normative 'usability,' as well as the success of deterring cyberattacks on rationalist grounds.

Structural deterrence, when necessary, precedes immediate deterrence. It is obviated by states' ability to conduct reliable rationalist calculations about a given act of aggression. Thus, for well-established means of attack, such as moving ground troops to occupy a territory, or dispatching of fighters to enter airspace on a bombing sortie, structural deterrence is hardly necessary. An attacker using such conventional tactics could easily calculate the range of potential retaliatory actions from their target — at least until the calculation begins to consider cyberattack capabilities. In this emerging arena, however, the calculation may break down thanks to the difficulty of assessing ramifications of a counterattack. It is even harder to assess if the primary means of aggression is to be a cyberattack.

Structural deterrence becomes necessary to a rationalist calculation when three pre-conditions are met:

First, that method must exist at the intersection of punishment and denial strategies — i.e., it must not be a state-ending capability, such as nuclear weapons (which, Cold War planning aside, most populations rightly equate to complete destruction and military defeat).[64] For example, a new novel and undetectable delivery system for nuclear weapons or a catastrophic biological weapon would immediately and obviously invoke the full measure of a would-be defender's available arsenal. Conversely, a new method for seizing government officials' assets would under no reasonable circumstances put all such assets into play. Cyberattacks,

[64] For an excellent overview of the differences between both theories, the distinction between them in the nuclear and conventional contexts, see: Robert A. Pape Jr., "Coercion and Military Strategy: Why Denial Works and Punishment Doesn't," *Journal of Strategic Studies* 15, no. 4 (1992): 429-32. For an more in-depth presentation of the punishment strategy in the nuclear context, see: Robert Powell, "Nuclear Deterrence and the Strategy of Limited Retaliation," *American Political Science Review* 83, no. 2 (1989).

for the general reasons outlined in the prior chapter and the paucity of state custom regarding their use, clearly fall in this intersection.

Second, that 'new' method must be one that, either by its nature or the evolution of present technology, eludes direct assessment of likely threat. Such circumstances might come to pass if the disruptive consequences are principally second- and third-order, and highly complex — such as a disruption to a crucial part of a global supply chain, food supply, or general-use information network — and/or if the capability itself is presently difficult or impossible to detect, as cyberattack capabilities indeed are.

Third and most importantly, that capability must not be able to be deterred 'in-kind' as described previously, thus requiring exogenous capabilities to effectively deter another state's use thereof. Combined, these three conditions create the circumstances under which traditional rationalist deterrence is not meaningfully possible, and where a strategy of structural deterrence is the only means for states to develop and, ideally, shape the rationalist calculations of others.

Parallels. Cyberattacks are not alone in blurring the line between peacetime and wartime coercion. In their seminal 1974 study of deterrence in the context of American foreign policy, George and Smoke remark on the under-developed study of those "deterrence or threats of conflict below limited war on the spectrum of violence."[65] Such events, they argue, constitute "a range of phenomena" where violence may be "covert, low-level, or not yet visible."[66] Even their study, however, draws a bright-line around situations like "counterinsurgency, and guerrilla warfare,

[65] George and Smoke, *Deterrence in American Foreign Policy: Theory and Practice,* 44.

[66] *Ibid.*

espionage…and ‘black’ operations,” which might be not deterred through obvious military or diplomatic means. Furthermore, their study avoids exploration of actions that themselves occupy a customary interstitial space between them. Yet cyberattacks presently exist in that sort of limbo, and such, merit more careful examination than general deterrence theories outlined above.

Structural deterrence is better suited to explain potential pathways for a strategic relationship than a retrospective interpretation of how individual decisions contributed to a particular historical outcome. In other words, it is normative-prescriptive rather than historical-explanatory; as such some historical parallels are relevant, though imperfect.[67] For example, peacetime blockades have long been a questionable act in international relations, falling at the intersection of economic coercion (by effect) and military coercion (by method).[68] The technical aspects of this parallel are considered in greater detail in Chapter 3, which examines questions of cyberattacks as uses of force and their potential for invoking rights of self-defense under international law. As a matter of rationalist deterrence, it is worth noting that peacetime blockades have invoked a similar kind of retributive ambiguity given their unsettled state in instances like the 1827 French, Russian, and British blockade in support of Greek rebels against Turkey; the British blockade of the Republic of New Grenada in 1837; the partial 1962 American quarantine of Cuba during that year’s Missile Crisis; and the present-day blockade of the Gaza Strip by Israel and Egypt. In

[67] George and Smoke make similar provisos about deterrence of limited war. *Ibid.*, 61.

[68] Blockades have long been a feature of declared war since their earliest record, from the Athenian blockade of the island of Aegina during the First Peloponnesian War (458-7 BC), to the Fatimid Caliphate’s naval blockade of the Kingdom of Jerusalem in 1102, to the 1991 blockade of the Croatian coast by the Serbian navy during the Bosnian Crisis (Croatian War of Independence).

such cases, it was not entirely clear to the aggressor whether or not the full measure of traditional military force could or would be brought to bear to terminate the naval action. It was difficult to assess the likely threat given their second-order consequences. And while the instrument (warships) could certainly be deterred in-kind (with a strong navy), the tactic did not lend itself to in-kind retribution. The result is a still-simmering, century-old question — separate from the related one of international law examined in the next chapter — about whether or not a would-be aggressor can expect the subject of its blockade to respond with full military force.

Likewise, a similar parallel might be considered in the case of unilateral peacetime economic sanctions. States executing such sanctions absent international mandate, particularly when the nature of such sanctions are novel — such as those against Iranian petroleum interests or targeting telecommunications — may do so without full knowledge of whether or not they might trigger any kind of traditionally understood military response by the other side. Economic sanctions can be punitive, but can in the case of a fragile regime depending on a certain commodity be a denial (i.e. defeat) strategy. Finally, while deep economic interdependency between two states might render an in-kind response to economic sanctions an effective deterrent, as a practical matter, the condition would hold for any non-interdependent would-be belligerents.[69] Thus nations subject to economic sanctions are at various times invoking the threat and use of traditional military force against their instigators, while

[69] This exception is, however, significant — for instance, one might argue that such conditions presently exist between the United States and People's Republic of China, with the former far less willing to coerce over human rights and other abuses in the same way it does with a nation upon which it is far less dependent, e.g. Iran.

the nations enforcing those sanctions (obviously finding them preferable to military conflict) deny such outright confrontation as a result.[70]

A glimpse at these cases offer a preview of the overwhelming evidence that states are, in the case of cyberattacks, engaging in structural deterrence. It is to this evidence that the study now turns.

Evidence of Structural Deterrence

As discussed previously, there are no present cases of states demonstrating *and* decisively claiming credit for deployment or use of cyberattack capabilities — frustrating their ability to deter using accumulated cyberattacks capabilities. But that is not to say that states are not actively engaged in efforts to deter one another's use of cyberattacks. As this section will argue, states are actively exercising strategies of structural deterrence, with the prospect of traditional military defense at the fulcrum.

States seeking to deter cyberattacks against them are doing so via two strategies of indirect deterrence. One, typified by the Unites States, United Kingdom, and their allies, would shape the international environment such that a would-be attacker pondering a cyberattack would have to factor the likelihood of a traditional military retribution into its rationalist calculations. The other, bolstered by Russia and China, seeks the opposite outcome: that cyberattacks would evade traditional military retribution and thus, the rationalist calculations of responding to them would be limited to other diplomatic and economic means.

[70] It is also for this reason that a number of scholars and advocacy organizations examine the questions both within the framework of international legality and existential humanitarian concerns — rather than strictly in the context of the *jus in bello*. See, e.g. Anna Segall, "Economic Sanctions: Legal and Policy Constraints," *International Review of the Red Cross*, no. 836 (1999).

Inclusive Strategy: Cyberattacks as Conventional Military Weapons

In cases of structural deterrence, states seek to shape others' expectations about acceptable reaction to a practice via their individual and collective posturing, and that is particularly true in the case of the United States, the UK, and Australia. Combined, there is evidence these states are advancing a complex strategy of structural deterrence that seeks to link powerful traditional military force and well-known military alliances to the rational calculations of a state pondering a cyberattack against them. They are promoting what might be deemed the '*inclusive view*' of cyberattacks in a deterrent calculation, which would mainstream cyberattacks — and most importantly their consequences — with kinetic military force against them.[71]

States pursuing this strategy do so by asserting three specific claims about cyberattacks within international relations: first, a *negative* assertion that cyberspace is not a distinct international space for the maintenance of international security; second, a *positive* assertion about willingness to invoke rights of self-defense when faced with a cyberattack; and third, a *collective* assertion of applicable treaty obligations — all aimed at shaping international custom and, perhaps, the development of international law. This section will document those claims, using the United States as a focal point and expanding analysis to its close and second-tier alliances, before presenting the counterpoint pursued by this group's historical adversaries in the space.

The United States' *International Strategy for Cyberspace* represents the synthesis of years of private deliberations and consultations with allies on the issue of

[71] The two chapters that follow explore the international legal veracity of claiming such actions might constitute "uses or force," or "armed attacks" – for the purposes of this chapter, that distinction is less relevant than the rationalist calculation states make in deciding how/if to respond to such an act.

international cybersecurity.[72] It is also rare in being a comprehensive, dedicated official policy statement on international relations and cyberspace, making it the strongest basis for understanding that state's strategy for deterring others from using cyberattacks.[73]

The negation of cyberspace as a somehow exceptional international sphere in international security, and thus one that might portend new expectations of action and reaction to attack, is challenged early in the document:

> Cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior — in times of peace and conflict — also apply in cyberspace.[74]

Though obvious to scholars of international relations or law, the characterization here can be understood as an implicit refutation of the *exclusive* view espoused by the United States' prime adversaries in cyberspace (explained in depth below). More importantly though, it grounds U.S. cyber-defense policy in the existing *jus ad bellum*,[75] *jus in bello*,[76] conventions on human rights,[77] and other relevant obligations

[72] Brennan, *Remarks at the Launch of the U.S. International Strategy for Cyberspace*.

[73] Thus this document is a more important barometer of the state's policy than, for instance, its Defense Department's *Strategy for Operating in Cyberspace*. It is also more relevant in the context of the national-level decision-making that would go into an armed response to a cyberattack, since in the American system, final military command and decisions to use force rest in the White House with the President in his role as military Commander-in-Chief.

[74] USISC, 9

[75] USISC, 9-10

[76] USISC, 14

[77] USISC, 9. While beyond the scope of this chapter, it is worth noting the pursuit of a parallel and consistent policy by the United States, supported most vocally by Switzerland, Sweden, France, and the Council of Europe, in extending existing human rights law to this space. In particular, references to the applicability of the Universal Declaration of Human Rights (esp. Art. 19), the International Covenant on Civil and Political Rights, and Council of Europe protections on freedoms of expression, privacy, and civil liberties have all been employed to considerable effect internationally. Further evidence of the formation of this norm — particularly as it relates to Egypt's domestic Internet shutdown — as an exemplar for security-focused cyber norms, is taken up in the final section of this study.

under international law. President Barack Obama's foreword to the document reinforces this claim, stating "the digital world is no longer a lawless frontier, it is a place where norms of responsible, just and peaceful conduct have begun to take hold."[78]

If this statement forms the basis for the negation of cyberspace as demanding *lex specialis*, the assertion that it is no less willing to respond to substantial cyberattacks as with any aggression of similar consequence is similarly unequivocal:

> We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.[79]

The United States is making two related claims: first, its willingness, and second, its right to armed self-defense when faced with a cyberattack of sufficient gravity.

The former is more obviously a statement designed to inform rationalist deterrence calculations, and is the foundation of the United States' structural deterrence strategy. Perhaps less subtly, a senior U.S. military official was quoted in the Wall Street Journal asserting, "[i]f you shut down our power grid [with a cyberattack], maybe we will put a missile down one of your smokestacks" — taken abroad as a signal of a new, bellicose posture relative to cyber incidents.[80] This aspect of the structural deterrence posture is over a decade old; to quote retired U.S.

[78] USISC, *Preface*.

[79] USISC, 6, emphasis added.

[80] Siobahn Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, 30 May 2011.

Air Force General Charles Dunlap, "[a] cyber attack is governed by basically the same rules as any other kind of attack *if the effects of it are essentially the same*."[81]

But this structural deterrence posture is incomplete without the second claim relative to legitimacy. Especially when used by states that doctrinally proscribe or freely authorize certain uses of force based upon their understanding of legitimacy under international law, statements like these reinforce the credibility of the purely deterrent statement.[82] The caveats the White House unilaterally applies to its use of force in this context echo its prior National Security and National Military strategies:

> In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.[83]

These policy statements also squarely ground the United States' self-defensive posture in Article 2(4)'s 'force' standard and Article 51, both important for the following chapter's legal analysis. The reference to military force specifically draws attention to the U.N. Charter's distinctions explored in the previous chapter, making implicit reference to the *jus ad bellum* and *jus in bello* as validating bases for action. As a result, in drawing connection to the international legal framework that would legitimize the act, the United States is seeking to construct the deterrence space to favor its preferred balance — in which a would-be cyberattacker would face the prospect of its overwhelming military capabilities.

[81] *Ibid.*, emphasis added.

[82] Thus, the section's appeal to "inherent" right of self-defense, and therein, that the language in the U.S. President's assertion mirrors that of the U.N. Charter's Chapter VII, Article 51. The next chapter evaluates the durability of this claim, as well as the potential limitations on such a response.

[83] USISC, 14. See also: United States Joint Chiefs of Staff, *National Military Strategy* (Washington: U.S. Department of Defense, 2008).

This credibility of the deterrent is buttressed by its third claim: that it is collective, and that military alliances will interpret cyberattacks in a similarly inclusive manner. The U.S. strategy articulates a basis for what Washington describes as a “regional and international consensus of states” on core security norms in cyberspace (including self-defense), and in a critical but less-cited passage, the U.S. strategy adds, “certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners” — a clear invitation for other treaty partners to share this view.[84]

This view both reflects, and presages invocation of Article 31, paragraph 4(b) of the Vienna Convention on the Law of Treaties, which asserts that a treaty interpretation may also take account of “any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation.”[85] Many of the United States’ defensive treaty commitments stem from either party recognizing and activating rights of self-defense, and so it seems natural that the United States would seek to first establish its own basis for action, and reinforce that basis through treaties premised on the collective exercise of that same right.

The two other strongest examples of nations seeking to elaborate this structural deterrent — particularly in the context of their defensive treaty commitments — are two of the United States’ closest military allies: Australia and the UK.

[84] USISC, 18, 14.

[85] United Nations, "Vienna Convention on the Law of Treaties."

Australia has joined the United States in asserting, in recent years, a clear willingness to respond with traditional military force to a cyberattack — focusing in particular on its grounding in collective defense treaties. Australia has in Joint Statements with the United States routinely highlighted the inclusive view of cyberattacks within international custom, most clearly at the 2011 AUSMIN Summit between the Australian and U.S. Defense and Foreign Secretaries, which focused in large part on the question of cyberattacks in the context of the Australia, New Zealand, and United States (ANZUS) Treaty. That communiqué read, in part,

> Our Governments share the view that, in the event of a cyber attack that threatens the territorial integrity, political independence or security of either of our nations, Australia and the United States would consult together and determine appropriate options to address the threat.[86]

The Australian Defence Minister emphasized at the summit that a "substantial cyber attack" on either country would trigger the ANZUS treaty; reflecting last chapter's conclusion that "we're talking here at a level that is much higher than, for example, people using the Internet, using cyber space to steal commercial or state secrets. We're talking about a significant attack upon the communications fabric of a nation" — precisely the kind of attack the previous chapter defined.[87]

As with the United States, Australia has brought top leadership to shape the discourse on this particular topic. Kevin Rudd (who has served as both Foreign and Prime Minister) reinforced his government's thinking, noting "one cyber attack can cripple an economy for hours and days on end. Let there be no doubt, cyber attacks are not only attack on governments. They can cripple businesses, and Australian

[86] Australia Department of Foreign Affairs and Trade, *AUSMIN 2011: Transcript of Joint Press Conference with Defence Minister Stephen Smith, US Secretary of State Hillary Clinton and US Secretary of Defense Leon Panetta* (Canberra: 15 September 2011).

[87] Simon Mann, "Cyber War Added to ANZUS Pact," *Sydney Morning Herald*, 16 September 2011.

businesses are not immune…[t]hat is why it is critical that this become a formal part of our alliance deliberations."[88] Thus, beyond asserting that Australia might invoke its military capabilities in response to a substantial cyberattack, Australia simultaneously commits allied capabilities to its defense in this respect as well. The combined effect is — if understood — a powerful strategy of structural deterrence, publicly linking those overwhelming capabilities in the hope that they will factor into the developing calculus Australia's adversaries in considering a cyberattack.

Like Australia, the UK has also asserted its willingness and right to mobilize conventional forces in response to cyberattack — both individually and in concert with its American ally.

From a matter of defense policy and with similar deterrent implications, recent UK governments have taken great steps to doctrinally tie cyberattack and defense capabilities to traditional military force. The UK 2010 Strategic Defence and Security Review notes, in somewhat less specificity than its American counterpart, "future conflict will see cyber operations conducted in parallel with more conventional actions in the maritime, land and air environments," and vows to "bring together existing expertise from across Defence, including the Armed Forces […] in a way that integrates our activities in both cyber and physical space."[89] Specific statements by senior officials mirror formal policy. The UK Foreign Minister William Hague said in a widely-publicized interview, "[w]e will defend ourselves in every way we can, not only to deflect but to prevent attacks that we know are taking place," adding in a

[88] Department of Foreign Affairs and Trade, *AUSMIN 2011.*

[89] David Cameron, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, ed. Cabinet Office (London: The Stationary Office, HMG, 2010), 27.

separate interview, "the need for governments to act proportionately in cyberspace…and in accordance with national and international law" — a clear reference to the existing *jus in bello*.[90] UK Defence Minister Nick Harvey points out from a doctrinal standpoint, "cyberspace adds a new dimension, but its use in warfare should be subject to the same strategic and tactical thought as existing means."[91]

Clearly the strategy of structural deterrence is shared between more than a single alliance; the UK, for its part, has reserved some of its more specific statements about international security and cyberspace to joint statements with its American ally. For example, during their May 25, 2011 meeting, the UK Prime Minister and U.S. President asserted, "the same kinds of 'rules of the road' that help maintain peace [and] security […] internationally must equally apply in cyberspace."[92] Cameron and Obama noted a desire to expand consensus about these state rights referred to previously, citing a desire to "continue to build our cyber security alliances, including through the already strong relationship with the United States and the establishment of new relationships with like-minded nations."[93]

This collective enthusiasm for collective, structural deterrence does have limits — and demonstrates the utility and potential peril of this inclusive strategy of structural deterrence. The United States, United Kingdom, and New Zealand appear committed to ensuring the credibility of their structural deterrence project is not

[90] Murray Wardrop, "William Hague: 'Britain Faces Growing Cyberspace Arms Race'," *The Telegraph*, 18 October 2011. William Hague, *Foreign Secretary's Closing Remarks at the London Conference on Cyberspace*, ed. Foreign & Commonwealth Office (London: The Stationary Office, HMG, 2011).

[91] Harvey, *Ibid*.

[92] The White House, *Joint Fact Sheet: U.S. And UK Cooperation on Cyberspace* (Washington: U.S. Government Printing Office, 2011).

[93] Cameron, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 48.

undermined by alliances that might call for but fail to execute a response. In its alliance with North Atlantic Treaty Organization (NATO) members, and its separate security pact with South Korea, the United States appears to be exercising greater cautiousness, resulting in a careful balance between exerting deterrent influence and overexertion that might result in strategic entanglement. If the U.S.-UK and ANZUS alliances show the full measure of a strategy to shape the international environment and bring collective military defense to deter cyberattacks, then the NATO and U.S.-South Korea alliances demonstrate its limits.

NATO has in recent years asserted an ambiguous posture that acknowledges, but does not truly echo, member states' assertions of a collective right of self-defense to cyberattack.[94] NATO claims in public documents to have been considering aspects of cybersecurity since at least 2002.[95] Then, however, the focus was strictly on cyber-defense and force readiness — in essence the protection of NATO and host country's digital systems — and not on the potential activation over the treaty's Articles 4 and 5 on the basis of a cyberattack.[96]

There remains a significant tension within the alliance of the proper role cyber-defense should play — whether the specter of cyberattack should be dealt with as a tactical and strictly defensive or strategic and deterrent matter. The former view

[94] For further background on NATO's strategic challenges and role in cybersecurity issues, see: R. David Edelman, "NATO's Cyber Decade?," in *NATO and the 21st Century: New Security Challenges*, ed. Richard Prosen (Oxford: Oxford University Press, forthcoming).

[95] NATO's own public-facing introduction to the topic highlights, "Although NATO has always been protecting its communication and information systems, the *2002 Prague Summit* first placed cyber defense on the Alliance's political agenda." North Atlantic Treaty Organization, "Cyber Defense: Background & History," http://www.nato.int/cps/en/SID-CC11FE39-6C487843/natolive/topics_78170.htm.

[96] NATO's reasons for approaching the problem thusly stem in large part from recent experience: in 1999, anonymous hackers attempted to overload the Alliance's messaging system in advance of Operation Allied Force.

would devote limited Alliance resources to defending NATO and host country military networks against cyber-threats that might affect planning and force readiness. Countries holding this view, chiefly France and the UK, see NATO's extremely limited cybersecurity capacity on its own networks as indication that the institution is ill-prepared to deal with the strategic implications of a cyberattack, and that such issues are best left to member states defining their rights, for instance in the bilateral context. These countries hereto enjoyed preeminence in the articulation of NATO's defensive posture — characterizing the cyber threat as a principally technical defensive matter, rather than, say, regulated or deterred — and their view is reinforced by the 2010 New Strategic Concept, 2010 Lisbon Summit Declaration, and subsequent statements by the NATO Secretary-General.[97] A vocal dissenting community, however, views the issue as core to the Alliance's continued relevance, and that it must be comprehensively built into NATO's doctrine and planning, including in the context of Articles 4 and 5.[98]

A contrasting view might argue that key Member States in the Alliance have not yet consolidated their views, and that this lack of clarity within NATO is simply a function of a developing, and highly imperfect consensus about the rights of self-defense. Yet that argument ignores the political dynamics of NATO's policy

[97] North Atlantic Treaty Organization, *Active Engagement, Modern Defence: Strategic Conept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (Lisbon: NATO, 2010), 11-12, 16-17. *Lisbon Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Lisbon* (Lisbon: NATO, 2010). "Press Conference by NATO Secretary General Anders Fogh Rasmussen Following the NATO Defence Ministers Meeting on 4 June 2013," news release, 4 June, 2013.

[98] Note the relatively restrained language in NATO's 2010 *New Strategic Concept* in contrast to the pointed statements, in NATO's own publications, by alliance member heads of state such as Estonia's Toomas Hendrik Ilves. See: Chris Riley, "Interview with Toomas Hendrik Ilves: Cyber Attacks, NATO - and Angry Birds," *NATO Review Magazine*, 13 June 2013.

formulation. The United States and United Kingdom are exceptionally influential in the formulation of NATO alliance policy, and would only be encouraged by countries like Estonia were they to seek similar commitments from the Alliance. Therefore it would seem only more important for them to pursue a similar agenda to build like-minded consensus at NATO, and with it, widen the base of their structural deterrent strategy. The United States, the UK, and Australia have practiced no such evangelical restraint in multilateral forums like the U.N. General Assembly, 2010 U.N. Group of Governmental Experts on the issue, or the Organisation for Security and Cooperation in Europe (OSCE).[99] This restraint is therefore less explainable as a glaring omission, and far more so as an intentional practice.

What emerges is a distinct sense of uncertainty not on the application of rights, but on who is to be entrusted with their implications — in other words, a conscious effort to ensure the inclusive strategy of structural deterrent remains *credible*. There is little question that the events in Estonia served to motivate both internal deliberations and public deterrent statements by NATO members and others.[100] If these statements were indeed many years in the making and largely deliberate, implied as well is a detectable (if somewhat contradictory) statement about the limits that states like the United States and United Kingdom seek to impose on

[99] See: any of those nation's submissions to the 2010 GGE. See also: United Nations Secretary-General, "Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General," (New York: United Nations, 2011), Australian Submission (18-23, esp. 22). Organization for Security and Co-operation in Europe, "Remarks of the Coorindator for Cyber Issues, U.S. Department of State" (paper presented at the OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Rule, Vienna, 9-10 May 2011).

[100] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations*, ed. Eneken Tikk, vol. 1 (Tallinn, Estonia: NATO Cooperative Cyber Defence-Centre of Excellence, 2010), Preface, 8.

such rights of self-defense. At the same time, such statements in the alliance context suggest that such claims develop in direct proportion to states' trust of one another if empowered with such a mandate. Specifically, the United States and other NATO states remain conflicted about asserting a full-fledged Article 4/5 response to cyberattacks, fearing *overexpansion* of self-defense rights in ways that might undermine credibility by excessively lowering the threshold of response. They do so perhaps with good reason: as cited previously, NATO member Estonia drew as a matter of policy equivalency between nuclear and cyberattacks.

This anxiety appears manifest in the U.S.-South Korea relationship's present lack of a parallel statement to the U.S.-UK or ANZUS collective deterrent statements. This may stand to reason: the South Korea has, as of this writing, suffered three national-scale cybersecurity incidents.[101] While magnified by the nation's dependence on networked technology (by many accounts the world's highest), all were small to moderate in effect — failing to meet the threshold of those attacks described in this study. Yet official statements out of South Korea in response have often drawn broad conclusions about what occurred, citing "attack," "invasion," and not just a right, but necessity to respond both in-kind and with force.[102] South Korea has thus responded to such incidents with fiery rhetoric that, if given the full weight of American defensive treaty commitments, might commit the latter to a wholly unwanted response.

[101] BBC News, "New 'Cyber Attacks' Hit S Korea," 9 July 2009.

[102] See, for example, interview with South Korean National Assembly member HA Tae-Kyoung, summarizing the government's position and response of the Blue House and President Park Geun-hye. Jong Ik Cho, "Ha Tae Kyoung Interview on the Growing Cyber-Terrorism Threat from North Korea and the South's Response," *NK Vision*, 15 May 2013.

Exclusive Strategy: Cyberattacks as Novel and Unregulated

> "The Parties shall cooperate and act in the international information space within the framework of this Agreement…including the principles of peaceful settlement of disputes and conflicts [and the] non-use of force..."[103]

Naturally, the practice of structural deterrence is competitive. One nation or group of states' interest in shaping the deterrence calculation in their favor will surely find opposition from its potential adversaries. Just as the aforementioned nations have sought to exploit their overwhelming military advantage, a second bloc of states led by Russia and China are practicing a similar but inverse strategy, this one seeking to *deny* those states availability of that force in the event of cyberattack. The latter do so with full and public knowledge that, in the words of Russia's top expert on cybersecurity issues, cyberattacks "are a powerful tool for enhancing military potential."[104] This 'exclusive' or 'exceptional' view is far simpler to document, but no less important in the broader context of self-defense's customary development in international law.

This second camp of states premises the exclusive strategy of structural deterrence on two claims. The first is that cyberspace has circumstances materially different from traditional international security space as to merit exceptional consideration under international law. The second is that states have an obligation to settle disputes pacifically in all circumstances that arise from cyberspace — implicitly but quite obviously excepting them from the *jus ad bellum* and by extension any need

[103] Shanghai Cooperation Organisation, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security* (2009). In Sergei Komov, ed. *International Information Security: The Diplomacy of Peace* (Moscow: Russian Federation Official Publications, 2009), 202-13.

[104] Krutskikh, "Advancement of Russian Inititaive to Ensure International Information Security (Chronicles of the Decade)," *ibid,* 126. Krutskikh is, here, referring specifically to the United States.

for the *jus in bello*. The latter is based on the conviction that accepting the applicability of present law would provide a basis for presumptively lawful armed conflict in cyberspace — and at the margins, a basis of self-defense in response to action previously tolerated, such as aggressive cyber-espionage. These claims combine into a thesis that would deny would-be victims legitimacy in responding with military force to a cyberattack, thus preserving the opportunity to use this asymmetric tool against a better-armed adversary with a more favorable deterrence calculation.

A rich canon of Russian strategic literature and official doctrine has sought to advance this structural deterrence strategy for more than a decade. Writings from top Russian security officials responsible for new and emerging threats as early as 1999 observed "no international laws […] regulate the use of information weapons, to limit them as is done under treaties with other weapon types and military activities."[105] Citing this gap, the same official heighted an "objective needs to legally regulate the world-wide processes […] of information security."[106] Subsequent official doctrine, notably the *Russian Federation Military Policy for Provision of International Information Security*, repeatedly calls for definition of "allowable methods" of cyberattack, noting that "there is no doubt that in order to implement the Russians Federation's military policy in the international information security areas, it is necessary to improve…existing international law."[107]

[105] "Information Challenges to Security (1999)," 12.

[106] *Ibid.*, 13.

[107] *Ibid.*, 32.; Sergei Komov, "Russian Federation Military Policy in the Area of International Information Security: Regional Aspect (2007)," *ibid.*, 43.

It is worth noting an amelioration of this dissent, at least insofar as it relates to the Russian Federation. Prior to the 2008-9 Group of Governmental Experts (GGE), Moscow routinely asserted the insufficiency, and regularly the *outright inapplicability* of international law (meaning, in context, the *jus ad bellum* and *jus in bello*) to cyberspace.[108] One emblematic conclusion, included by the Kremlin as reference points to Russian official doctrine on the matter, concluded, "current national and international legal frameworks are insufficient…to address the scope and complexity of the subject of cybercrime, cyberterrorism and cyber warfare."[109] Joining with consensus in the 2012-2013 GGE, however, Russia signaled for the first time a shift in position, acknowledging that such international law *applied in full* to this space, but not precluding the view it remains generally insufficient.[110]

The motivations of the People's Republic of China are different, but its strategy is generally aligned with the Russian Federation on how to leverage structural deterrence to achieve a favorable deterrence arrangement vis-à-vis cyberattacks.

Consider, for instance, the position of China during those same 2008-9 GGE negotiations — when China actually strengthened its attachment to the exclusive position. A review of that session's negotiating history indicates that, at its penultimate session, the Chinese delegate (sent to replace his predecessor and,

[108] Anatoly A. Streltsov, "International Information Security: Description and Legal Aspects, (2008)" *ibid*.

[109] World Federation of Scientists Permanent Monitoring Panel on Information Security, *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, ed. Henning Wegener (World Federation of Scientists, 2003).

[110] United Nations Group of Governmental Experts (2011-12), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2011-12)* (New York: United Nations (UNIDIR), 2013).

presumably, toe a line more consistent with Beijing's) removed any reference to the Law of Armed Conflict applying to cyberspace.[111] Instead, that language was replaced with a general assertion of the applicability of the *U.N. Charter*, making special reference to non-interference in sovereign matters. The subsequent Draft Code of Conduct circulated in September, 2011 by Russia, China, Tajikistan, and Uzbekistan also went to great pains to avoid reference to "self-defense," while noting the desire to prevent the use of cyberspace to "carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies."[112]

This process is, as mentioned, competitive; Russian documents repeatedly lament how the process of consolidating their positions internationally has been "extremely slow on account of counterproductive attitudes displayed by the United States" and other nations with opposing views on the specific matter.[113] Indeed, an early (2004-5) U.N. Group of Governmental Experts was unable to produce a consensus report due, according to Russian officials, to "the question of whether international humanitarian law and international law sufficiently regulate the security aspects of international relations in cases of 'hostile' use of ICTs for politico-military purposes."[114] In other words, the United States and its allies, Australia and the UK,

[111] Compare, for instance, the United States Expert's submission to China's, and in turn, the final product. United Nations Group of Governmental Experts (2008-9), *GGE (2010)*. On file with Texas Law Review.

[112] See: Russian Federation et al., "Letter to the Secretary-General on a Draft International Code of Conduct for Information Security," (New York: United Nations, 2011).

[113] Komov, "Russian Federation Military Policy in the Area of International Information Security: Regional Aspect," 34.

[114] See, for example: "Contribution by Russian Federation Expert" to the 2010 GGE; SCO Agreement *op cit.*

argued for the inclusive view; the Russians, Cubans, and Belarusians for the exclusive position — producing fundamental deadlock.

On this position's second core feature — that armed self-defense should not be extended to cyberattacks for fear of inviting the creep of larger military forces into cyberspace — it is simple to see how such impressions were formed. For over a year prior to the release of the U.S. Department of Defense's *Defense Strategy for Operating in Cyberspace* (DSOC), the U.S. military and others engaged in what can best be described as a rhetorical campaign of dissuasion. In response, round criticism followed from Kremlin- and Beijing-backed think tanks and press outlets, accusing the United States of stoking a "new cyber arms race," and seeking to exploit "technological superiority" to wage "new forms of aggression" abroad.[115] Subsequent statements, for instance, by the U.S. Secretary of Defense claiming "We are all going to have to work very hard not only to defend against cyberattacks but to be aggressive with regards to cyberattacks as well" only served to stoke this perception with the United States' adversaries.[116]

The result is that in practicing its own form of structural deterrence, Russia in particular has pursued a strategy that would emphasize the illegitimacy of armed reprisal to a cyberattack and deemphasize the invocation of any rights of self-defense. Nearly every bilateral or multilateral agreement or statement submitted by the Russian Federation on the issue of cyberattacks contains binding provisions calling for the

[115] Xinhua News Agency, "U.S. Cyber Strategy Dangerous: Chinese Experts," *China Daily USA* 2011. Igor Panarin, "Supremacy in Cyberspace: Obama's 'Star Wars'?," *RT*, 11 January 2012.

[116] Mann, "Cyber War Added to ANZUS Pact."

pacific settlement of disputes arising from cyberspace.[117] None refer to recourse to armed force, or any of the self-defense rights of the U.N. Charter or mutual defense treaties — in marked contrast to states pursuing an inclusive strategy. In fact, in its first six successive United Nations First Committee resolutions on "International Information Security," the Russian Federation made no mention of the potential for state use of cyberattacks at all.[118] Even in that period, challenges to the legitimacy of military use of and response to a cyberattack were clear, with an initial draft of the resolution noted its purpose was to "prevent military applications [of cyberattacks] that may be compared to the use of weapons of mass destruction."[119]

[117] See, e.g.,: Shanghai Cooperation Organisation, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security*. Russian Federation et al., "Code of Conduct." Association of Southeast Asian Nations (ASEAN) Regional Forum, *Statement by the Ministers of Foreign Affairs of the ASEAN Regional Forum Participating States on Cooperation in Ensuring International Information Security* (Bandar Seri Begawan, Brunei: ASEAN, 2010).

[118] The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of international Security, delivered to the General Assembly, U.N. Doc. A/59/116/Add, 1 (Dec. 28, 2004); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc, A/59/116 (June 23, 2004); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc, A/58/373 (Sept, 17, 2003); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc, A/57/166/Add.l (Aug, 29, 2002); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/57/166 (July 2, 2002); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/56/164/Add.l (Oct. 3, 2001); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/56/164 (July 3, 2001); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly. U.N. Doc. A/55/140/Add.l (Oct, 3, 2000); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/55/140 (July 10, 2000); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/54/213 (Aug, 10. 1999) (providing various state contributions to the Secretary-General).

[119] "Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General," (New York: United Nations, 1998). In Tikk, Kaska, and Vihul, *International Cyber Incidents: Legal Considerations*, 1, 3.

Russia and China's motivations in so doing stand to reason: both seek to prevent escalation of a cyberattack emanating from their territory into a kinetic military conflict in which their adversaries might have decisive traditional military advantage. Moreover, if press accounts and public testimony are to be believed, the volume of malicious activity (cyber-enabled espionage, industrial theft, and low-level attack) emanating from the PRC are substantial and perhaps greater than any other state. Given that, the potential for armed reprisal to China's cyberspace activities might be particularly acute; denying victims of that activity the legitimate use of their strongest deterrent would help create more favorable conditions for preserving an advantageous status quo.

By definition, a successful structural deterrence posture must enjoy reasonable consensus of states, or preponderance of power, to affect the inputs of states' deterrence calculations generally. Russia and China have, in a manner consistent with the one previously documented in the context of the US-UK and ANZUS alliances, sought to export these views. The key venue for doing so has been the Shanghai Cooperation Organisation (SCO).[120] SCO members jointly promoted a baseline Agreement that seems clearly designed to form an initial *lex specialis* for cyberattacks in the context of international security. It enjoys some formal status, having been cited among others by Russian President Medvedev in his 2011 SCO Heads of State meeting.[121] This effort was followed up at the United Nations by a similar text, submitted by most SCO countries but failing to include support from Kazakhstan and Turkmenistan, which the Chinese Foreign Ministry hailed as "the first relatively

[120] SCO member states include: China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan.

[121] Russian Federation et al., "Code of Conduct."

comprehensive and systematic document in the world […] to formulate international rules to standardize information and cyberspace behavior."[122]

By seeking an opposing consensus to the Western bloc, this group has sought to create conditions whereby existing international law — including self-defense exceptions to the prohibition on use of force — are inapplicable to cyberspace. The result, were this approach to succeed in narrowing states' conceptions of available response options to a cyberattack, would deprive them of the ability to use traditional military capabilities to deter a cyberattack. This normative enterprise would have profound effects on the rationalist calculations of states in assessing whether to carry out a cyberattack.

Whose Deterrence Succeeds?

To date, neither the inclusive position championed by the United States, Australia, and the UK, nor the exclusive approach led by Russia and China, enjoys pre-eminence. With so few examples of substantial cyberattacks being used within or outside a traditional military conflict, there have not yet been meaningful test cases. Nonetheless, it is worth probing briefly the prospects for success of these dueling positions, particularly in the context of the specifically rationalist calculations they seek to inform.

In the realist mode, one might observe that as a matter of sheer resources, the members of the Shanghai Cooperation Organisation combined barely constitute half of the defense spending of the United States alone (to say nothing of its treaty allies). Even adding to the former group swing states like India and Brazil (hardly staunch

[122] *Ibid*.

supporters of the exclusive position), their aggregate military spending again does not come close to eclipsing the United States. If structural deterrence positions are to obtain, they require the clear support of large and powerful states able to impose those conditions on others.

Likewise, in a neoliberal mode, one might note the importance of broad institutional coalitions, driving consensus among a plurality of smaller states' views. In this strategy, a state would remain (as Russia has) committed to leveraging international institutions whose designs seek to level the playing field — like votes at the United Nations General Assembly. But even there, as evidenced by over a decade of nearly zero momentum on such proposals to develop a *lex specialis* for cyberattacks, those states with the greatest self-interest in the exclusive view have yet to win enough friends, or demonstrate enough suasion in political-military affairs, to create a culture where their version of self-interest overcomes those of the inclusive view.

Neither of those indications are, however, necessarily predictive. After all, accepting them as such would be to presuppose that national "power," or the current configuration of geopolitics, will inform the outcome of this particular debate — possible, but intellectually unsatisfying. Left out would be the third dimension that structural deterrence introduces: the merits of each particular argument for or against opening the aperture of legitimate responses. That debate's battle lines may be geopolitical in origin, but their substantive, legal basis may inform if not dictate which frame succeeds.

The unsettled nature of this debate creates an opportunity for critical analysis that neither party has yet seized: to evaluate the veracity and durability of states' numerous arguments about the status of cyberattacks within international law. Such a survey of regulative restraint of cyberattacks will be valuable in its own right — as states continue to apply their approach to influencing international law — but, for the reasons just articulated, will also shape the prospects for rationalist restraint of cyberattacks as well. If international law deems cyberattacks an illegal use of force permitting armed reprisal with traditional weapons, the prospects that rationalist deterrence might restrain their use go up exponentially. This is the study that Chapter 3 undertakes.

Conclusion

This chapter explained the imperfect fit of cyberattacks into rationalist international security. As a general matter, any deterrent dynamic requires state recognition of both potential acts of aggression and their likely effect, as well as some reliable sense of their nation of origin. While those general criteria hold for a number of well-known means of coercion, the development, deployment, and execution tools of a cyberattack could only under narrow circumstances form a credible deterrent. The result is that cyberattack capabilities may be powerful instruments of war, but notably weak in projecting power in peacetime.

Just as it is difficult to leverage cyberattack capabilities as deterrents, it is also challenging to deter a state from developing or using those capabilities. In-kind deterrents, in which Asgard would develop a cyberattack capability of its own to deter such an attack by Babel, would leave neither with any greater ability to defend. That condition would more readily lead to an arms race than it would mutual restraint on rationalist grounds. Consequently, hopes for a discrete notion of 'cyber-deterrence' are misplaced; deterring cyberattacks can only be meaningful in the broader context of international security, where the full measure of diplomatic, economic, and military tools can be brought to bear.

Leveraging traditional state power — especially military power — against a would-be cyberattacker is not straightforward. States do not agree on whether or not a traditional military response would be appropriate to a cyberattack. With no custom upon which to base their behavior, even the scope of potential responses to an attack is unclear. Again, the basic inputs of informed, rational deterrence are unclear, making it not just impossible to assess *whether* a state might be deterred, but far more practically, making it difficult for states themselves to determine how to respond to cyber threats. One is left either giving up on this logic of restraint as presently meaningful, or moving beyond rigid strictures that were in most instances architected for a different, bipolar (and explicitly nuclear) era in international relations.

Rationalist deterrence will be impossible until states reach customary or regulative consensus over whether or not militaries can lawfully repel cyberattacks; indeed, states are already seeking to influence that outcome. That process, called structural deterrence, seeks to shape the rationalist outcome through normative and neoliberal means, in which states vie to build legal, bilateral, and institutional consensus for what measures can be used to deter a kind of attack. States are doing so, this chapter argued, with profoundly rationalist motivations: whether in the case of the Western bloc in seeking to deter cyberattacks by tying their response to overwhelming military force, or the Eastern bloc seeking to deny that right to limit prospects for undesired escalation. Both camps are seeking to leverage their various institutional arrangements to further their position, though none presently enjoys consensus.

Most notably though, all of these states are staking the outcome of their deterrence postures on legal claims that they have not fully articulated, and that scholars have not fully scrutinized. Whether rationalist deterrence meaningfully restricts state use of cyberattacks hinges on the ‘victor’ of this structural project; that debate, in turn, ultimately depends on the durability of the international-legal arguments in its favor.

The balance of this study conduct such a critical analysis: first, whether there is any merit to state claims that cyberattacks constitute an illegal use of force invoking a right of self-defense (Chapter 3); and second, the prospects a cyberattack might be a prohibited act under the law governing just conduct in war (Chapter 4). While each represents a distinct regime shaping state action, this chapter has demonstrated that the interconnections between them are equally impossible to ignore.

Chapter 3:

Cyberattacks and the *Jus ad Bellum*

TABLE OF CONTENTS

As the last chapter outlined, states are staking entire deterrence strategies on how international law might treat cyberattacks, but doing little to justify those claims. Specifically, many are invoking the United Nations Charter as evidence of cyberattacks' illegality and states' "inherent" right to defend against them. But do those claims have any basis in international law? Can the *jus ad bellum*, or canon of law limiting states' recourse to force, apply to cyberattacks, and can it meaningfully restrain states contemplating cyberattack — either directly, or by empowering victims to respond with force? This chapter addresses those questions, which are important in their own right, and essential to the outcome of both the structural deterrence process outlined in Chapter 2 and the relevance of the *jus in bello* that Chapter 4 will discuss.

This chapter has two interrelated parts. First, it considers whether or not cyberattacks might be recognized as a prohibited use of force of the sort described by U.N. Charter Article 2(4). Only if cyberattacks are recognized as meeting this threshold might the legal framework and the customary practice fashioned around it be activated, and might the U.N. regime provide a means to restrain cyberattacks. Recognition of potential illegality is, of course, only half the picture. Therefore the second half of this chapter examines whether a cyberattack would therefore also invoke rights of self-defense, and the conditions the law would place on deploying a forceful response. Together, both conclusions determine whether the *jus ad bellum* framework might be a meaningful force of restraint.

Argument and Scope of the Chapter

This chapter argues that, through numerous interpretations of U.N. Charter framework, cyberattacks are illegal and actionable uses of force under existing international law.

It begins by problematizing the popular conception of 'cyberwar,' arguing that the neologism adds little and distracts from a more relevant debate over how existing international law and custom apply to the act. Recognizing then that states' cyberattack decisions will certainly be judged by existing international law and practice, I argue in the next section why, in the absence of cyberattack-specific law, the *jus ad bellum* and specifically the U.N. Charter offer the most useful framework for such an analysis. I then argue that cyberattacks might invoke the core provisions of the *jus ad bellum*'s foundational statute, the Charter's Article 2(4), and explain how several interpretations of it cover cyberattacks — as recognizably military instruments, and confirmed by the effects they cause. I conclude that cyberattacks are clearly presumptively illegal, but that illegality is on its own likely insufficient to reliably restrain state behavior.

The chapter then turns its focus to the part of the *jus ad bellum* that might enforce such a restraint: the Charter's remedial provisions. There I argue that it is too early to consider whether the U.N. Security Council may have a restraining effect, but that the "inherent" right of self-defense enshrined in Article 51 may be immediately powerful. Even accepting a narrow scope for that right of self-defense, I argue that a self-defensive response is clearly lawful, if certain well-understood conditions were met: namely if the attack had sufficient gravity, had a military effect, was attributable, and could be stopped by the action contemplated. Finally, I argue that cyberattacks may reinvigorate debates over the need to consider the attacker's intent as part of judging rights of self-defense.

The conclusion of this section, and the chapter as a whole, is that ample legal basis exists to render cyberattacks illegal and actionable within the *jus ad bellum*. International law can thus be a strong restraint on state use of cyberattacks, provided that states exercise it and establish a custom on that basis.

3.1 The Misleading Concept of 'Cyberwar'

Does a state's use of a cyberattack against another state bring the two into a state of 'cyberwar'? In recent years, popular literature has been rife with claims that the use of computer networks in interstate coercion might herald in a new era of strictly digital conflict. One of the most cited popular monographs takes this neologism for its title, and a cottage industry has sprung up defining and debunking for policymakers the concept of 'cyberwar.'[1] Therefore, before embarking on any more disciplined study of 'war' as recognized by states, it is

[1] See, for example: Clarke and Knake, *Cyber War*; Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2009). For counterpoints, see: Rid, *Cyber War Will Not Take Place*; Seymour Hersch, "The Online Threat: Should We Be Worried About a Cyberwar?," *The New Yorker*, 1 November 2010.

worth briefly evaluating the utility of this particularly evocative concept in the field.

For the purposes of rigorous study, the ‘cyberwar’ premise remains undeveloped and, this section argues, perhaps with good reason. The phrase is both overly broad and underdetermined, applying the moniker of war to actions that may not meet such a threshold, and assuming a special category for digital conflict without demonstrating why present law and practice would not apply.

The problems begin with the definition of ‘cyberwar,’ which encompasses far more state activity than is analytically useful. Taking Clarke’s definition as emblematic, “cyber war…refers to actions by a nation-state to penetrate another nation’s computer networks for the purposes of causing damage or disruption.”[2] The concept draws attention first to the technology or method of coercion, and second to a condition of interstate hostility. The former is unproblematic. It is the latter aspect, the reference to ‘war,’ that ultimately undermines the utility of the phrase as it is used in volumes like Clarke’s.

In its use of ‘war,’ at least as war is recognized within contemporary international relations, the concept does not stand up to much scrutiny. The definition put forth by Clarke begins by widening the definition of what constitutes war in ways incompatible with, and unhelpful to, understandings of war. Taken on its own, ‘cyberwar’ loses precision by designating as warlike any activity that involves penetrating computer networks, with no reference to the effects of this primary action, for the purpose of damage or destruction of an undefined intensity or magnitude. Indeed, within this definition acts of

[2] Clarke and Knake, *Cyber War*, 6.

‘cyberwar’ do not meet a reasonable threshold of significant interstate coercion. Examples of activities meeting the ‘cyberwar’ threshold range from the absurd, such as one state’s agents hacking into foreign computers to delete an embarrassing photo of a political leader, to the relatively benign, such as a computer security team shutting down the service of a botnet wreaking havoc on local Internet service providers.[3] To be sure, this is not ‘war’ as understood within international relations, with its constituent severance of diplomatic ties, a state of recognized hostility, and impending or recently endured loss of life.

The alternative and more nuanced reading of the ‘cyberwar’ premise is that this activity is warlike in its hostilities, but falls outside the regimes and definitions that the term ‘warfare’ normally invokes. Consider, for example, how Clarke’s definition of ‘cyberwar’ falls outside L. Oppenheim’s well-known definition of war:

> “…a contention between two or more States through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases.”[4]

Against this definition, cyberattacks do create some novel challenges. ‘Armed forces,’ would likely be involved in a cyberattack, though combatants may not be easily recognizable as such. The conditions of desired peace might be largely unknown at the time of cyberattack and might not be able to be imposed by cyber

[3] A *botnet* is a number of Internet-connected computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a “zombie” or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. According to Russia-based Kaspersky Labs, botnets — not spam, viruses, or worms — currently pose the biggest threat to the Internet’s overall health.

[4] L. Oppenheim, *International Law, a Treatise*, vol. 2 (London: Longmas, Green and Co., 1912), 60. Dinstein also uses Oppenheim’s seminal work as a point of departure for his own critique of international law’s definitions of warfare.

means, in the way a territorial occupation might. Finally, it may not even be possible to know the identities of one or more of the belligerents, which is the fulcrum of Oppenheim's definition. In this respect, Clarke is right to seek a more accommodating definition to describe this new phenomenon.

The field of international security has adapted its definitions before, and more modern approaches to defining the conditions of interstate conflict can fully internalize the practice of cyberattacks. For instance, a compatible definition of 'war' can be found in Yoram Dinstein's seminal work, in which he draws a useful distinction between "war in the material sense" and "war in the technical sense."[5] His is a particularly important definition of war in an era of frequent, limited, and intra-national conflict. Dinstein highlights that war as we know it has a *material* recognizability, such as the use of weapons to kill and armies to occupy territory, and is a *technical* condition of interstate relations, activated by such means as a unilateral declaration or by the recognition of an "armed attack" externally adjudicated, such as by the United Nations Security Council.

Given such versatile yet distinct concepts of 'war,' it is at least possible to chart the course of how the 'cyberwar' concept might have explanatory power, were its further premises not flawed. Underlying the 'cyberwar' literature are two dubious claims. First, the literature claims that the use of computer networks heralds a paradigm shift in the general practice of warfare, in which cyberattacks supplant kinetic attacks as a principal means of coercion. Second, it posits that cyberattacks are inaccessible to international law and custom, representing instead

[5] Yoram Dinstein, *War, Aggression and Self-Defence*, 4th ed. (Cambridge: Cambridge University Press, 2005), 9.

a form of as-yet-unrecognized permanent interstate conflict defined by tit-for-tat network disruption between strategic competitors.

The first such claim would demand a revision to the concept of war in the material sense. Certainly, there is growing evidence that states are amassing the capability to use cyberattacks as instruments of power.[6] But this is hardly novel; after all, states have been using various forms of electronic jamming and disruption for almost half a century. It is difficult to see how a 'cyberwar' would be conceptually distinct from war, which by its very nature would likely involve a full range of technologies including, but not limited to, network disruption tools. Public positions of states suggest a retreat from (or at least interest in containing) the notion that serious cyberattacks might become commonplace absent broader armed conflict.[7] Even the U.S. military general appointed with the task of national defense in cyberspace, Keith Alexander of USCYBERCOMMAND, conveyed in public testimony his skepticism of even the possibility of an independent 'cyberwar.'[8] It seems clear that in this respect, 'cyberwar' is grounded neither in a legal definition of 'war,' nor in the common practice of states as it relates to conflict of the sort regarded as such.

[6] McAffee and Good Harbor Consulting, *Virtual Criminology*.

[7] In fact, a cursory discourse analysis of public statements by the United States government in the period 2009-2010 demonstrates the conscious abandonment of the phrase, most notably by the U.S. White House and subsequently the U.S. Department of Defense.

[8] Committee on Armed Services, United States Senate, *Hearing to Consider the Nomination of Lt. Gen. Keith B. Alexander to Commander, U.S. Cybercommand*, 15 April 2010. Alexander: "[A cyberwar] would not exist in itself but as part of a larger military campaign. I believe the tools and stuff for command and control that we have today to effect those in cyberspace are analogous to the tools that we had 40 years ago for jamming communications, but now, in cyberspace, you can not only jam, but you can do a lot more to information. And therein lies part of the problem."

The second claim — that a special condition of ‘cyberwar’ might be necessary to understand the use of cyberattacks by states — is more intriguing and relevant to this study, though ultimately difficult to sustain. The question it presents is whether, to accommodate cyberattacks, we need to reform our understanding of war in the technical sense. The problem is that the mere concept of ‘cyberwar’ presupposes the answer to that question by creating a new concept, and its key proponents have done little to document that assumption. So while claiming variously that nations are presently engaged in a low-level ‘cyberwar,’ or warning that the next major international conflagration will be either ignited by or fought via competition in cyberspace, none document why such practices would fall outside existing international law and custom.[9]

In sum, the notion of ‘cyberwar’ should be left behind in international relations. It is unhelpful because the assumptions behind it are underdeveloped; they are underdeveloped because its most important premise, that existing international law and custom are incompatible with cyberattacks, is suspicious. As this study argues, it is premature to argue and unwise to assume that states will extricate cyber activities from the legal and political context in which they presently operate. International law, in particular, seems highly applicable to state use of a cyberattack. That latter topic is a notable lacuna in the literature, and the subject of the balance of this chapter.

[9] Mike McConnell, "How to Win the Cyber-War We're Losing," *The Washington Post*, 28 February 2010; Clarke and Knake, *Cyber War*, 6.

3.2 Sources of International Law Regulating Cyberattacks

International law restraining the use of cyberattacks could take two forms, which ultimately more accurately reflects the current state of the development of international relations governing that practice. If there existed a *lex specialis*, or specific corpus that applies exclusively to cyberattacks, it would be especially powerful for these purposes. The alternative would be applying more familiar *lex generalis,* designed to be applicable to a range of state activities, to the practice of cyberattacks in order to determine fit. This section traces the sources, status, and shortcomings of the former, before turning the attention of the subsequent sections to the more extended project of evaluating the latter.

***Elusive* Lex Specialis**

In pursuing international law that might explicitly apply to state use of cyberattacks, one might turn to a range of potential sources that already exist. The International Court of Justice's Statue Article 38.1(b), articulating the scope of the Court's consideration, is generally accepted as an authoritative listing of the sources of international law more broadly. It cites four main sources: (a) international conventions…establishing rules expressly recognized; (b) international custom; (c) the general principles of law as recognized by civilized nations; and (d) judicial decisions and other "teachings of the most highly qualified publicists of the various nations."[10]

Beginning with those sources that can be quickly dispensed with, there have thus far been no ICJ or other equally eminent opinions relating to

[10] United Nations, *Statute of the International Court of Justice* (1946), Chapter II: "Competence of the Court," Article 38.

cyberattacks, or for that matter cyberspace. As has already been discussed, academic treatments of the subject have been vastly outpaced by popular works that, at time of this writing, remain primarily policy-focused in their appeal and analysis. Those that might be considered the work of "highly qualified publicists" are featured throughout this work, but little international consensus has accorded such status upon the commentators of this subject as of yet.

Evidence of a convention or treaty-based *lex specialis* relating to coercion in/via cyberspace is equally difficult to locate. Perhaps the clearest indication no such text exists is the decade-long dispute between the United States and Russian Federation over the need for such a 'global cyberspace treaty.' Russia has, through annual resolutions in the United Nations First Committee,[11] sought Member States' views on "information security," with a particular view towards regulating interstate acts of "information attack."[12] The United States, Canada,

[11] G.A. Res. 65/201, U.N. Doc. A/RES/65/201 (30 Jul. 2010); G.A. Res. 64/25, U.N. Doc. A/RES/64/25 (2 Dec. 2009); G.A. Res. 63/37, U.N. Doc. A/RES/63/37 (2 Dec. 2008); G.A. Res. 62/17. U.N. Doc. A/RES/62/17 (5 Dec. 2007); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (6 Dec. 2006); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (8 Dec. 2005); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (3 Dec. 2004); G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (8 Dec. 2003); G.A. Res. 57/53, U.N. Doc. A/RES/57/53 (22 Nov. 2002); G.A. Res. 56/19, U.N. Doc. A/RES/56/19 (29 Nov. 2001); G.A. Res. 55/28, U.N. Doc. A/RES/55/28 (20 Nov. 2000); G.A. Res. 54/49, U.N. Doc. A/RES/54/49 (1 Dec. 1999); G.A. Res. 53/70, U.N. Doc. A/RES/53/70 (4 Dec. 1998).

[12] For national views, see: See The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/64/129/Add.l (Sept, 9, 2009); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N, Doc. A/64/129 (July 8. 2009); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly. U.N. Doc. A/63/139 (July 18. 2008); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly. U.N. Doc. A/62/98/Add.I (Sept, 17, 2007): The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/62/98 (July 2. 2007); The Secretary-General, Developments in the Field of Information and Telecommunications In the Context of International Security, delivered to the General Assembly, U.N. Doc. A/61/161/Add.l (Oct. 31. 2006); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security: delivered to the

the United Kingdom, and others have strongly opposed this view in their own annual submissions.[13] It is clear that those countries registering opinions intend for their views to serve as a basis for, if not the source of, customary international law. Statements of opinion do not themselves reflect a consensus of the sort described in Article 38'a §(b) or (c) — despite being the longest-running regular consultations on the issue at the international level.

Some commentators have also suggested that Article 42 of the International Telecommunications Union's Constitution and Convention — the U.N. body's treaty-level governing document approved by all of its Member States — serves the *specialis* function sought here.[14] That article of treaty law does, *prima facie*, proscribe states from "harmful interference their administration might cause to the radio services of other Member States."[15] Besides problems of ascribing such intentionality to a nearly 150-year-old series of articles, that section governs not Member State behavior writ large, but the maintenance of Special Arrangements concluded between them in the service of global telegraph, and now telecommunications, networks.

General Assembly. U.N. Doc. A/61/161 (July 18. 2006); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/60/95/Add.I (Sept, 21. 2005); The Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly. U.N. Doc. A/60/95 (July 5, 2005); *Op cit.* p. 118 footnote 68.

[13] Ibid.

[14] Richard Hill, "WCIT: Failure or Success, Impasse or Way Forward?," *International Journal of Law and Information Technology* 21, no. 3 (2013): 8.

[15] "Constitution of the International Telecommunications Union," in *Constitution and Convention of the International Telecommunications Union*, *S. Treaty Doc. No. 104-34* (2010), Article 42.

The extent to which existing regional regulations — such as those of the Council of Europe or European Union — might shape international law's interpretation of cyberspace would be more useful in another context. In Europe for instance, there exists enough legislation and procedure on the topic of cyberspace to fill an entire volume with source material from the Council of Europe, EU, G8, OECD, and OSCE.[16] Nonetheless, these varied laws do not focus on the topic of *interstate* coercion beyond the context of criminal enforcement.[17] There is of course much to be explored in this distinct field of study, as cyberattacks also open a range of domestic legal and international criminal law issues outside the scope of this study.

It is clear that while some national laws and international agreements might relate tangentially to the action of cyberattack in the criminal context, none constitute a *lex specialis*. The final candidate, then, is the potential for international custom relating to this particular practice. Yet it is precisely the lack of international custom with regard to cyberattacks that motivates this inquiry. When Estonia suffered denial-of-service attacks in 2007, with significant impact on government services and society, Estonian officials claimed it had suffered the equivalent of an attack by weapons of mass destruction.[18] NATO's response was one principally of doctrinal confusion and consequent inaction. Were Russia directly or partially responsible, it seems reasonable from the circumstances that

[16] Eneken Tikk, ed. *Frameworks for International Cyber Security: Legal and Policy Instruments.*, vol. 1 (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2010).

[17] In fact the only treaty-level document obviously relating to the topic is the Budapest (Council of Europe) Convention on Cybercrime, which would again subsume such acts of interstate aggression to the law enforcement context.

[18] United Press International, "NATO Will Lay out New Plan for Cyberwar," 10 March 2008.

Moscow had no intention of resorting to kinetic war over the dispute. Even this one-off, small-scale incident demonstrates three conflicting perspectives — none with the apparent upper hand — on the customary consequences of this kind of attack. Throughout this study, we will examine other examples of state practice that might form the basis of emerging 'international custom.' Each will draw from state experience in other contexts though, as it simply seems too early, and number of relevant incidents too few, to form the basis of state custom that might form a cyberattack-specific corpus of international law.

In the absence of compelling *lex specialis*, present study must turn to the *lex generalis* that would govern cyberattacks as a potential act of interstate coercion. In this context, two obvious regimes of international law might be in different ways applicable — the *jus ad bellum*, which this chapter will discuss, and the *jus in bello*, an altogether more specific canon of law that is the subject of the next chapter. The *jus ad bellum* offers a particularly interesting and significant legal test. First, analysis within it offers a very real prospect of cutting through the assumed novelty of the technology and meaningfully (and practically) situating it within well-understood paradigms of interstate conflict. There is also little doubt in Clarke's contention, echoed by other modern war theorists like Singer, that digital systems will become an increasing part of the modern military experience.[19] With so many militaries rushing to integrate these types of capabilities into their kinetic arsenals, determining whether or not the *jus ad bellum* recognizes cyberattacks is more than just a test that is relevant to the

[19] Peter Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: The Penguin Press, 2009).

cyberspace; it may be a profound referendum on the modern relevance of and future prospects for the entire *ad bellum* regime.

Applicable **Lex Generalis***: U.N. Charter & the Jus ad bellum*

The U.N. Charter is a natural starting point in situating cyberattacks within interstate conflict. As a legal document, the key objectives of the U.N. Charter are to recognize acts of armed coercion and set out the mechanisms to limit them. Analytically, the United Nations Charter, and in particular Article 2(4), offers the most robust evaluative framework judging the legality of coercion in international politics. Specifically, it serves as the bedrock for the recognition of the use of force; it forms the basis of the international legal standards governing the *jus ad bellum*, "the first expression of the basic rules [regulating the use of force] in their modern form."[20] The Charter's terminology has even become the basic vocabulary for identifying and evaluating uses of force in the international system.[21]

This is not to say that Article 2(4) is without challenge, but rather that it is without peer in terms of a codified and recognized *jus ad bellum* regime. Certainly, following the U.S. invasion of Iraq, substantive challenges regarding intervention and pre-emptive self-defense led even the U.N.'s own Secretary-General to deem the international community at a "fork in the road" regarding use

[20] Christine D. Gray, *International Law and the Use of Force*, 3rd ed. (Oxford: Oxford University Press, 2008), 4.

[21] Article I of the Kellogg-Briand Pact, for instance, condemned the "resort to war," which the cynical practitioner of international politics might simply use as semantically flexible, relegating most belligerence beneath the threshold of war (as we have seen, a somewhat content-free distinction). Article 2(4), rather, makes significant improvements by introducing the new and rather more nuanced vocabulary of the "use of force." See: Albrecht Randelzhofer, "Article 2(4)," in *The Charter of the United Nations: A Commentary* (Munich: C.H. Beck, 1995), 111.

of force "no less decisive than 1945 itself, when the U.N. was founded."[22] The final sections of chapter will examine those questions. Even with these challenges, however, the U.N. Charter system remains the reference point of the *jus ad bellum,* case law, and scholarship, and must be our analytical starting point.

3.3 Cyberattacks as an Article 2(4) Use of Force

This section analyzes the basis for considering cyberattacks a "use of force," the state behavior that is most straightforwardly prohibited by Article 2(4).

Article 2(4) states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[23] According to Christine Gray, "states and commentators generally agree that the prohibition is not only a treaty obligation but also customary law and even *jus cogens,* though there is no comparable agreement on the exact scope of the prohibition."[24] The article's basic proscription on the use of force outside of the narrow provisions permitted for self-defense (per Article 51) or pursuant to Security Council action (per Chapter VII), has been reaffirmed in its basic content numerous times, in General Assembly Resolutions, Security

[22] Kofi Annan, *Address of the Secretary-General to the General Assembly (23 September)* (New York: United Nations, 2003).

[23] Charter of the United Nations, Article 2, para 4.

[24] *Case Concerning Paramilitary Actions In and Against Nicaragua (Merits)*, ICJ Reports (1986). (hereafter *Nicaragua.*) 14, para 190. Note that the concept of "threat of force" falls outside the scope here, but further resources in this regard can be found in: Nikolas Stürchler, *The Threat of Force in International Law* (Cambridge: Cambridge University Press, 2007); Marco Roscini, "Threats of Armed Force and Contemporary International Law," *Netherlands Law Review*, no. 54 (2007): 229; Gray, *International Law and the Use of Force*, 8.

Council Debates, and by the International Court of Justice.[25] It has been operationalized in the form of Article 4 of the NATO alliance, which declares, "[t]he Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened."[26]

Assessing the provision's relevance to cyberattacks, two questions leap to the fore: first, might a cyberattack be recognizable as a use of force by nature or its effects, and second, how might a cyberattack threaten a state's territorial integrity, political independence, or run afoul of the U.N.'s purposes? The balance of this chapter argues that there may well be grounds upon which cyberattacks are illegal under Article 2(4), both generally as uses of force, and of the sort specifically recognized by the more 'specific' provisions about territorial integrity, political independence, and the purposes of the UN. It also addresses the most common rejoinder by outlining why cyberattacks would not be exempted as 'force' simply because the instrument of attack is not exclusively military, nor because its damage is principally economic.

Since this is perhaps the only topic on which there exists literature regarding cyberattacks in international law, this section uses as its starting point those earlier analyses. First it critically examines those early works, and argues that the methodological tools of established scholarship lay a strong foundation

[25] *See*: Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, G.A. Res. 2131 (XX) (1965) (hereafter cited as *Intervention)*; Declaration of the Principles of International Law, G.A. Res. 2625 (XXV) (1970) (hereafter cited as *Principles)*; Definition of Aggression, G.A. Res. 3314 (XXIX) (1974) (hereafter cited as *Definition)*; *Nicaragua.*

[26] *North Atlantic Treaty*, Article 4.

for recognizing what we know today as ‘cyberattacks’ to be illegal force. It next evaluates how ‘coercion’ becomes ‘force’ from the standpoint of the ‘instrument’ of a cyberattack, rather than its effects. It argues for several key criteria to distinguish forceful acts from those beneath that threshold. Though I conclude that these criteria clearly label cyberattacks as uses of force, I argue that it is also important not to entirely jettison a consideration of effects, which can offer helpful confirmatory analysis in a manner clearly supported by the Charter regime. After using a cyberattack’s effects to confirm this result, the section concludes that under both restrictive and expansive readings of Article 2(4), cyberattacks classify as a use of force.

Earlier Scholarship on Cyberattacks as Uses of Force

A decade ago, when a number of early papers on cyberattacks emerged, two primary issues preoccupied and served as unnecessary stumbling blocks for that early scholarship. Many began by focusing on the legal debate over whether or not political and economic methods of coercion were excluded under Article 2(4), and whether a cyberattack therefore legally has more in common with a sanction, or an attack. Accepting that acts were to be judged by their characteristics as instruments rather than their effects, though, scholars like Schmitt and Silver were then perplexed by the fact that most cyberattacks appeared to be primarily economic, rendering them ‘lesser’ acts not covered by a strict reading of Article 2(4).[27]

[27] Silver, "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter," 80-82; Schmitt, "Use of Force," 901-4.

To preface this discussion, it is important to locate the origins of the conclusion that held back much of the earlier scholarship — primarily, the exclusion of economic and political means of coercion as ‘lesser’ uses of force. The concern is well founded; the majority of scholarly opinion appears to favor this view that, regardless of method of analysis, strictly economic and political coercive measures do fall short of the “use of force” standard.[28] Many point to the *travaux préparatoires* of the Charter, and that the San Francisco Conference failed to adopt a proposal to extend the use of force to economic sanctions, implying their exclusion a lesser category.[29] Here, the elaboration process of the term “use of force” is quite relevant, particularly the *Nicaragua* case at the International Court of Justice (ICJ), which singled out the 1974 *Definition of Aggression* and the 1970 *Declaration on Friendly Relations* to identify customary law on the issue.[30] Proponents of the restrictive view therefore note that economic and political instruments are never codified as ‘functional’ uses of force, and separated explicitly from the supplemental view offered by the 1987 *Declaration on the Non-Use of Force*.[31] On its own, then, this majority,

[28] See also: Jack Plano, Lawrence Ziring, and Roy Olton, *International Relations: A Political Dictionary* (Santa Barbara: ABC-CLIO, 1995), 358.

[29] For further context, see: Edward Gordon, "Article 2(4) in Historical Context," *Yale Journal of International Law* 10 (1985).

[30] The Nicaragua case focused on whether or not certain kinds of support furnished to third-party fighters constituted prohibited ‘armed force’ under the U.N. Charter. Among its many conclusions was that providing financial and logistical support to third parties was not tantamount to complicity in armed force conducted by the recipients. That judgment has been important, and viewed by some as confirming the status of, similar distinctions between “use of force” and “lesser acts" drawn by the U.N. General Assembly in the cited Resolutions. See: *Military and Paramilitary Activities in and against Nicaragua (Nicaragua V. United States of America), Merits, Judgment*, ICJ Reports 14, para 189, 98 (1986). (Hereafter cited as *Nicaragua.*) See also: U.N. G.A. Res. 3314 (1974); U.N. G.A. Res. 2625 (1970).

[31] U.N. G.A. Res. 42/22 (1988).

restrictive definition of ‘force’ is impossible to ignore. If, however, political and economic acts are excluded, how is one to adjudicate whether or not an act falls within these categories?

Methodology Evaluating a Use of Force: Instrument or Effect?

Here the methodology and analysis of the early scholarship on cyberattacks is particularly helpful. As a starting point, it seems clear that the determination of relevance in a “use of force” test is made on the basis of the instrument used, and not the effects caused. Therefore, if the use of a military instrument has economic and political consequences, its 2(4) status relies exclusively on the legally relevant military nature. The converse, however, is not true; economic or political instruments with military externalities would be considered lesser acts.

The most common defense of the instrument-based approach comes as a means of distinguishing it from other, lesser acts of coercion — which, by and large, tend to be evaluated on the basis of their effects.[32] In the simplest cases, it appears to suffice. Causing a crisis within a state’s military through economic sanctions on arms transfers is not a use of force; using bombers to destroy a state’s stock exchanges would be.

Cyberattacks, however, are far more complex, and demand flexibility that this instrument-exclusive evaluation simply does not offer. A more sophisticated argument would accept ways of identifying a particular kind of instrument beyond such a rigid taxonomy. More compelling and useful then is the notion that this

[32] See: Silver, "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter," 87, in particular his critique of Sharp’s “destructive effect” standard.

instrument-based classification is meant as a ‘prescriptive shorthand’ to what is at its core an exhaustive consequence-based rationale within the overall context of the U.N. charter.[33] Such an approach is based on the idea that “because the results of applying economic and political instruments generally constitute lesser threats to shared community values, the “use of force” standard serves as a logical breaking point in categorizing the asperity of particular coercive agents.”[34] This is the evaluative mechanism that Schmitt uses in his most comprehensive legal study of Article 2(4) and cyberattack concepts. In it, he argues that in order to make assessments within the existing international framework, instrument-based analysis cannot simply be ignored in preference of effects, as it is in works such as Silver’s. However, cyberattacks do not naturally lend themselves to instrument-based analysis, hence this complex rationale for what is ultimately a standard evaluation. This view is largely compelling; it accommodates both differences between unfriendly state acts and outright uses of force, and the need for more nuance and complexity in judging borderline candidate actions.

Schmitt’s work a decade ago proposed that cyberattacks fell short of the use of force. His analysis was ultimately encumbered by the state of technology in the era, when the level of interconnection between public and private systems was less profound. Nonetheless his methodology still holds true today — particularly this nuanced approach to the instrument-versus-effects question. Today there is a clear need to revisit that analysis in the context of the increased damage that cyberattacks might do, and the increasing dependency of militaries,

[33] Schmitt, "Use of Force," 917.

[34] *Ibid*., 912.

economies and societies upon them. Schmitt's provides an ideal framework to conduct it, under these changed circumstances.

Therefore, the three subsections that follow ask longstanding questions in a new context: must 'force' be 'military' force; must its instrument be recognizably military and how would one go about identifying it as such; and if this instrument-based analysis is not entirely conclusive, are there further grounds for identifying a cyberattack as a "use of force?"

Must Force be 'Military'?

Very little consensus exists on whether Article 2(4)'s scope is limited to use of 'armed' force in the sense of it being military in nature or execution. Randelzhofer regards the "use of force" used in Article 2(4) as something of an anomaly, claiming that in the context of paragraph 7 of the Preamble, as well as Article 44, the term 'force' in 2(4) "clearly means armed force."[35] He further claims that the subsequent *Friendly Relations Act* adopted by the General Assembly in 1970 clarifies the term in that it "deals solely with *military* force."[36] Yet that Act is hardly sufficient interpretation to of the Charter to be satisfying in the given context, and as Dinstein points out, the "the expression of 'force' is not preceded by the adjective 'armed,' whereas the phrase 'armed force' appears elsewhere in the charter."[37] There is something of a paradox here, as Dinstein

[35] Albrecht Randelzhofer, "Article 2(4)," in *The Charter of the United Nations: A Commentary*, ed. Bruno Simma (Munich: C.H. Beck, 1995), 112.

[36] *Ibid*.

[37] Dinstein, *War, Aggression and Self-Defence*, 85-6.

further claims “the term ‘force’ in Article 2(4) must denote…military force.”[38] The “armed attack’ standard that is routinely used in the remedial context in the U.N. Charter is not the same as the more nuanced, expansive “use of force” broadly asserted in Article 2(4)’s prohibitive context. “Armed attack” is far more explicit and evocative of kinetic and military attack than simply ‘force.’

A balance must be struck then between a generic notion of ‘force’ in the Charter’s prohibitive text, and the explicit requirement of “armed attack” in its remedial sections to which we will shortly turn. That middle ground, and indeed the most straightforward, would accept that ‘force’ must be implicitly ‘military’ — but also accepting that the concept of ‘military’ force can be a dynamic one since, as Silver points out, “as the techniques of warfare evolve, so too does the general understanding of what constitutes ‘military’ force.”[39] The corollary to this approach is that we must exclude *strictly* political and economic instruments of coercion the definition of illegal ‘force.’ Given the clear distinction in location and terminology between the prohibitive and remedial sections of the U.N. Charter, this reading seems fully consistent with the law itself.

The rest of this chapter will therefore focus on what (in the prescriptive shorthand approach) defines a ‘military’ *vice* lesser instruments of coercion, and whether or not cyberattacks possess those attributes.

[38] *Ibid.*

[39] Silver, "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter," 84.

Cyberattacks as Identifiably Military Instruments

There are in fact several general qualities that make military coercion distinguishable from its economic and political counterparts.[40] These include the *immediacy* of an attack (rather than those that take time to have an effect, like sanctions), *directness* (with consequences directly tied to the aggressive act, rather than requiring contributory factors to operate), *invasiveness* (occurring physically in the victim state, violating sovereign rights), and *criticality* (designed to multiply, rather than limit, disruption). Cyberattacks, as instruments, satisfy all these criteria.

Immediacy. Electromagnetic signals travel at the speed of light, and the effects of a cyberattack would take place within seconds of commencement, likely without warning.[41] Not all cyberattacks' consequences would be immediate (for instance, it may take time for a public utility system controlling an oil pipeline to overload), but by definition if the core component or instrument of a cyberattack is an electromagnetic signal, or the disruption thereof, the attack itself is near instantaneous.[42] Even in kinetic cases, the disruption caused by the cutting of fiber-optic cables or destroying network hubs is immediate and system-wide. The

[40] This analysis draws from Schmitt's own taxonomy in "Use of Force," pp. 914-5, but differs considerably in emphasis and removes several components that seem in the present context somewhat strained. Most importantly, while that taxonomy attempts to provide a framework for evaluating particular events as a use of force, this broader framework seeks to demonstrate how cyberattacks as a broad category may run afoul of Article 2(4).

[41] More precisely, while electro-magnetic signals travel at the speed of light, there is indeed a perceptible period between execution and effect — usually (in the case of a cross-global attack) on the order of a second or two, as signals relay through cables, across switches and transoceanic cables, and are ultimately received and processed by the recipient computer. Nonetheless, because of the nature of the Internet's 'packet-switching' technology, the net result of zero *warning* for victim states is most significant.

[42] The 'directness' criterion outlined below bridges this gap, and is indeed more relevant, in such marginal cases as SCADA attacks.

overall strategic significance of this instant action is therefore great. The delay between warning and effect in most uses of force offer field commanders, generals, or policymakers time to decide upon and orchestrate appropriate responses; cyberattacks offer no such luxury.

Again, the novelty here is not to be overstated, and the phenomenon of immediacy has been much examined in literature on the so-called 'revolution in military affairs.'[43] The immediate nature of a cyberattack is little more than an extreme version of (peacetime or wartime) 'network-centric warfare,' the key development of which, according to military theorists, is the acceleration of decision-making. As a strict matter of military hardware, capabilities to deliver explosive payload anywhere on the planet in under an hour are moving towards readiness.[44] To the soldier and commander, decision time on the physical battlefield is reduced by instantaneous communications and targeting orders (such as to anti-aircraft missiles). In cyberspace then, the functionally non-existent time between deployment and effect substantially limits freedom of action in contingency planning, flexibility of response, and even targeting a retributive response.

Directness. While economic measures like sanctions and political measures like broadcasting propaganda rely on secondary or tertiary effects to carry out the objectives of the action, cyberattacks bring about their effects more

[43] *See*: Clifford J. Rogers, "Revolutions in Military Affairs - a Historian's Perspective," in *Toward a Revolution in Military Affairs?*, ed. Thierry Gongora and Harald Von Riekhoff (Westport: Greenwood Publishing Group, 2000).

[44] United States Congressional Research Service, *Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues* (Washington: Congressional Printing Office, 2013).

or less directly. The extent of that directness, of course, depends on the attack's broader objectives. If the goal of an attack were to create social instability and loss of life, a cyberattack's disruption of information infrastructure — in affecting public and private, civilian and military data — is far more a primary than secondary instrument. Take, by contrast, the example of economic sanction — a generally acknowledged exempted instrument, which is unfriendly, but short of use of force. Sanctions presume that they will create financial instability in the domestic markets that will, in turn, bring about behavioral change not on the part of those directly interacting with the market, but those regulating it and representing its participants (i.e. government elites). In this case, the action does not bring about the objective, but effectuates it through a secondary contributory factor (regime impoverishment, or popular demands for change). In the case of a cyberattack, however, the attack is much more directly related to the objective.

Invasiveness. *C*yberattacks are also far closer to traditionally invasive military attacks than previous literature often implied. The confusion likely arises from the sense of irrelevance in applying national borders to actions that take place in cyberspace. To get a sense of this concept, note that the routing system for the Internet operates through a standard called 'packet-switching,' which enables messages to travel through cyberspace by passing from one server to the next, moving closer and closer to the destination using what each successive machine deems the 'next best step.' The result is that these digital signals arrive at their destination, but with little control over routing between origin and destination of information, and no regard for political or geographic frontiers. Every participating node computer on the Internet is responsible for neutrally passing data to its next waypoint; a message might travel between data centers scattered across the globe to reach an ultimate destination.

The result is that, at first glance, national borders are potentially less relevant in a cyberattack, since a digital attack might travel through dozens of countries, and ascertaining its origins presents a major challenge. Yet with regards to destination, the fact that the attack effort has penetrated and had effect within the national borders of the victim state is doubtless. In fact, the manner of invasion simply utilizes the open architecture of the Internet to masquerade as a legitimate signal — just as a hostile aircraft might disguise itself as a radar anomaly to gain access to a nation's airspace, only to deliver an incendiary payload or collide with a target. Clearly, by affecting machines or infrastructure physically based in a target country, cyberattacks meet the threshold of invasiveness.

Criticality. Exploiting dependence on particular critical elements of the state as a force multiplier also gives some military instruments an overwhelming quality distinct from sanctioning and other activity. At its most basic, critical infrastructure can be understood as systems that the incapacity or destruction of which would have a major "debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" — in other words, basic state functions.[45] Thus, attacking dams, bridges, electricity grids and similar targets have force multiplying effects, affecting entire populations in fundamental ways that distinguish them from attacks on non-

[45] *Critical Infrastructure: Control Systems and the Terrorist Threat* (Washington: Congressional Printing Office, 2003), 1.

essential infrastructure. Attacks that target critical infrastructure have always been given special consideration even in the *jus in bello* context—take, for example, the heated debate within American policy circles over *Operation Rolling Thunder*, designed to bomb key dams and bridges during the action in Korea.[46] The linkages between cyberspace and nearly every other military arena, as well as between information infrastructure and a wide range of social functions in a technology-reliant society, make the latter quite similar to (if not by definition) critical infrastructure.[47] As such, further examination of cyberattacks as an instrument must bear in mind that by targeting a resource shared among and enabling multiple sectors, the act carries one of the hallmarks of a military instrument.

Using the above criteria, the instrument-based framework for contextualizing cyberattacks is suddenly less artificially categorical and far more useful. The decade-old literature that sought — and ultimately failed — to situate cyberattacks within the "use of force" paradigm might have a means to approach that task anew. Cyberattacks appear as a practical and legal matter to be military acts of sufficient instantaneousness, directness, invasiveness, and criticality.

[46] Strategic bombing is another concept that has obvious overlap, from the standpoint of targeting critical infrastructure for secondary effect, to cyberattacks. Nonetheless, the debate surrounding it is largely an *in bello* one, excluding it from this study. *See:* W. Hays Parks, "Operation Rolling Thunder and the Law of War," *Air University Review* (1982); Robert A. Pape Jr., *Bombing to Win* (Ithaca: Cornell University Press, 1996).

[47] United States Congressional Research Service, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues* (Washington: Congressional Printing Office, 2007), 13.

Beyond Rigid Instrument Analysis: The Dual-Use Counterpoint

The preceding section has offered a number of ways that cyberattacks can be reliably (if provisionally) deemed military instruments. But upon what grounds, then, did previous scholars dismiss them as largely excluded uses of force? Is it not somewhat artificial, in the context of a cyberattack, to ignore effects entirely? Indeed, the shared nature of that infrastructure might appropriately lead one to question the durability of Article 2(4) analyses relying exclusively on the nature of an instrument.

This brief section proposes an important role for an effects-based analysis, in the case of cyberattacks, and potentially for other "use of force" analyses moving forward. It argues that in cases where the line between economic and military effects might be blurry, targets and consequences do have some confirmatory value; they can be used as a secondary test to verify the military character of the instrument. Owing to today's reliance on that shared infrastructure, (a fact not quite as salient at the time of Schmitt's analysis), this approach is particularly relevant to cyberattacks, and provides a secondary basis for recognizing the act as an illegal force under international law.

Much of what frustrated previous scholars' attempts at excising the economic and political components of cyberattacks was the lack of a meaningful distinction in the nature of the technological instrument itself. There is no fundamental difference between a computer intended for military operations and one used for civilian purposes. Computing architecture is, by its very design, inherently capable of executing any function that code dictates to its processor. It is for this reason that computers arrive 'out of the box' with little more than an operating system, but are capable of being customized with any number of applications of the user's preference. Computers utilized by governments, including ministries of defense are, in all but the rarest cases, commercial off-the-shelf products of the same type available to the general public.[48]

Dual-use technologies exist across every domain. On land, a Humvee is an example of a dual-use technology—it can haul playground construction equipment, or can just as easily have a machine gun affixed to render it a weapon. On the seas, civilian cargo ships can conceal weapons, as the history of naval interdictions during the First and Second World Wars demonstrate.[49] In the air, some warplanes might appear quite distinctive from commercial jets, but history shows how even that civilian platform can be instantly weaponized. Instrument-based analyses cannot be sidetracked by the regular, or indeed the predominant, use of a platform for economic purposes. What matters in the context of 2(4) is the character of the data being sent, the plane's use, and the ship's contents.

To this end, perhaps one of the most profound developments of the past ten years has been the endurance of the 'open' or fully interoperable network architecture, lack of robust security, and the utilization of shared information infrastructure for the vast majority of private *and public* computer networking.[50]

[48] Tubbs, Luzwick, and Sharp, "Technology and Law: The Evolution of Digital Warfare," 11. Whilst some security experts find this state of affairs outrageous, this preference is quite justifiable on three grounds. First, governments avoid having to be responsible for the development of such technology. Second, using commercial off-the-shelf products takes advantage of the private sector's short lifecycle for technology products, permitting upgrades to better (and more secure) technology on a more regular basis. Third, it provides the security advantage of a heterogeneous environment, as the use of diverse commercial products reduces the likelihood that any single vulnerability creates risk across an entire ecosystem.

[49] Lance Davis and Stanley Engerman, *Naval Blockades in Peace and War* (Cambridge: Cambridge University Press, 2006), 239-45.

[50] Jonathan Zittrain, *The Future of the Internet — and How to Stop It* (New Haven: Yale University Press, 2008), 43-52.

Much of this was unanticipated by the literature a decade ago, when a greater distinction existed between public and private, military and economic information infrastructure. Cyberattacks, which exploit or attack this infrastructure, therefore have much greater potential to on the whole do damage across many more critical sectors than was true in the late 1990s and early 2000s. As the introduction explained, the most serious large-scale cyberattacks disrupt data of all sorts, thus (by some interpretations) blurring the line of economic, political, and military instruments of coercion. So, what may have seemed a largely economic instrument to previous analysts is, today, at the very least multi-dimensional. Even if one were to reject the analysis from the previous section, cyberattacks are simply irreconcilable with rigid (and largely artificial) distinctions between coercive and non-coercive instruments. Noting that, the only serious alternative then is to sacrifice the primacy of the instrument-based distinction, and seek a standard that draws upon the effects of an attack as a non-ideal ancillary test. In this case as well though, cyberattacks meet the standard of "use of force."

If cyberattacks at their most complex combine economic, political, and military coercion, and instrument-based distinctions are not fully satisfying, the legally relevant feature of them is the military component. When (because an instrument-based evaluation is incomplete) effects are used to verify a "use of force," the mere presence of economic and political externalities cannot exempt a cyberattack from meeting the threshold. This more modern analysis of cyberattacks in their most complex form — causing mass disruption across multiple sectors — further suggests they can indeed be assessed within the "use of force" framework of Article 2(4), simply with appropriate caveats. All this does not render the preceding scholarship on cyberattacks and international law useless; rather it makes usable the broadly affirmed tools of Article 2(4) by recognizing on even restrictive grounds that cyberattacks bear a functional similarity to acknowledged “use of force” instruments.

It is therefore clear that various aspects of cyberattacks, both primarily as instrument and confirmed by their effects, render them strong candidates for recognition as a “use of force” under Article 2(4).

3.4 Cyberattacks as Violations of “Integrity,” “Independence,” or “Purposes”

On the question of legality, the final remaining issue is whether a “use of force” specifically imperils rights of “territorial integrity,” or “political independence” stated in the Charter, or is otherwise consistent with the “purposes of the United Nations.” This section argues how, given both broad and narrow interpretations of these clauses, cyberattacks clearly violate these provisions as well — and thus are, in the damaging form under analysis herein, presumptively illegal under the *jus ad bellum*.

Violations of the “Purposes of the United Nations”

As a general matter, the Charter broadly recognizes uses of force “inconsistent with the Purposes of the United Nations” to be illegal. Somewhat reflexively, it considers such threats or uses of force beyond its strict authorization to be inconsistent with its purposes. Many scholars see this provision as a functional catchall, understood to extend coverage to any use of force not otherwise authorized by the Charter.[51] This position, that "this 'other manner' language extends coverage to virtually any use of force not authorized within the Charter," is generally regarded as a mainstream position among international legal experts.[52]

Given the expansive and mainstream reading of the "Purposes" clause then, cyberattacks are under the preceding analysis self-evidently illegal. If the Charter's aims are to "maintain international peace and security," and promote "international cooperation" and the "economic and social advancement of all people," disrupting the information infrastructure of another state would seem quite directly to threaten the peace, create insecurity, run afoul of one of the better manifestations of global cooperation, and largely retard economic and social progress.[53]

Yet this self-evidence of force's illegality is not without its controversy, and for the purposes of applying the broadest swathe of the relevant international law, not necessarily sufficient as an evaluative tool for this study. Therefore, for those taking the less mainstream view that the "Purposes" provision weakens the Charter's practical application, or that new recognition of uses of force would benefit from additional support, the analysis that follows evaluates how specifically a cyberattack runs afoul of these enumerated protections.

[51] Dinstein, *War, Aggression and Self-Defence*, 86; Randelzhofer, "Article 2(4)," 106, 17-8.

[52] Schmitt, "Use of Force," 901-4.

[53] Charter of the United Nations, *Preamble*, Article 1(1), Article 1(3).

Article 2(4)'s 'Specific' Provisions

Article 2(4)'s more specific provisions, recognizing outright uses of force against the territorial integrity or political independence of a state, offer an additional and compelling case for the illegality of a cyberattack — particularly for those unconvinced by a broad interpretation of its "Purposes" clause.

These specific clauses can be read two ways, first as a narrow proscription on occupation or annexation, or as a more expansive opprobrium on interstate coercion that highlights those extreme cases. While a few scholars have favored the former interpretation, a close reading of the Article's history seems to demonstrate original intent of the latter.[54] In the Dumbarton Oaks preparatory conference draft, Article 2(4) initially left out those two illustrative clauses of territorial integrity and political independence, reading: "All members of this Organization shall refrain in their international relations from the threat or use of force in any manner inconsistent with the purposes of this Organization."[55] Only later, in San Francisco, did states insist on specific provisions on the duty to respect the territorial integrity and political independence of states—which, as a product of its historical moment, was an unremarkable emphasis.

Thus the mainstream interpretation on this clause, that it was intended not to create exceptions for so-called 'minor' or 'temporary' incursions but to emphasize particular concerns of Member States, seems quite reasonable.

[54] Ian Brownlie, *International Law and the Use of Force by States* (Oxford: Oxford University Press, 1963), 265-8, 69, 78-9.

[55] United Nations Conference on International Organization, Dumbarton Oaks Proposals, Doc 1, G1, 3. As quoted in Thomas M. Franck, *Recourse to Force: State Action against Threats and Armed Attacks* (Cambridge: Cambridge University Press, 2002), 12.

Michael Wood similarly concludes, "it is clear from the negotiating history" that the territorial integrity and political independence clauses "were inserted to strengthen the Principle, not to create a loophole."[56] Franck also emphasizes "the Charter's absolute prohibition on states' unilateral recourse to force, Article 2(4), is deliberately located in Chapter I, entitled 'Purposes and Principles.' The drafters considered these enumerated principles of transcendent importance, elucidating all other provisions of the Charter."[57] Assuming that the intention of this additional clause was to water down the provisions of the 2(4) would be "utterly incongruent…with the evident intent of the sponsors" of the amendment itself.[58]

This is not to suggest that those two clauses are simply anachronistic throwaways; they do guide recognition of the "use of force." Uses of force that jeopardize the territorial integrity or political independence of a state would serve as the most obvious cases of recognized force; those that do not may well be recognized, simply less obviously. While the following sections do not intend to assert *lex specialis derogat legi generali,* these two provisions offer an even more exhaustive study of how cyberattacks might most obviously run afoul of even a restrictive view of the law.

[56] Michael Wood, "International Law: Lecture 3," in *Hersch Lauterpacht Memorial Lectures* (Cambridge, UK: Cambridge University Press, 2006), 7.

[57] Franck, *Recourse to Force*, 11.

[58] Ibid., 12.

Cyberattacks as a Threat to Territorial Integrity

It is hard to find grounds upon which cyberattacks might threaten a state's territorial integrity in a conventional sense. The direct consequence of a cyberattack is unlikely to be the loss of a sovereign state's territory to the attacking power. Attacks on a nation's digital infrastructure may *violate* its sovereignty by affecting physical machines within its borders, but this violation is not tantamount in any literal sense to the severance or occupation of a state's land. From this vantage, then, a cyberattack may be threatening, but does not meet this criterion.

Admittedly, this study accepts the mainstream view that the Charter's proscriptions are general and adaptable, despite critiques by scholars like Reisman. The latter's argument, that the Charter cannot be read or interpreted separately from the historical context of its authorship, nor from the basic and outdated assumptions that it makes about state practice, are insufficiently vindicated by states' enduring recognition of — if not always have fidelity towards — the U.N. regime.[59] Nonetheless, in the specific context of cyberattacks, Reisman's argument is compelling in one respect: by acknowledging that cyberattacks would pose a future dilemma for the international peace and security regime *if it lacks the ability to recognize them*, cyberattacks may indeed challenge the utility of the 'contiguous land' and 'borders-in' view of protected sovereignty.

[59] Michael Reisman, "Coercion and Self-Determination: Construing Charter Article 2(4)," *American Journal of International Law*, no. 78 (1984): 642.

This next section will explore two ways in which, through an expanded view of the notion of "territorial integrity," a cyberattack might satisfy the conditions of Article 2(4).

Threat to Integrity. Expanding the notion of "territorial integrity" offers a novel view of how cyberattacks might be recognized under Article 2(4). To be sure, "territorial integrity" was in original construction a straightforward proposal, a sign of the psychological wounds of Czechoslovakia and indeed all of German-occupied Europe. The state practice intentionally circumscribed by the U.N. Charter was the forceful annexation of the territory of sovereign states, or the forceful breakup of a weak state to its more powerful neighbors. But is that all "territorial integrity" can connote?

If one takes the view that the Charter's provisions are not strictly bound by the context of its authorship, one might look today to the deeper meaning of what territorial integrity signifies. "Integrity" means, quite literally, the condition of being unified. Clearly, this cannot imply contiguity; after all, the present-day United States is a non-contiguous union of territories some of which lie over 5,000 miles from one another, as were the remnants of the British Empire in 1945. The meaning, then, must imply that the integrity of a state is a political or social condition; in full meaning, states are prohibited from functionally dislodging territories from their capitals, or the other constituent parts of their state. This reading is fully consistent with even a strict, historicist reading of Article 2(4).

An attack of sufficient gravity on information infrastructure might well have the effect of threatening the unification, by upending the means of connection between territories and the rest of their nation. To see how, it is worth recalling the physical realities that undergird cyberspace and as such, the means of ‘cutting off’ a territory from contact is not terribly difficult to envision.

Two very different vectors exist if one seeks to attack information infrastructure to ‘cut off’ a territory — both of which could be combined for a particularly severe disruption to a territory’s connections to the outside world.[60] Cyberspace may be a non-physical concept, but the actual fiber optic cables, microwave dishes, routers and hubs that serve it are indeed physical, and often reside within national borders. The effects of a major cyberattack against a far-flung territory, if well coordinated and planned, could be the near-complete severance of a territory’s military, economic, and private-sector communication to the rest of the state.[61] One can think specifically about the effect that severing one major fiber-optic cable, and disrupting a handful of satellite downlinks, might have on a remote territory such as the U.S. state of Hawaii. The practical reality of such an attack may, in this view, amount to a direct threat to the unity of that territory with the rest of its nation, particularly if an ethnic or political group promoted factionalism within the affected area. In this respect, then — with no ability to communicate, govern directly, or transact commerce — one might indeed see a cyberattack as a threat to the territorial integrity of the overall victim state.

[60] A third possibility, the deployment of an electro-magnetic pulse, could potentially disrupt every electrical component on a continent-sized area by detonating a nuclear device just above the upper atmosphere. While technically a kind of cyberattack, it is so far at the margins of this discussion, and so massive in its consequence, that there is little question its use would classify as prohibited force in the international context.

[61] Because of an increasing convergence of such data traveling over shared information infrastructure, the cascading effects of such an attack are immense, and exponentially proportionate to the level of technology dependence in that territory.

Cyberspace as 'sovereign territory.' A cyberattack might threaten territorial integrity in a more diffuse sense as well, if one accepts the view that a nation's networks constitute its sovereign 'territory.' This brief subsection examines the competing views on that issue, arguing that both the view holding sovereignty impossible, and the view holding it fully applicable to 'cyberspace,' are neither fully correct. Rather, it makes the case for a conception of cyberspace sovereignty that focuses on the physical assets that enable it — while accepting that the technology poses unique challenges to a bordered conception of the state.

Cyberspace is made of physical infrastructure, but that infrastructure routes data without regard to geography. This architecture is both physical and conceptual; militarily useful but largely commercial; and inextricable from its global linkage. For all these reasons, cyberattacks pose a conceptual challenge to the relevance of state borders in judging acts of hostility. Internationally, three principal perspectives exist on the relation of cyberspace to sovereign borders. Each of these three perspectives can yield dramatically different outcomes as to whether or not forceful violations of that space might be prohibited by international law.

Cyberspace as post-Westphalian. Historically, the first dominant (and somewhat utopian) view of global networks was articulated by the Internet's first engineers and user-evangelists through the 1980s and 1990s. In that view, articulated most famously in activist John Parry Barlow's *Declaration of the Independence of Cyberspace*, global networks represented a self-governing and inviolable commons not subject to the jurisdiction or regulation of sovereign "national" states.[62] Put simply by Barlow, states "have no sovereignty," and "legal concepts of property, expression, identity, movement, and context do not apply."[63] Equally popular during this period was the more causal view, that the information revolution would render sovereignty irrelevant, and economic success largely a function of connectivity.[64] This utopian view is, for the purposes of this study, largely a *post-national* vision of the relationship between cyberspace and sovereign territory. In its original version, it accords to 'netizens' a post-Westphalian identity bounded only by technology. Needless to say, this is not the future that came to pass. Online identities have not supplanted national identities, and nationalism has even become a powerful force for conflict and disruption.[65]

This post-national vision suffers from its radical incompatibility with today's international environment, which remains largely dominant. The view seizes too much upon the challenges of applying law and policy to a conceptual space, and ignores the physical, territorial realities of the technology. More a product of futurism and ideology, the simple fact that state regulations *can* be placed on human behavior online, in accordance with the state claiming citizen jurisdiction over that individual or corporation seems to disprove its core assertions. The fact remains that while *cyberspace* cannot be regulated, the

[62] John Perry Barlow, "A Cyberspace Independence Declaration," *Electronic Frontier Foundation*, February 8, 1996, http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration (accessed January 12, 2010).

[63] Ibid.

[64] See, for example, Walter Wriston, *The Twilight of Sovereignty: How the Information Revolution Is Transforming Our World* (New York: Scribner Books, 1992). Wriston argued that even manufactured products (so-called 'hard' goods) would have increasing information content, decoupling geography and production and reducing the relevance of national borders.

[65] See, for instance: Xu Wu, *Chinese Cyber Nationalism* (New York: Lexington Books, 2007).

behaviors of the humans and firms that interact thereupon, and to some extent the states conducting their affairs there as well, are subject to enticement and dissuasion in the form of law or custom. It is little wonder then that attempts to recognize this kind of post-national vision of cyberspace, and of its critical resources, were also roundly defeated at the United Nations both at the World Summit on the Information Society, and in subsequent General Assembly debate.[66]

Cyberspace as national territory. By contrast, at various times over the last decade Russia, Cuba, and China have claimed the applicability of sovereign boundaries to cyberspace — listing "trans-border" flows of "destabilizing information" as tantamount to a physical incursion.[67] This view of sovereign and bordered cyberspace, distinctly in the minority but nonetheless asserted publicly, was also expressed strongly in a 2009 Shanghai Cooperation Organisation *Agreement on Information Security*, binding Russia, China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan to definitions that consider 'the information space' national territory.[68] This view might be called the '*territorial extension*,' view of cyberspace: that it can somehow be meaningfully

[66] World Summit on the Information Society (WSIS), *Tunis Agenda for the Information Society*, (Geneva: United Nations Press, 2005). See especially para 30. See also: U.N. A/RES/65/141.

[67] See: *Op. cit.*, 78 note 12.

[68] Shanghai Cooperation Organisation, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security*.

nationalized, and is therefore subject to the same claims of non-interference as physical territory.[69]

This territorial extension view offers little in the way of evidence for how, precisely, the nationalization of conceptual cyber-space might be realized, except for declarations against non-interference in the "political, moral or spiritual systems of other states."[70] This theory does not ground its analysis in the material reality of cyberspace — that its switches and fiber exist in real space. Moreover, despite extensive literature asserting sovereign rights to the space, these views fail to account for the transnational *reality* of much of what transpires online. Data can traverse dozens of countries en route to its destination, irrespective of origin or destination. Individual 'packets' are not tagged by national origin, nor sorted in accordance with their contents' suitability to the host country's social mores. The technology that undergirds cyberspace is functionally neutral in this regard, and thus claims of sovereignty (and the calls for strict or intermediary liability for states or Internet service providers via whom data is emanating or transmitted) have little beyond political desire that reinforces them. The absence of legal or customary justification for this view render such a view rhetorically useful, but unsatisfying.

From a practical standpoint, state attempts to assert the same kinds of claims over cyberspace that customarily apply to physical territory are equally

[69] There is a clear incongruence with the Russian Federation's view in this context; it would seem to suggest applicability of international legal principles, simply extended to cyberspace. This stands in contrast to the earlier-cited statements about the insufficiency of international law in dealing with the potential for 'information weapons.'

[70] Komov, *Diplomacy of Peace*, 594.

unconvincing. After all, most Internet users sign up for social networking sites, or purchase online goods, without much attention to that website's place of incorporation or legal regime. To that extent, it may be true that average users interact with states online only in the case of interference — for whatever reason — of their access or conduct. The infrastructure itself does not distinguish between nationalities. While the previous examination found grounds upon which the *act* of a cyberattack might *result* in a threat to territorial integrity so construed, few conclusions can be drawn *ex ante* as to the applicability of the same rights to cyberspace.

Cyberspace as global; infrastructure as sovereign property. A final, more moderate view neither accepts nor rejects the notion of cyberspace as a place where sovereignty might be asserted, but focuses those claims (and legal jurisdiction) where they can be most readily exercised: over individuals and physical infrastructure residing within the borders of a state. Legal scholar Jack Goldsmith brought this view to prominence in 1998, and in his subsequent volume with Tim Wu asserted that the digital networks on which individuals rely are built upon physical machines and human transactions — and applying law and regulation to this realm is not *ex ante* impossible.[71] While this argument is most often applied to the applicability of legal regimes and regulatory measures, it has important defenders in the context of international security. As cited previously, in 2009, U.S. President Obama asserted that his country's "*digital infrastructure*

[71] Jack Goldsmith, "Against Cyberanarchy," *University of Chicago Law Review* 65 (1998); Jack Goldsmith and Tim Wu, *Who Control the Internet?: Illusions of a Borderless World* (Oxford: Oxford University Press, 2006). For more on the increasingly bordered reality of the Internet, see: Michael Geist, "Cyberlaw 2.0," *Boston College Law Review* 44 (2003).

— the networks and computers we depend on every day — will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority."[72] Notable is not just its elevation of this technology to the level of a strategic asset (one that quite plainly "will be defended"), but its emphasis on the *infrastructure*. To borrow a phrase from securitization theory, the 'referent object' of security is the physical infrastructure that enables networks to form and transactions to take place, not 'cyberspace' per se.[73]

States may obviously claim reasonable sovereignty over the physical information *infrastructure* that resides on their shores, and the commercial activity that their citizens and corporations conduct online. But even if a state's 'networks and computers' are considered 'strategic national assets,' does that render the data upon them tantamount to digital territory? A state defends the operation of storefronts on a Main Street—with police and, if necessary to repel foreign invasion, the military. So are the online storefronts — the websites — of Amazon.com or Baidu.com assured freedom from disruption by virtue of being an extension of a state's territory?

Here we find the limitations of relying on the present, majority view of what constitutes a state's most critical assets in the context of interstate coercion. States' comments on the disruption accompanying cyberattacks have not yet been placed in terms of a violation of its territorial integrity. It seems, however, that

[72] Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure" The White House, Washington, DC, May 29, 2009. Emphasis added.

[73] For more on securitization theory, from which this terminology draws, see: Barry Buzan, Ole Waever, and Jaap de Wilde, eds., *Security: A New Framework for Analysis* (London: Lynne Rienner Publishers, 1998), 23-5.

grounds may exist and that such a practice is possible, as states do engage in a process asserting sovereign jurisdiction over the infrastructure that cyberattacks disrupt. Thus, when the target of a disruption might include information infrastructure that serves the whole of society, while U.N. Charter and other use-of-force provisions might apply, the fit is often imperfect — and entails interpretive leaps from solid legal consensus. Territorial integrity is hardly the only object of focus of Article 2(4). In fact, most scholars agree that its reference is illustrative and emphatic, not restrictive. We now turn then to the second clause of Article 2(4), which is a somewhat more straightforward basis for cyberattacks' illegality.

Cyberattacks as a Threat to Political Independence

Moving then beyond the question of territorial integrity, there are indeed grounds upon which a cyberattack might threaten a state's "political independence." To reiterate, the advantage of finding justification within the political independence clause is in its comparative straightforwardness. Relative to the clause about to be examined regarding the "Purposes of the United Nations," this concept has been rather less contentious in the academic debate over justifiable uses of force. Perhaps more so even than "territorial integrity," the premise of political independence too may be regarded along a spectrum from strict interpretation, focusing on the absence of occupation of a foreign force in a nation, to a broader version that would encompass both the legal authority of a state and the ability of that structure to perform the functions of government and provide basic services.[74]

The latter, more expansive definition comports with the customarily understood meaning of "political independence," grounded in the U.N. Charter and further custom and international law reaffirming the independence of governments to act by their own accord — or to use more common terminology, affirming the 'non-intervention' of foreign powers in domestic governance.[75] Just as the ICJ ruled in *Nicaragua* that the Charter, strictly interpreted, "by no means covers the whole area of the regulation of the use of force in international relations," so too has the customary interpretation of "political independence" expanded somewhat since 1945.[76] Even then, its meaning was less clearly fixed to particular historical context as "territorial integrity" might have been.

While armed occupation is obviously at the core of this provision's concerns, it represents the violation of political independence at its most extreme. Elsewhere, of course, the Charter makes consistent reference to 'sovereign equality' — Article 2(1) — and holds as a core tenet a defense of the doctrine of non-interference. Some scholars, like Randelzhofer, argue that any non-military coercion is covered not by Article 2(4) but by the general principle of non-

[74] Also engaging with this premise of "political independence" is the extensive commentary on humanitarian intervention, self-determination, and other significant debates challenging the scope and content of existing prohibitions on force. While these debates center on some of the same issues, it is impossible to do them justice in this context, and drawing extended connections between them and this study would likely leave both too speculative at the present moment.

[75] See: Antonio Cassese, *International Law*, 2nd ed. (Oxford: Oxford University Press, 2005), 53-6; Brownlie, *International Law and the Use of Force by States*, 312; Oppenheim, *International Law, a Treatise*, 2, 406.

[76] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua V. United States of America), Merits, Judgment*, 14 at Para. 176.

interference.[77] While the simplicity of this view is attractive, subsequent interpretation does not support that clear a distinction. At least, Article 2(4)'s guarantees of "political independence" and the principle of non-interference are consistent and, in the expansive view, inter-woven.

Focusing not on the legal condition then (which cyberattacks do not realistically threaten outright), but the restraint on decision-making and maintenance of order, there are two important and related ways in which cyberattacks can threaten political independence. The first and more obvious way a cyberattack might threaten political independence would be the breakdown of civic order, particularly by exploiting the feedback of dependencies between information infrastructure and the constituent elements of high-tech societies. In short, by jeopardizing a government's ability to maintain law, order, and communication with its citizenry renders it unable to perform the basic functions of a politically independent state. Secondly, there are a number of ways in which modern, developed societies' political independence has become reliant on the functioning of various global commons, including global trade flows and international information infrastructure (which largely regulates logistics of the former). In this respect, the interruption of shared resources might bring about a similarly damaging effect on civic order and restrict political decision-making even if the event itself is outside a nation's borders.

Political independence is also directly related to military preparedness. Any action that appears to be (or is actually) seriously disadvantaging a state in an impending military conflict could be judged as threatening its political

[77] Randelzhofer, "Article 2(4)," 113.

independence. As noted earlier, it is difficult as a practical matter to separate civilian and military information infrastructure; as such, a disruption of the former might could well disrupt military command-and-control, and by extension to a state's political independence of a more basic form.

It is important to note that only a major cyberattack, targeting a highly technologically dependent nation, appears an obvious candidate for outright recognition under this clause. By analogy, physically destroying electricity grids across a broad region would cause not simply the loss of power, but economic losses, compounding civic unrest and stressing law enforcement, which would itself be crippled by the loss of telecommunications that facilitate first responders. Major cyberattacks replicate this feedback across many more critical sectors. Therefore this conclusion, coupled with the very real grounds upon which cyberattacks might be considered generally as uses of force, suggest compelling additional grounds that they would be recognized as illegal under Article 2(4).

Conclusion: Presumptively Illegal, Potentially Actionable

This chapter has identified several grounds upon which cyberattacks can be recognized as generally and specifically prohibited by Article 2(4) of the U.N. Charter. Broadly, it developed grounds on which the law would recognize cyberattacks as uses of force, sharing both meaningful qualities and significant effects with those activities we recognize in the kinetic space as 'force.' This analysis goes beyond the methodological challenges that frustrated analysis by Schmitt and others a decade ago, as the method and impact of what are understood today as 'cyberattacks' are far clearer to those conducting legal analysis. To complete that assessment, I also demonstrated how those uses of force so-recognized fell within a range of criteria set forth by Article 2(4): as inconsistent with the UN's purposes, as threats to political independence, and with an expansive reading, even territorial integrity in some limited cases. In all these circumstances then, and regardless of the breadth of one's reading of Article 2(4), cyberattacks with the consequences discussed herein appear prohibited as matter of international law.

The most conclusive analysis possible, within the spirit and letter of the *jus ad bellum*, simply acknowledges that such attacks are *presumptively* illegal, and that this position may well be used by a state articulating the policy decision to respond on the basis of that illegality. Estonian Ministry of Defence and NATO legal expert Eneken Tikk, when asked what *precise conditions* would constitute a "use of force," summarized that "even the NATO defence board examining the issue [of cyberattacks] agreed…we should not worry about threshold. That is a policy question. The real question is what happens next."[78]

As we have seen, Article 2(4) serves as a kind of last resort in the international community — a blanket and aspirational prohibition on force that can be construed both narrowly and broadly. But law alone is not what restrains state behavior. This is a crucial distinction between a treaty and its operation, between law and regime. To have durable effect on state behavior, the U.N. *regime* hinges in practice upon its remedial mechanisms, and the framework of lawful self-defense that accompanies them.

The balance of this chapter evaluates how this illegality might serve as the foundation for justifying a response, in self-defense. Illegality under Article 2(4) is a necessary precondition to the activation of rights of self-defense under the

[78] Tikk, *Frameworks for International Cyber Security: Legal and Policy Instruments.*

Charter's remedial framework. It is necessary but insufficient. Different standards and customs, themselves subject to interpretation, permit action by a victim state in response to such an act. Determining how the U.N. Charter framework not just condemns, but might conclusively *limit* the use of cyberattacks by justifying a response in self-defense, is the question to which this study now turns.

3.5 Applying the Remedial *Jus ad Bellum*

Presumptive illegality, however important for the long-term contours of international politics, is no guarantee of restraint. The authors of the U.N. Charter recognized this reality, as well as the radical departure from state practice the Charter would constitute if it denied parties all recourse to immediate self-defense. The remedial regime that emerged to enforce Article 2(4) — leveraging the Security Council and a specific right of self-defense — was designed to back up idealism with pragmatism. Its operation is essential to the relevance of the modern *jus ad bellum,* especially its prospects for restraining state recourse to cyberattacks.

The balance of this chapter is devoted to the question of whether cyberattacks invoke these lawful rights of self-defense under the U.N. Charter. If so, the combination of presumptive illegality and lawful repellent force would provide a powerful disincentive for a would-be attacker. If instead a would-be attacker might suffer little beyond legal reproach — and knew the victim had no lawful recourse to force — cyberattacks may be even more attractive than other means of coercion. The three sections that follow aim to determine which the *jus ad bellum* supports.

The argument of the next three sections is as follows:

This section (3.5) frames the options available to states under the remedial *jus ad bellum* (under Articles 39 and 51), recognizing at the onset critical views as to the regime's overall efficacy. It argues that the self-defense provisions are more controversial but more analytically satisfying for these purposes. It then frames the key debates on that issue, specifically the scope of the 'inherent right to self defense,' and argues for an approach examining whether and how cyberattacks qualify as an 'armed attack.'

The next section (3.6) examines whether cyberattacks constitute an armed attack so-defined. It begins by noting that there is no universal definition to evaluate an 'armed attack,' and that most uses of force occupy a grey area requiring further elucidation. The section then argues four key criteria to make such a determination: gravity, military effect, attribution, and prevention (all in regular use by scholars and in the case law), and concludes it reasonable that a cyberattack would satisfy each.

The final section (3.7) concludes this chapter by connecting the legal status of cyberattacks with the status of self-defensive rights against them, and proposes the overall effect of the *jus ad bellum* on their use.

***Introduction to the Remedial* Jus ad Bellum**

Under the U.N. Charter's Chapter VII, states falling victim to an illegal use of force — including, as we have seen, a cyberattack — are potentially entitled to two remedies. They may petition the Security Council under Article 39 for third-party authorization of force or other corrective action. They may also, and without third-party authorization, employ forceful self-defense under Article 51. The former is uncontroversial but also unsatisfying; the latter, far from automatic, is potentially more powerful but also places this discussion at the center of several longstanding debates in international law that this section intends to address.

It is worth noting at the onset that the successful operation of this regime is a matter of longstanding controversy — and this chapter does not seek to sidestep that reality. The sheer number of armed conflicts after 1945 might lead one to question whether the Charter's provisions exercise any meaningful restraint. However it is indisputable that "never in history has there been such widespread and well-founded recognition of the costs and horrors of war."[79] Scholars such as Schachter have repeatedly and effectively rebutted the notion of the *jus ad bellum*'s bankruptcy by outlining states' understanding of costs associated with non-compliance, and with clear evidence of states adapting to their perceptions of the regulations it imposes.[80] Moreover, states' repeated reference to the regime in justifying their actions and recriminating adversaries, is more than just the "ritual incantation of a magic formula;" as Gray and others argue, it reflects a need to counter awareness with third-party legitimacy for forceful action.[81] It is itself notable that states feel a need to advance any legal argument to defend such security decisions.[82] Scholars rightly point out that while there persist disagreements — particularly in the scope of self-defense, and

[79] Oscar Schachter, "The Right of States to Use Armed Force," *Michigan Law Review* 82, no. 5/6 (1984): 1620.

[80] "In Defense of International Rules on the Use of Force," *University of Chicago Law Review* 53 (1986): 114.

[81] Gray, *International Law and the Use of Force*, 119.

[82] Schachter, "In Defense," 123.

issues tangential to this study like humanitarian intervention and interference in civil conflict — the core substantive law is largely coherent and not “so vague and fragmentary as to allow…unlimited latitude to use force.”[83] I do not presuppose here that activation of the remedial regime necessarily means the *ad bellum* regime will function to restrain cyberattacks. Instead, this chapter is designed to test if the regime can even operate, with its existing strengths and shortcomings, on this new technology. Recognition under the remedial regime is essential to presumptive illegality being more than the weakest of restraints, inviting a cynical “ritual incantation” after obvious violation.

Article 39 and the U.N. Security Council

Chapter V of the U.N. Charter grants the Security Council “primary, but not exclusive responsibility for the maintenance of peace and security,” a role reaffirmed by the ICJ in its consideration of how U.N. expenses are disbursed.[84] Specifically for these purposes, Chapter VII, Article 39 directs the Security Council to “determine the existence of any threat to the peace, breach of the peace, or act of aggression, and […] make recommendations, or decide what measures shall be taken…to maintain or restore international peace and security.”[85] The result is a particularly broad remit to render judgment on the legality of cyberattacks — broader, in fact, than the criteria of Article 2(4) just discussed. The Security Council could take on this issue, which would more than

[83] "Right of States," 1645.

[84] Vaughn Lowe et al., eds., *The United Nations Security Council and War* (Oxford: Oxford University Press, 2010), 5.

[85] U.N. Charter, Article 39.

qualify within one of Section 39 criteria. With primary responsibility for the maintenance of peace and security, and clear prospects for these capabilities to affect them adversely, one would presume that eventually the Security Council will render judgment on such an act. As of this writing though, no state has successfully brought (or even seriously proposed bringing) cyberattack activity before the Security Council.

Lacking any precedent, the present ability to examine the interface between the Security Council and cyberattacks is limited to the point of nonexistence. It would also be methodologically perilous, given the approach of this study. Analysis under the letter of the law, or drawing analogy to well-known weapons of war is generally possible, with principal risks of over- and under-inclusion. Drawing analogy between prior Security Council decisions to propose future choices would be to draw analogies that are on all sides context-dependent. Security Council choices, though grounded in the same Charter law, are fundamentally political ones — or at least fundamentally informed by political reality.[86] It is not a judicial body. Moreover, applying prior precedent to potential, future action would require holding the practice of the Security Council static (which it is not), as well as the behaviors of its membership (which are anything but static).[87]

[86] Schachter, "In Defense," 122.

[87] The institution's dynamism when faced with new security issues is well captured in several chapters of Lowe, Roberts, Welsh, and Zaum's edited volume on the Security Council, including those by Cortright, et al. Greenstock, Welsh, and Boulden. See: Lowe et al., *The United Nations Security Council and War*, Chapters 8, 10, 24, and 27.

Instead, examining then the 'automatic' activation of the Charter's remedial provisions — which is to say those permitting a state to exercise its rights to self-defense enshrined in Article 51 — is likely to bear more fruit.[88]

Article 51 and the "Inherent Right to Self-Defense"

"Nothing in the present Charter shall impair the inherent right of individual or collective self-defense…" — so begins Chapter VII, Article 51, which many scholars regard as the cornerstone of the U.N. Charter's remedial landscape for states confronted with an illegal use of force.[89] The content of the article — that states retain a right to individual and collective self-defense even in the presence of the Charter's ban on force — is generally intuitive. Its scope, by contrast, is a subject of considerable debate. How far this right extends, and in response to what actions, is one of the most important debates in international law, and international security more generally. After noting the connection between this and Article 39, this section frames the basic contours of the debate between 'restrictive' and 'expansive' interpretations of Article 51, and suggests a framework for analysis of cyberattacks therewithin.

Though the rest of this chapter will examine the debates and applicability of Article 51, it should be noted that the operation of Articles 51 and 39 are inextricably linked, and conclusions about one may ultimately inform the other. The Charter-guaranteed right of self-defense is, as originally designed, only a

[88] The Charter endows the U.N. as an institution with other functions that may well be relevant to cyberattacks, such as Articles 33-8 on pacific settlement of disputes, and Article 26 on arms control plans. Though outside the scope of this study, they could form a fruitful basis for further inquiry. For a comprehensive overview, see: *ibid.*, 2-10.

[89] U.N. Charter, Article 51.

temporary and stopgap measure "until the Security Council has taken measures necessary to maintain international peace and security."[90] Perhaps with good reason, this clause is often overlooked, since many have declared this aspect of the U.N. collective security system stillborn, at least as originally designed. For this reason, and out of the desire to avoid speculation or prognostication, this chapter might be said to focus on what action would be deemed justified *prior* to potential intervention by the Security Council, or perhaps more plausibly, in the absence of any pronouncement. The sections that follow may inform, but do not focus on Security Council action, other than to the extent that the conditions outlined in each are those that the Council would almost certainly consider in rendering judgment on a remedial use of force — which is, itself, quite rare.

The Contested Scope of Article 51

The debate over the scope of Article 51 is fundamental to this study because it informs whether there is a meaningful distinction between the illegality just outlined, and a state's ability to lawfully respond to such an act. While the intuitive suggestion — and approach favored by this study — does recognize a heightened standard for the deployment of force, it is worth outlining the divided scholarship on the issue and reasons for making this choice.

This longstanding academic debate hinges on divergent views of the origins and meaning of 'inherent right.'[91] The more expansive of the two

[90] U.N. Charter, Article 51.

[91] See: E. Jiménez de Aréchaga, "International Law in the Past Third of a Century," *Recueil des Cours de l'Academie de Droit International (RCADI)* 59, no. 1 (1978): 94-6; Brownlie, *International Law and the Use of Force by States*, 270-5; Dinstein, *War, Aggression and Self-Defence*, 175-82; Gray, *International Law and the Use of Force*, 117-21. For the distinction

viewpoints regards the Charter as distilling an existing and broad customary right of self-defense. Supporters of this view regard the legal 'right' asserted in the Charter as a codification of a fundamental state right to survival, which has its origins in the 'primitive' legal concept of self-help.[92] They also root this notion in domestic legal systems, where self-defense is generally sanctified, in creating exceptions deeply relevant in 1945 — when unrestrained right of warfare was dwindling but not yet obsolete.[93] Proponents of this view therefore either consider the notion of "armed attack" functionally identical to other explanations of illegal activity (e.g. "aggression" or "use of force") appearing elsewhere in the Charter, and/or affirm that the Charter has no intention of restricting the scope of a right whose content rests independent of the document.[94] This view has a handful of outspoken adherents in the legal academic community.[95] While the

between 'right' and 'inherent right' — important but not germane to the argument of this section — see Dinstein, *War, Aggression and Self-Defence*, 178-9.

[92] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, ICJ Reports 226, 226, 63 (1996). See also: "International Law as a Primitive Legal System," *NYU Journal of International Law and Policy* 19, no. 1 (1986-1987): 12. For origins of this argument, see Hans Kelsen, *General Theory of International Law and State* (Cambridge, MA: Harvard University Press, 1945), 339.

[93] On the waning of this 'right' in the historical context, see: Georg Schwarzenberger, "The Fundamental Principles of International Law," *Recueil des Cours de l'Academie de Droit International (RCADI)* 87 (1955). For a novel and compelling expansion of that argument in the modern context, see: Mueller, *Retreat from Doomsday*.

[94] Aréchaga, "International Law in the Past Third of a Century," 95.

[95] For example: D.W. Bowett, *Self-Defence in International Law* (New York: Praeger, 1958), 184-5; Stephen Schwebel, "Aggression, Intervention and Self-Defense in Modern International Law," in *Justice in International Law: Selected Writings of Judge Stephen M. Schwebel*, ed. Stephen Schwebel (1994); Julius Stone, *Aggression and World Order: A Critique of United Nations Theories of Aggression* (Clark, NJ: The Lawbook Exchange, Ltd., 1958), 44; Schachter, "Right of States," 1634.

ICJ has taken great strides not to weigh in on this matter,[96] some Dissenting Opinions have lent this debate some credence arguing the issue on fundamentally pragmatic grounds (most famously, Judge Schwebel's dissenting opinion in the *Nicaragua* case).[97]

By contrast, experts like Dinstein and Gray regard the expansive reading "counter-textual, counter-factual, and counter-logical," and at best, "at variance with the mass of state practice and has to discount the views of the vast majority of states."[98] Rather than focusing on whether or not the Charter enshrined an existing 'natural' right, the argument for a restrictive reading of Article 51 centers on the phraseology at the time of authorship and the broader Charter context. Specifically, it notes the special status that the U.N. Charter's authors clearly intended for the construction of "armed attack" used in Article 51, *vice* other constructions like "use of force" or "aggression." It is impossible to discount the precise insertion of the "armed attack" concept, the absence of which is notable in Articles 2(4), 39, and elsewhere throughout the Charter. By inference then, the concept of an "armed attack" is a specific form of the use of force and aggression which, "because of its seriousness, creates a *periculum in morta*" entailing the

[96] Christine D. Gray, "The Charter Limitations on the Use of Force: Theory and Practice," in *The United Nations Security Council and War*, ed. Vaughn Lowe, Adam Roberts, Jennifer Welsh and Dominik Zaum (Oxford: Oxford University Press, 2010), esp. 95 note 31.

[97] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion*, ICJ Reports 136, 373 (2004). Schwebel does not however contend that the ICJ (or U.N. organs broadly) lack competence or authority to adjudicate or define matters invoking rights of self-defense — only that the origin of the right lies beyond the restrictive view that ascribing intentionality to the phrase "armed attack" necessitates. See: Stephen Schwebel, "Aggression, Intervention and Self-Defense in Modern International Law," in *Justice in International Law: Selected Writings of Judge Stephen M. Schwebel*, ed. Stephen Schwebel (1994).

[98] Dinstein, *War, Aggression and Self-Defence*, 183; Gray, *International Law and the Use of Force*, 118.

right to use force in legitimate defense, rather than waiting for measures of protection by the United Nations."[99] The result is that Article 51 considerably restricted the scope of permitted self-defense from the "vague customary right [of] self-preservation," yet left it intact to preserve the maintenance of the *jus ad bellum* regime.[100] This view comports largely with U.N. practice;[101] with evidence of their origins in the text,[102] and the range of subsequent legal analysis that makes clear Article 51 carefully enumerates limited exceptions to the blanket prohibition on the use of force, and does not introduce a distinct reference extra-textual natural law.[103] Aréchaga further notes that while "the political and moral justification for [a distinct "armed attack"] requirement in the Charter is so obvious in the world of today that it would seem unnecessary to have to justify it from a legal point of view."[104] Scholars and states favoring a more restrictive reading are more numerous and, it seems, generally more convincing.[105] The

[99] Aréchaga, "International Law in the Past Third of a Century," 95. See also: Dinstein, *War, Aggression and Self-Defence*, 184-6.

[100] Brownlie, *International Law and the Use of Force by States*, 274. See also: Norman M. Feder, "Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack," *NYU Journal of International Law and Policy* 19 (1986-7): 405.

[101] E.g. cases outlined in: Rosalyn Higgins, *The Development of International Law through the Political Organs of the United Nations* (Oxford: Oxford University Press, 1963), 200-1.

[102] Archéaga notes that the alternative viewpoint is neither "convincing nor in accordance with the canons of treaty interpretation agreed at the Vienna Conference on the Law of Treaties." Aréchaga, "International Law in the Past Third of a Century," 96.

[103] Randelzhofer, "Article 2(4)," 603. Randelzhofer refers to this as the "dominant view," and is further supported by Kelsen, Oppenheim, Skubiszewski, Lamberti, and Zanardi. For support of this view within U.N. practice, see: Higgins, *The Development of International Law through the Political Organs of the United Nations*, 200-1.

[104] Aréchaga, "International Law in the Past Third of a Century," 95-6.

[105] See: Higgins, *The Development of International Law through the Political Organs of the United Nations*, esp. 167-230.

International Law Commission, in its comprehensive survey and analysis, also favors such a restrictive view.[106]

In line with those scholars, I regard this 'majority view' (of the scholarship and of states) favoring a restrictive interpretation of Article 51 as generally more compelling as well as in line with the preceding interpretation of Article 2(4). It also provides a more useful and discrete framework in which to understand whether cyberattacks might invoke self-defensive rights, focusing not on the origins of the right and its inherence, but the content of the "armed attack" term of art. This is the kind of 'connotative reading' of the Charter that Feder calls for, and one that I concur provides a more useful analytical framework to explore Article 51's scope and relevance to a cyberattack.[107]

3.6 Rights of Self-Defense Following a Cyberattack

This section considers what special criteria beyond presumptive illegality that a cyberattack would need to meet in order to reach the "armed attack" criteria. Separate but relatedly, this section also examines the circumstances that are necessary for forceful self-defense to be permissible under international law.

Defining "Armed Attack"

There is no meaningful dispute as to whether an armed attack permits self-defensive action. Novel technologies, however, push the boundaries of what

[106] International Law Commission, *Report of the International Law Commission to the General Assembly* (1980).

[107] Feder, "Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack," esp.410-12.

constitutes such an event. The emblematic case of "armed attack" envisaged by the Charter's authors is clear-cut: one nation's army marching on another's territory, using military instruments (an army) in an illegal use of force that could threaten a state's very existence with political overthrow and territorial occupation. The history of state and non-state use of force since 1945 complicates this straightforward approach. As Franck noted as early as 1970, though, modern warfare "has inconveniently by-passed these Queensberry-like practices."[108] Cyberattacks are another case study in a canon of legal analysis fraught with ambiguity.

There is also little question that the customary interpretation of an "armed attack" has evolved, both through state practice and case-specific interpretation by the ICJ, yet no monolithic definition of the concept has emerged to date. This is historically curious. Even in the context of the Charter's initial development, advances in air power had threatened traditional concepts of military movement and targeting, and nuclear weapons were challenging conventional notions of military deterrence. Yet the *travaux préparatoires* makes clear that delegates in San Francisco never seriously entertained defining the term.[109] Since then, states have in many cases been loathe both to apply formal definition, and in some cases, even to invoke Article 51 when doing so might stretch its application.[110]

[108] Thomas M. Franck, "Who Killed Article 2(4)? Or Changing Norms Governing the Use of Force by States," *American Journal of International Law* 64 (1970): 812.

[109] Randelzhofer, "Article 51," 668; Schwebel, "Aggression," 532.

[110] Most notably, the United States' insistence that its 'quarantine' of Cuba during the 1952 missile crisis was empowered by regional treaty arrangement, not the Charter. For broader legal implications, see: Feder, 422-4; Schachter, 134-5. For emblematic legal commentary on the event itself, see: Myres S. McDougal, "The Soviet-Cuban Quarantine and Self-Defense," *American Journal of International Law* 57 (1963); William T. Mallison, "Limited Naval Blockade or

The ICJ has expressed even more permanent reticence at providing general criteria for an "armed attack," preferring instead to issue judgment on the category of activity.

Substantial scholarship is devoted to examining the legality of certain acts that tested the boundaries of states' rights of self-defense. Key examples include the legality of logistical support paramilitary groups (*Nicaragua*), of cross-border incursions (*Congo*)*,* and of armed response to attacks on non-military targets (*Oil Platforms*).[111] Like the ICJ, neither has the Security Council produced a singular definition, though it did provide regular judgment on responses to an accumulation of events (such as its resolutions on the Israeli security wall).[112] Some additional areas of study, such as protection of nationals abroad, retrocession of colonial enclave, and humanitarian intervention abroad, seem plainly irrelevant to this specific case. However those broad concepts may be important justification for a response in self-defense to a cyberattack. All these cases point to the idea that singular grounds for defining a cyberattack as an "armed attack" will be elusive, but that more circumstance-specific scholarship can help provide meaningful analogies to understanding states' rights in this new case.

Quarantine-Interdiction: National and Colelctive Defense Claims Valid under International Law," *George Washington Law Review* 31 (1962). This is not to say states have been fully unwilling to expand *any* definition; consider for instance the U.S. 1986 bombing of sites in Libya and Tripoli for counter-terrorism purposes, citing Article 51.

[111] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua V. United States of America), Merits, Judgment. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo V. Uganda), Judgment*, ICJ Reports 168(2005). *Oil Platforms (Islamic Republic of Iran V. United States of America), Judgment*, ICJ Reports 161(2003).

[112] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion*, 14, at 101–04, paras 01–95.

Therefore, one must reformulate the question slightly to address the issue. The relevant question cannot be whether a cyberattack meets a certain definition of an ‘armed attack,’ but rather what are the key justifications a state would levy to support a forceful response to a cyberattack under Article 51 and its subsequent interpretation?

To answer that question, I argue for four criteria, drawing together and expanding some of the case law and precedent of other state actions pushing the boundaries of Article 51. A state would have strong grounds for justifying self-defense to a cyberattack if the attack: (1) was discrete and of sufficient gravity, (2) had military effect, (3) was strongly attributable, and (4) could be ceased/largely prevented with the defensive action.

Gravity

Much of the issue of gravity has been dealt with in the study’s overall definition of a cyberattack, and in the prior discussion of cyberattacks satisfying the “use of force” criteria under Article 2(4) — as they surely do. However assessing an event’s gravity is inevitably case-specific. Further general refinement of the notion of gravity specific to the context of self-defense remains elusive, but two specific issues can help clarify the potential acceptability of self-defense. The first would be identifying (and excluding) *de minimis* incursions. The second, a central topic within scholarship on the issue, concerns whether an ‘accumulation of events’ might trigger Article 51, as proposed by some states in the context of their adversaries’ cyber activities.

Illegal but *de minimis* events. The ICJ has been consistent in making clear that illegal use of force that is nonetheless *de minimis* in its effect would not invoke a right of self-defense. The hallmark case on this point (and many others) was *Nicaragua*, the judgment of which drew an oft-cited distinction between an "armed attack" and "a mere frontier incident."[113] This distinction was highly controversial within the scholarship, namely for either narrowing too far the concept of self-defense, or eroding the utility of the *jus ad bellum* regime in the face of an uptick in low-intensity conflict.[114] Nonetheless, there is an intuitive if not universally recognized distinction between full-scale invasion and an errant bullet over a border, a small-scale skirmish, or a destructive act only inconveniencing commerce in a contested area. For this reason, the U.N. General Assembly's 1974 *Definition of Aggression* — itself of controversial legal status — did nonetheless include a 'de minimis' clause excluding cases where "the events concerned or their consequences are not of sufficient gravity."[115] Those events would at the very least impose severe proportionality requirements on the response, perhaps to the point of precluding it outright.[116] There is no need to adopt one position or the other here, since a response even if authorized would be so miniscule to be of little international consequence.

[113] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua V. United States of America), Merits, Judgment*, para 195.

[114] See: Dinstein, *War, Aggression and Self-Defence*, 195; John Lawrence Hargrove, "The *Nicaragua* Judgment and the Future of the Law of Force and Self-Defense," *American Journal of International Law* 81, no. 1 (1987): 139; Michael Reisman, "Allocating Competences to Use Coercion in the Post Cold-War World, Practices Conditions, and Prospects," in *Law and Force in the New International Order*, ed. Lori F. Damrosch and David J. Scheffer (Boulder, CO: Westview Press, 1991), 40.

[115] United Nations General Assembly, *Definition of Aggression (A/RES/3314 [XXIX])* (1974), Article 2.

[116] Brownlie, for instance, concludes the former and accepts no categorical limitation on the activation of the right, only on the scale of recourse. Brownlie, *International Law and the Use of Force by States*, 366.

With that in mind, a cyberattack event that might fall into this *de minimis* category would have several special characteristics. They include a victim's immediate or rapid recovery and reconstitution; the uninterrupted functioning of targeted infrastructure; or the attacker's failure to compromise critical national systems, broadly defined. One can envision an attempted cyberattack on recognizable military assets, or an attempted nationwide Estonia-style attack, but with little to no effect due to rapid remediation. In those circumstances, a state might have grounds, judging from the attack's targets and tactics, to claim an armed attack, but the international scrutiny applied to a forceful reaction would be significant on the basis of minimal gravity. This is not simply a matter of existing law and external perception: states seeking a regulative regime against cyberattacks would also do well to keep the threshold high, lest cyberattack become a means of frequent and destabilizing military escalation.

Accumulation of events. A related and equally relevant issue is whether or not an accumulation of events, rather than a discrete and more severe single event, could invoke lawful self-defense. American officials, for instance, have at various times claimed that the Comprehensive National Cybersecurity Initiative constituted a declaration of intent to 'fight back' against cyberattacks from abroad based on an accumulation of events.[117]

The status of law on this question is mixed. Schachter argues for a time-limitation on events that are considered 'discrete' for the purposes of response,

[117] John Markoff, David Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *The New York Times*, 25 January 2010.

but wisely does not propose a specific timeframe.[118] That is likely the soundest, if least specific approach. Feder adds that the United Nations Security Council generally rejected the premise of a ‘pin prick’ theory of armed attack.[119] Gray, however, argues it has “not gone so far,” and instead the ICJ’s judgment in *Nicaragua* seems to leave open the possibility for lawful response to an accumulation of events.[120] In other cases such as *Cameroon/Nigeria, Oil Platforms,* and *Congo*, as Gray notes, the Court has left this potential open without precluding the notion.[121] There seems no definitive conclusion as to whether an accumulation of events could as a general matter of law invoke rights of self-defense, only that the notion is not categorically unjustifiable.

It is simple to envisage a cyberattack whose effects were slow and continuous, for instance if a virus were programmed to spread quickly but act slowly. Such insidious sabotage, if cascading to a point of substantial damage, would make for a fascinating test case in the case law, and force more concrete opinion on the matter. It is premature to consider its position within international law, though one might speculate that this is a far riper case to assert the premise than the 1982 Israel-Lebanon case. Accepting the controversy on the status of law, all that is possible at this phase is to accept that a discrete cyberattack event

[118] Schachter, "In Defense," 132.

[119] Feder, "Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack." Feder focuses here on the 1982 Israeli incursion into Lebanon in response to the Palestinian Liberation Organization’s frontier attacks on Israeli towns, and Lebanon’s inability to restrain those attacks.

[120] Gray, *International Law and the Use of Force*, 155-6. Gray cites para. 231 as key evidence.

[121] *Ibid.*, 156.

would less controversially invoke rights of self-defensive force than an accumulation of cyberattack events.

Military Effect

To merit force in self-defense, a cyberattack would likely have to have demonstrable impact on military preparedness or deployment. Earlier sections have touched on the notion a cyberattack that spectacularly derails a military's ability to equip, deploy, and exercise command-and-control is an obviously hostile act — and more likely than actions against other government targets to meet the "armed attack" threshold. Such seemed to be one of the ancillary conclusions of the ICJ in *Oil Platforms.* In that case, the United States claimed rights to shell oil platforms in self-defense following an attack on a U.S.-flagged vessel, compounded by a mine strike by one of its warships. In its judgment against the United States, the Court drew an important distinction between the legal effect of a single attack on a merchant vessel and a similar event targeting a more identifiably military vessel.[122]

Consider, as well, the treatment of the issue in the *Definition of Aggression.* Accepting that the *Definition* constitutes at least one source of customary international law, it is worth noting that document clearly lowers this threshold from 'significant effects' when military targets are concerned, specifically citing as aggression an incursion "by the armed force of a State on the land, sea or air forces, or marine and air fleets of another State."[123] This 'Article

[122] See *ibid.*, 145 and note 32.

[123] Res. 3314, Article 3(d).

3(d)' definition does so in two important ways. First, it suggests that attacks on military assets need not be geographically limited to the borders of the victim state. Second, it reflects that attacks on military assets, more starkly than other cross-border hostilities, must be interpreted as aggressive acts of exceptional illegality. Both stand to reason; in the modern age of military power projection, large militaries hold assets permanently stationed globally — and are subject to attack while outside their home state's borders.[124] Likewise, the definition reflects the juridical reality that attacks against military serve an ostensible purpose of skewing a present or future armed conflict. As such, targeting clearly military assets is one of the more obvious characterizations of an armed attack.

Applying this notion to cyberattacks does run some risk of over-inclusion, providing states seeking a broad remit to use force as an opportunity to justify that action on the margins of the law. To remain in keeping with a restrictive view of Article 51, and insulate the rationale from customary abuse, the parameters of what defines a 'military asset' in the digital age require greater clarity. Some simplified cyberattack cases fall easily within this clause in the *Definition*. For instance, using digital means to weaken command-and-control of ballistic missile arsenal, particularly a nuclear arsenal, falls well within this definition, as they fall under the exclusive purview of militaries. The same would be true of using a cyberattack to disable the navigational and other systems of a large and mobile naval fleet, or military aircraft whether in flight or grounded. In cases of obviously military (flagged, sole-purpose) equipment, cyberattacks on them are

[124] For instance, as of December 31, 2011, the United States military claims presence in 150 countries, with almost 200,000 active-duty personnel deployed abroad.

almost certain to fall under the Article 3(d) definition, and the ICJ's approach in *Oil Platforms*.

Decoupling military infrastructure from the borders a victim state is helpful, but particularly susceptible to abuse. For instance *prima facie*, a cyberattack on a maritime navigational beacon (or satellite) essential to a fleet's deployment into a theatre of imminent conflict would seem to meet this definition of aggression. This characterization would hold if that beacon were within a state's territorial waters, but equally if it were positioned well beyond the victim's borders. Moreover if a state incited, commissioned, or orchestrated the attack, it would under this analysis bear hallmark responsibility for an armed attack.

Yet not all digital infrastructure that is 'important' to a military seems consistent with the spirit of Article 3(d). A cyberattack against servers used by the Royal Navy might appear as an attack against the UK's marine fleet, but not if those servers were simply used to process payroll across the Ministry of Defence. Those with a preference to see their rights of self-defense invoked might argue, for instance, that the infrastructure is ultimately part of the 'overarching apparatus' of a military, and that without pay, soldiers might sew unrest, and thus the event was an armed attack against military preparedness. Even before questions of proportionality, the fact remains that while the assets may be military in ownership, the attack does not constitute an aggressive action *against* military capabilities in any direct way. Therefore it is important to clarify that a cyberattack must have the effect of damaging a military's ability to equip, deploy, and exercise command-and-control — not simply to organize and train — to meet this threshold.

Conversely, similar skepticism might be applied to the aforementioned case of that navigational beacon, or more accurately, the networked infrastructure that serves it. A cyberattack rendering that infrastructure inoperable is certainly of military concern. That infrastructure, however, might not be military on its surface at all. It is exceptionally likely that beacon, like the vast majority of modern militaries' unclassified logistics systems, leverage shared information infrastructure. Knowing which infrastructure — for instance, a Maltese Internet service provider providing that beacon's connectivity among thousands of its other contracts — could permit an attack to precisely target that military asset. In this case, the 'attack' would indeed be against an armed force. It could impact its ability to deploy. Is self-defense therefore lawful?

It hardly seems that one logically follows from the other, and thus, that the event meets the threshold of an "armed attack." Here, the argument that any event targeting marginally 'military' information infrastructure is an "armed attack," especially in the likely case that infrastructure were shared by the military and civilians, seems particularly reminiscent of the United States' unsuccessful arguments in *Oil Platforms.*[125] Crucially, the Court held that the attacks on U.S.-owned (*vice* flagged) vessels, "even taken cumulatively…do not seem to the Court to constitute an armed attack on the United States of the kind that the Court [in *Nicaragua*] qualified as a 'most grave' form of the use of force."[126] Surely, the U.S. naval vessel's collision with a mine was by no means minor, but as the next section will explore, the ICJ was (controversially) unable to find aggression

[125] ICJ Pleadings, US *Rejoinder*, Section 5.

[126] ICJ Reports, (2003), para. 62.

directed at the state exercising self-defense. The relevant conclusion for analogy is that not all attacks on state-claimed property with military relevance constitute attacks on its military. A cyberattack disrupting a military is likely to cross the "armed attack" threshold, but in doing so it must have strategic effects greater than a number of technical inconveniences.

Attribution

Without confidence (and public evidence) of the identity of an aggressor, it is difficult for a state to lawfully react with force in self-defense. The alternative, 'lashing out blindly,' might serve some sort of deterrent value, but has little justification in international law.[127] Much has been made, and much previously cited, about some of the challenges of attribution to a particular technical attack. Given the novelty of the issue (even support for armed cross-border incursions was discovered to make cases eligible for ICJ judgment), there is far less scholarship on the specific question of *attribution*.[128]

This section will briefly frame that challenge, and argue for a distinction between *technical* and *geopolitical* attribution. While technical challenges for attributing a particular attacker are manifest, satisfactory (though imperfect) geopolitical attribution within the context of the international security

[127] Marin C. Libicki, "The Nature of Strategic Instability in Cyberspace," *Brown Journal of World Affairs* 18 (2011): 75.

[128] This concept is distinct from state responsibility, where the perpetrators are known, but the extent of their connection to the state is uncertain.

environment may be more realistic than portrayed in some of the earliest accounts of the threat.[129]

For context, the technical complexities of attribution represent a nontrivial barrier as it is conceived in, for instance, cross-border law enforcement. Because of the technical reality of cyberattacks, the exact identities of the attacker might, in a very real sense, not even be knowable to a victim state with any certainty or in any immediate timeframe. Determining whom, precisely, is responsible for a cyberattack at the moment of attack is exceedingly difficult, though not unprecedented in the context of irregular combatants previously encountered in military conflicts. The problem is multi-dimensional. In the case of a cyberattack, a state must first determine the physical machines involved in the attack—usually identified by their Internet Protocol, or IP Address. The process of narrowing down the list of potential attackers, from every machine connected to the public Internet, to those involved, and finally the one or few controlling the attack, is hardly straightforward.

A second layer of complexity comes in determining the ownership and jurisdiction of those machines: the diffuse authority over Internet infrastructure means that signals appearing to originate from one location may have no relation thereto.[130] In fact, a routine tactic of such attacks is to obscure the location and ownership of a machine by bouncing signals through multiple countries in an

[129] Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives, *Untangling Attribution: Moving to Accountability in Cyberspace (Testimony of Robert Knake)*, 2010.

[130] See: Libicki, *Cyberdeterrence and Cyberwar*, 41-52; David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks*, ed. Herbert Lin (Washington: National Academies Press, 2010), 25-40; Andress and Winterfeld, *Cyber Warfare*, 202-4, 49-50.

attempt to foil any tracing attempts. Finally, beyond locating the hardware and assigning ownership of it, there exists the final intelligence challenge of determining the actual user, or users, operating the machine. Assigning attribution for a cyberattack is therefore the quintessential all-source intelligence challenge, requiring simultaneous collection and analysis of signals intelligence, specialized digital forensics, and human intelligence sources.

Attribution might be technically possible in some cases of digital attacks against information infrastructure, but reconstructing the information necessary to do so with confidence can often take days or even weeks with present-day technology — and is often reliant on cooperation of foreign states to provide access to server logs.[131] There is no reason to believe that the attribution problem will be solved soon, or that identity-concealing technologies will not continue to outpace digital forensics. As such, cyberattacks, particularly in their purely digital form, have an inherently covert element that complicates attempts to apply traditional rules of military response.

From an analytical and international legal standpoint the attribution problem is complicating, but not sufficient to derail a disciplined analysis of the topic altogether — nor the application of the regulative regime on force. Attribution for a cyberattack is not purely a technical matter, any more than attribution for a missile launch is strictly a function of altitude and exhaust trail. This overreliance on technical circumstances is one of the key shortcomings of

[131] This challenge was the central motivation behind the Council of Europe's *Budapest Convention on Cybercrime*, the only binding, cyber-specific document of positive international law to date. That Convention, currently with over thirty parties, aims to reduce the barriers to voluntary cross-bordering information sharing of perishable data related to internationally recognized cybercrimes.

much of the literature on the topic to date, particular in the context of strategic deterrence.[132] Technical circumstances are, after all, only one aspect of the case states might build against an attacker in responding with force.

The technological specifics of a cyberattack may be unique, but the underlying challenges parallel others dealt with by modern militaries. A few parallels elucidate the matter. In the early days of long-range ballistic missiles and until advanced satellite and radar coverage was achieved over a range of launch sites, locating the origin of such a missile was a strategic uncertainty and profound liability.[133] Moreover, the increasing practice of basing missiles beyond national borders in crude measures of allied deterrence complicated the matter further. In this case, technical developments helped narrow attribution questions to, at the very least, a rough geography. But it is important to recall that a missile's trajectory hardly proves the identity of who gave orders to launch it. It was not inconceivable during the Cold War that the misfiring of an automatic trigger, or a military commander acting without orders but under internal rules of engagement, might launch (or test) absent a notification. Likewise, such a launch could quite realistically have been met with a denial, or pleas for time to investigate, from political leaders. In a more modern example, in 2007 the Chinese People's Liberation Army (PLA) conducted a test of an anti-satellite (ASAT) weapon. The test was met with great surprise and alarm in the West, but perhaps equal surprise within China's own civilian government, which met accusations of joining a 'space arms race' first with confusion, then telling

[132] Libicki, *Cyberdeterrence and Cyberwar*, 41-52.

[133] Bundy, *Danger and Survival*, 325-6.

silence, before days later issuing a statement defending the test.[134] Despite perceptions of this highly escalatory move, most evidence suggests the PLA's unilateral decision to move forward with such a move, in spite of its political consequences and without the full knowledge of civilian political leadership. All this bears a striking resemblance to the human-interface challenge of cyberattack attribution — that even with a breakthrough to identify the 'launch site' of sorts, that perfect attribution to identify the individual and orders under which he was acting are imperfect.

Likewise, apparent complicity for a significant use of force might relax the need for direct — which is to say personally attributed and/or a defined command relationship — attribution. Consider, for instance, the Security Council's and General Assembly's notable unity condemning the terrorist attacks of September 11, 2001, and the Security Council's implicit approval of a state's right to self-defense in response.[135] Leaving aside the considerable debate over the evolving self-defense custom in the U.S.-led operations in Iraq in 2003, it is notable that in the 2002 invasion of Afghanistan, the 'attribution' was not entirely straightforward under the very strict standard that international law customarily demands. In that case, the Security Council found it acceptable to draw the line between the individual claiming responsibility for the act, and a government known to be supporting his activities. At no point, however, was evidence of a

[134] Brendan Nicholson, "World Fury at Satellite Destruction," *The Age*, 20 January 2007; BBC News, "Concern over China's Missile Test," 19 January 2007; "China Confirms Satellite Downed," 23 January 2007.

[135] U.N. Security Council Res. 1368 (2001); U.N. Security Council Res.1373 (2001); U.N. General Assembly Res. 56/1 (2001).

command relationship established between the Taliban regime in Afghanistan, and Al-Qaida or Osama Bin Laden.[136] Nonetheless, in this particular case, historical state support was used as a proxy for state complicity, leading ultimately to the measures imposed by the Security Council, and taken by NATO, against the Taliban. With something less than a smoking gun, "international support for Operation Enduring Freedom [was] almost universal."[137]

The argument here is not that attribution is irrelevant, only that it is far more context-dependent than many commentators on cybersecurity give credit. In some cases, a use of force is directly attributable to an armed force directly controlled by a state. In other cases, however, that relationship is less clear, as modern weaponry, tactics, and methods of covert support force 'certitude' over the aggressor to mere 'deductive culpability.' In such cases — which today represent a significant number of potential armed attacks — technical evidence is rarely the determinant of perceived legality. The regulative regime clearly considers geopolitical context, in other words the rational likelihood and perceived incentives of an attack, with at least as much gravity as the protestations of the involved parties. Otherwise, the Taliban would have to be taken at its word that it had no incentive to participate in Al-Qaida's activities (or repeat what many American commentators regard as its obvious mistake accepting

[136] See, for instance, the phraseology of UNSCR 1378, "Condemning the Taliban for allowing Afghanistan to be used as a base for the export of terrorism by the Al-Qaida network and other terrorist groups and for providing safe haven to Osama Bin Laden, Al-Qaida and others associated with them," but not tying direct reference to the events of September, 11, 2001.

[137] Lindsay Moir, *Reappraising the Resort to Force: International Law, Jus Ad Bellum, and the War on Terror* (Portland, Oregon: Hart Publishing, 2010), 115.

Nicaragua's reasoning for attacks on its neighbors, denying them right to collective self-defense).[138]

Returning to the specifics of cyberattacks, some commentators have noted that activating the remedial *jus ad bellum* would require either the alignment of implausible circumstances, or 'lashing out blindly' at an attacker only remotely presumed.[139] The situation is not so dire. Cybersecurity decision-making no longer takes place in a vacuum of technical operations distinct from national security policy. Rather, the United States, United Kingdom, Russia, Australia, and others have integrated their senior-most cybersecurity policymaker into the apparatus of national security decision-making.[140] The practical result is that cybersecurity incidents are placed within the broader context of political and diplomatic conditions, sensitive intelligence insights, and military conditions on which states invest exponentially more. With this context in mind then, while the potential perennially exists for an unannounced, unanticipated attack from a previously unknown actor, those states most likely to invoke a right of self-defense are well aware of the threat profile of likely adversaries, and would

[138] For such arguments, see *American Journal of International Law,* 81 (1987), especially: Franck, 'Some Observations on the ICJ's Procedural and Substantive Innovations'; D'Amato, 'Trashing Customary International Law; Hargrove, 'the Nicaragua Judgment and the Future of the Law of Force and Self-defense'; Moore, 'The *Nicaragua* case and the Deterioration of World Order'.

[139] Michele Markoff, "National and Global Strategies for Managing Cyberspace and Security" (paper presented at the Conference of the Atlantic Cuncil: International Engagement On Cyber: Establishing Norms And Improved Security, Washington, 30 March 2011).

[140] As this writing those roles are, respectively: the Special Assistant to the President and Cybersecurity Coordinator, National Security Council Staff (United States); Director of the Cabinet Office of Cybersecurity and Information Assurance (United Kingdom); Deputy Secretary of the National Security Council (Russia); and the Deputy National Security Advisor (Australia).

therefore monitor cyberattack capabilities and preparations just like any other national security threat.[141]

Within the broader context of national security decision-making, and indeed the international security environment, cyberattacks do not simply materialize from an unknowable ether without motive or direction. They have and will continue in most instances to reflect already simmering geopolitical conflicts, rendering the kind of geopolitical attribution necessary to supplement (but not justify) a self-defensive attack possible, even absent a digital smoking gun.

Preventability, Pre-emption and Anticipatory Self-Defense

The final criteria relate to the proposed response, rather than the nature of the attack itself. To be lawful, a self-defensive response to a cyberattack must be aimed at prevention of an imminent attack inexorably proceeding — and not aimed at punishment or pre-emption. This notion of imminence, combined with a quality of inexorability described in greater depth below, is what would define the somewhat more palatable notion of prevention from the extremely polarizing and legally unsettled issue of pre-emption.

It is conceivable that a victim could prevent an impending cyberattack with an in-kind or distinct use of force, and that in so doing would be within a controversial but justifiable right of self-defense. Given the speed at which digital signals travel, some commentators mistakenly regard preventive action as impossible, and overlook this fruitful line of inquiry on lawful self-defense. To

[141] See: Cassell Bryan-Low, "British Spy Chief Breaks Agency's History of Silence," *The Wall Street Journal*, 29 October 2010.

do so would be, again, to fall victim to a purely technical view of cyberattacks, removing them from the geopolitical context and the very human planning, preparation, and decision-making they require.

Seeking consistency with international custom that the following paragraphs will explore in turn, to be lawful, the impending attack would need to be *known to the victim*, *imminent and externally verifiable,* and *inexorably proceeding* (in progress absent intervention). Moreover, the forceful preventive act must be the only *plausible successful measure within the timeline of attack*.

Known and verifiable. As a preliminary matter, a state contemplating self-defense must face what Grotius deemed "danger…present and real, not an imaginary danger."[142] In more modern terms, it is important for the maintenance of the *jus ad bellum* regime that evidence of an imminent attack be preserved and externally verifiable as a backstop to subsequent scrutiny, and evidence include proof of its imminence. Here it is important to be precise with the notion of imminence, clarifying between the more generous notion used by proponents of pre-emption (discussed below), and perhaps the more conservative definition used here, which includes an element of inexorability. In this definition, the victim would need to demonstrate, *ex post facto* and to the extent technically plausible, that the attack had reached the 'point of full preparation' or 'point of no return.'

Inexorable. To be lawful, self-defensive force must have a reasonable prospect of repelling attack; a state may lawfully deploy self-defense only if that attack is *inexorable,* unceasing on its own, thus necessitating force. A movement

[142] Hugo Grotius, *On the Law of War and Peace*, ed. Stephen C. Neff (Cambridge: Cambridge University Press, 2012 (first published 1625)), Book 2, Ch. 1.

of troops across a frontier remains the clearest definition of the concept, but defining that threshold in other contexts has been a subject of international law for almost two centuries. To this day the most enduring citation on the topic remains the commentary of nineteenth century U.S. Secretary of State Webster on the 1837 *Caroline* incident, which concerned pre-emptive attack by British forces in Canada on an American ship assumed to be part of anti-British insurrection. In discussing culpability for the ship's destruction, Webster concluded self-defensive force could be legitimate if taken in response to a "necessity" that was "instant, overwhelming, leaving no choice of means and no moment for deliberation."[143] Some scholars regard this passage the '*locus classicus'* of the law of self-defense,[144] though others contest its legal operation in light of the U.N. Charter,[145] most converge on the idea that Webster's comments set out at the very least the "basic elements" of the law in its present form.[146] Following *Caroline*, consensus remains strong around the notion that repellent force requires an attack in-progress.

As technology has evolved, the definition of 'in-progress' has also evolved. Precedents exist for making such a distinction in more modern and relevant areas of interstate hostilities, particularly modern aerial combat. While the absence of standing rules of engagement (SROE) for cyberattacks makes

[143] Hunter Miller, ed. *Treaties and Other International Acts of the United States of America*, vol. 4 (Documents 80-121: 1836-1846) (Washington: Government Printing Office, 1934).

[144] R.Y. Jennings, "The *Caroline* and McLeod Cases," *American Journal of International Law* 32, no. 1 (1938): 92.

[145] Gray, *International Law and the Use of Force*, 105-6.

[146] In addition to building arguments off the Jennings quotation above, Dinstein seems to validate this narrative drawing connection between its subsequent uses at the International Military Tribunal at *Nuremberg.* Dinstein, *War, Aggression and Self-Defence*, 249.

interpretation of this matter more challenging. To analogize from other fields of conflict, modern air combat brought similar questions to the fore with the existence of radar-guided missiles.[147] Other than in no-fly zones (for which no parallel presently exists in cyberspace), launching combat-ready sorties or patrols in a state's sovereign airspace would not constitute inexorability. If that squadron broke regular patrol and headed towards another state's airspace, that latter state would still not have the right to respond with force, since the act the supposed victim would be preventing is by no means inexorable, imminent, or verifiable. Aerial SROE are interpreted by most air forces, however, such that a warplane can freely engage (using force) once a radar lock for missile launch has been confirmed. Critics might argue that this is a particularly late point, with too high a risk, to delay action. Nonetheless the SROE intentionally reflect precisely that level of restraint, lest earlier actions escalate a conflict unduly, or pin fault for aggression on the victim.

Analogizing then to present cyberattack scenarios, the goal is to define a similar point of imminence and inexorability, where 'hostile intent' is on display, but still leaving whatever time necessary for a preventive action. If a defender became aware of a pre-configured attack ready for execution, it would be acceptable to prepare the means of defense and potentially repel cyber-attacks, but not to act upon the latter until the hostile power's order to execute the attack itself commenced. Reconnaissance of capabilities, and the majority of operational preparation of the environment (resembling traditional espionage in tools and tactics), would not suffice. Installing malicious software on critical machines

[147] Brownlie, *International Law and the Use of Force by States*, 209-316.

could be tantamount to a radar lock only if the software is understood to be destructive in nature, rather than just gathering information or preserving access for later infection. Since ‘targeting’ in the case of cyberattacks is a notably reversible phenomenon, and the decision to attack revocable both categorically and in increments, the law supports utmost caution.

Plausible Success. Finally, adding to these stringent conditions, a preventive action would, in all but the most obvious cases of a cyberattack meeting the “armed attack” threshold, need to be the only *plausible* means of success. The victim state, having suffered an armed attack that meets most of the aforementioned conditions — especially gravity — is scarcely under a requirement to exhaust additional options of diplomacy before acting in self-defense. However in some cases, where the question of whether an “armed attack” took place was a matter of dispute, subsequent judgments have rejected a right of self-defense on the grounds that the victim did not exhaust those options.[148]

Plausibility here does not presume that a state must dither with diplomatic engagement known by both sides to be fruitless, only to forestall an attack. However, if the victim state knows it possesses diplomatic, economic, or other leverage capable of dissuading the attacker from taking such action *and has time to deploy it*, custom would suggest a broad expectation they would constitute all but last resort. There are, then, certainly scenarios where a technical act bordering on use of force might successfully prevent an attack — for instance, severing the physical or logical connection of an attackers’ command-and-control machine for

[148] *Ibid.*, 259.

a digital attack or forcing an outage in systems used by a state's military and civilians by disrupting the Internet service provider. In all such instances, though, the legality of the preventive attack would depend first on the criteria aforementioned — particularly that of *gravity*. As with all acts in self-defense, they would need to meet expectations of *proportionality* and *distinction* (the implications of which the next chapter will explore).

Pre-emption and Anticipatory Self-Defense. Fundamental to the issue is the fierce legal debate over whether a customary right to preventive self-defense, let alone pre-emptive self-defense exists.[149] Simplifying for the purposes of this analysis, it is important first to distinguish between *preventive* and *pre-emptive* actions. *Preventive*, as used herein, describes action that would prevent an imminent attack either in progress or inexorably proceeding, and known to the victim state. By contrast, *pre-emptive* is therefore the more legally fraught term that would include Israel's bombing of presumed nuclear sites in Iraq in 1981 and Syria in 2007, as well as the United States' principal justification for invasion of Iraq in 2003. Perhaps the most interesting and controversial recent treatment of prevention is the Secretary-General's 2005 report *In Larger Freedom,* which claimed, "lawyers have long accepted that [Article 51] covers an imminent attack as well as one that has already happened."[150]

[149] For an excellent summation, see: Gray, *International Law and the Use of Force*, 160-65. See also: Dinstein, *War, Aggression and Self-Defence*, 297-9; Franck, *Recourse to Force*, 97-105; Moir, *Reappraising the Resort to Force*, 12-21; Anthony Clark Arend and Robert J. Beck, *International Law and the Use of Force* (New York: Routledge, 1993), 71-79.

[150] Kofi Annan, *In Larger Freedom: Towards Development, Security, and Human Rights for All* (New York: United Nations, 2005), para 124.

This more legally sound notion has been reinforced in the last decade in contrast to the Bush Doctrine and concepts of *pre-emption* upon which the United States justified its invasion of Iraq in 2003.[151] The scholarship remains deeply polarized on this issue, though with almost a decade's hindsight, does appear to favor exclusion of as full a doctrine of pre-emption as might have validated that conflict. The period following 9/11 is described by some commentators as the "high-water mark" of a state's self-defense rhetoric, and that the legal justifications for it (less convincing) were indicative of a shifting tide against such a broad claim.[152] As Christine Gray also points out in her later works, there was equally no attempt to ground these expansive rights of pre-emption in the existing *jus ad bellum*, namely the U.N. framework.[153] While as the previous section argued, it is conceivable that a preventive action could stop a cyberattack before deployment, precursor activities traditionally associated with pre-emption — such as the accumulation of proscribed capabilities — are far more difficult to distinguish and far more difficult to lawfully pre-empt.

In order to dispense with it, consider the contours of an argument in favor of a doctrine of robust cyberattack pre-emption — in other words, a justification for forceful removal of capabilities in the hands of a would-be aggressor before deployment on the victim's networks. The legal rationale for doing so would,

[151] Christine Gray notes that the key contribution of the Bush Doctrine was asserting a right of self-defense to pre-emptive military action, and helpfully traces a number of pre-2001 pre-emptive actions that did not rely on such a justification. Gray, *International Law and the Use of Force*, 160-5.

[152] Jutta Brunnée and Stephen J. Toope, "The Use of Force: International Law after Iraq," *International and Comparative Law Quarterly* 53, no. 4 (2004): 794.

[153] Christine D. Gray, "The Bush Doctrine Revisited: The 2006 National Security Strategy of the USA," *Chinese Journal of International Law* 5, no. 3 (2006): 563.

without question, have to be grounded in established law and, likely, existing normative proscriptions of the sort described in the next chapter. This was precisely the rationale leveled by the United States against the Hussein regime for accumulation of Weapons of Mass Destruction (WMDs), the mere possession of which created what the U.S. administration deemed an imminent threat to its national security.[154] Two problems exist in applying this rationale to cyberattacks. The first is that there is no legal agreement or sustained effort to date to place cyberattacks within the unique normative and legal category presented by WMD (the next chapter will, however, consider such an argument). Second, and perhaps more immediately as a practical matter, cyberattack 'capabilities' are far less easily identified and monitored than the instruments used to produce WMD. Computer viruses do not require rare minerals or precision equipment to produce. Their production equipment is dual-use and ubiquitous, and changes in operations cannot be observed by satellite imagery. Even the exacting planning, reconnaissance, and operational preparation required to execute a significant cyberattack use the same tools and techniques as cyber-espionage. With such a thin line between sub-force and armed attack activity, it would be difficult to articulate a pre-emptive doctrine that does not take action against threats uncertain to materialize. For these reasons, in the context of cyberattacks as well, "pre-emptive self-defense remains highly problematic."[155]

[154] George W. Bush, *Remarks by the President on Iraq (Cincinnati, Ohio)* (Washington: U.S. Government Printing Office, 2002).

[155] Gray, *International Law and the Use of Force*, 221.

Intent for Specific Harm

Finally, while legally unsettled as a requirement for judgment against the perpetrator, it seems essential that for it to launch a lawful response, the victim be able to articulate a coherent narrative of intent (*mens rea* in the criminal context) for specific harm by the aggressor. This notion is particularly important in the case of cyberattacks for the same reason that the ICJ (controversially) noted a need to ascertain the "circumstances and motivations" of an attack — to distinguish it from a frontier incident.[156] The United States and Russia have consistently referred in public statements to the need to reduce misperception that could lead to escalation in cyberspace. In June 2013, the two parties concluded years-long negotiations to establish a series of crisis communications and de-escalation protocols — using systems initially put in place for nuclear de-escalation — for cybersecurity issues.[157] Those moves highlight the possibility that states' gross negligence could result in the appearance of a smaller-scale cyberattack emanating from its borders. Such activity might provide pretext for conflict between a particularly unstable dyad, even if the event was entirely outside either government's control.

Comparison to present law. States guilty of gross negligence, or generalized force towards unspecific adversaries, are far less likely to find themselves on the receiving end of lawfully permissible defensive force than those intending specific harm. Cases at the intersection of force and indiscretion

[156] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua V. United States of America), Merits, Judgment*, para 231.

[157] The White House, "U.S.-Russian Cooperation on Information and Communications Technology Security," news release, 17 June, 2013.

abound, but perhaps the most helpful is the already-described *Iranian Oil Platforms* case. Justices in that case held that Iran's undersea mines, despite detonation on a U.S. warship, were insufficiently 'targeted' against U.S. interests as to classify as an "armed attack."[158] Specifically, the Court noted that Iran was simultaneously at war with the United States and Iraq. Moreover, it noted the nature of mining was not directed at any one single target or category of target (i.e. military vessels) but rather as a general deterrent to navigation. As such, the Court determined insufficient grounds to accept the United States' claims of rights of self-defense. This stance predictably ignited a strong rejoinder from the United States, scrutiny from the academic community, and left unclear how generalized aggression was *not* granted substantial and unjustifiable under the ICJ's standard.[159] Before engaging with that controversy, however, the Court did produce the straightforward conclusion that an "armed attack" legitimating armed response must possess clear and specific intentionality to harm the responding state.

Judging cyberattack intent. As a technical matter, cyberattacks bear some resemblance to instruments as diverse as conventional weapons, land and naval mines, and biological weapons in the challenges they pose to ascertaining the attackers' intent. In successful cyberattacks, the initial targeting would be a delicate matter, requiring reconnaissance and intelligence gathering, often outside

[158] *Oil Platforms (Islamic Republic of Iran V. United States of America), Judgment*, para 151-61.

[159] This latter criticism was the crux of the rebuttal offered by the State Department Legal Adviser subsequent to the decision. See: William H. Taft IV, "Self-Defense and the *Oil Platforms* Decision," *Yale Journal of International Law* 29 (2004): 294. Gray, however, finds this argument unconvincing given the clear existing illegality of such acts. Gray, *International Law and the Use of Force*, 146.

of the digital space. The question of intent is, however, largely a function of the kinds of tools used in the attack itself. In some cyberattack examples, the target follows closely enough that intent is simple to ascertain. For instance, a kinetic cyberattack that physically disrupts critical information infrastructure could clearly reflect intent if the outage was targeted — for instance, disabling a military base's external network connections. The same would be true in the Estonia attacks, which targeted few if any networks outside the nation; likewise if a cyberattack were to use carefully constructed tools that limited their effectiveness to certain national targets or geography. The *Stuxnet* worm, discovered by Russian researchers in June 2010 and documented in a series of subsequent articles, appears to be one such tool.[160] According to press accounts, it specifically targeted Iranian nuclear centrifuges, was designed to tunnel into only those networks to gain access to them, and to activate only after confirming its presence within Iran. In all such cases, the difficulty in assigning culpability is not one of intent, but attribution (see below).

Other cyberattack tools provide far less obvious signs of intent, resembling in some instances the complications posed by naval and landmines, and in another, by biological weapons. For instance, targeting shared information infrastructure serving a broad swathe of Internet users (for instance, aspects of the Domain Name System, or large routing hubs that serve government *and* private sector clients), would appear far more consistent with Iran's mining operation in

[160] BBC News, "Stuxnet Worm Hits Iran Nuclear Plant Staff Computers," 26 September 2010; Nicholas Falliere, "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems," *Symantic Connect*, 6 August 2010; Associated Press, "Iran's Nuclear Agency Trying to Stop Computer Worm," *The Independent*, 25 September 2010; BBC News, "Stuxnet Virus Targets and Spread Revealed," 15 February 2011.

Oil Platforms — disruptive, but difficult to ascertain specific targeting. In these cases, a state's objective may be large-scale disruption, or simply obfuscation of a more targeted outage. Due to these networks' interconnection, disabling functionality in the victim state could require disrupting infrastructure in another, thousands of miles away; to the victims, however, there would be no clear delineation between 'target' and 'collateral damage.' While typically less effective, and almost certainly less compliant with the *jus in bello* (as the next chapter will address), these latter types of tools could be particularly attractive to an aggressor state seeking to frustrate the regulative regime on force. It happens that these are also the tools and techniques that are most easily acquired on the open market, as they exploit widely-know vulnerabilities often through unsophisticated methods.

Likewise, the intent of a cyberattack that made use of a highly prolific virus to disable large swathes of pervasive infrastructure — rather than, for instance, by disabling the infrastructure by flooding it with traffic — would be subject to more straightforward scrutiny.[161] Indeed, in that case, multiple nations in on-going hostilities with an attacker might claim an attack against them, which if the interpretation of *Oil Platforms* were to hold, might stymie the case brought by any one. Here emerge the parallels between certain types of cyberattacks and biological weapons — categorized under today's parlance as a Weapon of Mass Destruction. Biological weapons are designated as such in part because their

[161] From a technical standpoint, the distinction here is between a virus like *Stuxnet*, which reportedly have effect only on obscure hardware known to be in use at Iranian nuclear facilities, and a virus like *Conficker*, which infects and spreads to nearly any Windows machine to which it is introduced.

intent is obscured by the inability to exercise meaningful discrimination in targets. The subject of whether cyberattacks might be proscribed under a similar rubric will be taken on in depth in the next chapter. For the purposes of determining an "armed attack" however, it is worth noting the development of such a special category in weaponry, in part to address this challenge of how such high-collateral weapons might demonstrate a discernable 'intent.'

Reference to 'terrorism.' As a concluding note on this question of attribution, there may be ways for states to shorthand this complex task of demonstrating intent by subsuming a cyberattack within existing precedent responding to so-called 'terrorism.' This approach comes with considerable legal and analytical baggage. The definition of 'terrorism' is highly contested and the debates far too detailed for substantial treatment here.[162] It is also not a conceptually clean comparison. As a tactic, one could envisage a distant scenario in which cyberattacks were used in a state-sponsored act of terrorism, but such origins would reveal little about the legality of the cyberattack itself. Finally, focusing on the concept of terrorism runs the risk of overemphasizing the use of disruptive digital tools by terrorists, a particular fixation of the literature in the early 2000s and the weaknesses of which have already been covered in-depth.

Nonetheless, it remains plausible that states could engage in a sustained legal and complementary normative campaign to define instances of cyberattacks under the same precedents governing responses to terrorist acts. South Korea, for instance, has sought to do just that in response to numerous cybersecurity events it

[162] For a comprehensive sample of the evolution and present arguments, see: Ben Saul, ed. *Defining Terrorism in International Law* (Oxford: Oxford University Press, 2006).

believed to be emanating from North Korea.[163] Such a strategy would be notable and potentially powerful, since the *jus ad bellum*'s provisions on self-defense from terrorism seem generally more permissive than those of response to other manner of force.[164]

In summary then, some more sophisticated and precise cyberattacks show an element of 'intent' discernable to most; others however, particularly those using blunter digital instruments, could frustrate the present regulative regime. Without question, present customary international law leaves much to be desired on this issue, particularly for the purposes of applying the existing regulative regime to cyberattacks. Absent that, states might pursue a strategy merging a cyberattack with the normative or legal features of 'terrorism' — an approach that may bear fruit, but may just as well become mired in a definitional debate limiting the prospects for consensus.

***Conclusions Applying the Remedial* Jus ad Bellum**

This section examined how existing international law and precedent could inform the legality of an act of self-defense to a cyberattack. The international law on the topic is clearly unsettled, and offers no simple tests for determining compliance with Article 51. Nonetheless, some well-developed specific concepts do apply to cyberattacks. First, there remains an exception preventing substantial response to *de minimis* attacks — though the cyberattacks under discussion in this study seem somewhat unlikely to be deemed a 'mere border incident.' An

[163] *Op. cit.* p. 102 footnote 65.

[164] Moir, *Reappraising the Resort to Force*, 147.

insidious but cascading cyberattack might well push the law on 'accumulation of events' forward, since with a sufficient level of aggregate effect, the law seems potentially receptive to authorizing a response. Certainly, it would do so in the event of a cyberattack targeting a military, but this condition is necessary but insufficient to authorize force in self-defense. The attack would need to have some strategic effect on the victim state. The timing of self-defense need not be once an attack has reached full effect, but a largely preventive response seems far more permissible as a matter of law than the contested (and technically questionable) notion of pre-emptive disarmament. Finally, to avoid misapplication of Article 51, I argued that some public demonstration of attacker intent was particularly important in the case of cyberattacks, though subsuming the event beneath the law and practice on terrorism might be one (fraught but possible) method to sidestep this requirement.

The presence of a strategy to craft a legal response does not, of course, render any response lawful. It remains bound by the exceptionally important legal consideration of proportionality. Absent context, it is impossible to conduct a determination of what specific responses the law might empower. That is a subject for future legal and policy analysis.

While the law remains unsettled on many important issues, there is little that would categorically prevent — and much that would empower — a state's exercise of its inherent right of self-defense under Article 51.

3.7 Conclusion: The *Jus ad Bellum* as a Restraint on Cyberattacks

This chapter argued that cyberattacks clearly run afoul of the U.N. Charter's restrictions on the use of force, and that even conservative readings of the right to self-defense point to states' rights to repel a cyberattack. More generally, the increasing use of the tool is likely to lead to development of customary international law on the use of force more generally. That acceleration is overdue to address issues across the spectrum of force, including, but by no means limited to, cyberattacks.

Beyond the scholarship itself, these arguments provide a template to assert the illegality of and a right of self-defense against cyberattacks. They demonstrate that while states themselves have been slow to develop the legal rationale for asserting cyberattacks against them illegal, such arguments are generally sound. The same holds for the claims of individual and collective rights of self-defense that the first half of this chapter documented. One could speculate, then, that the present regime regulating the use of force is operating, and that states' non-use of cyberattacks is in part attributable to it. This would assume, though, that the arguments herein represent a 'silent consensus,' well understood but unspoken by states in their security choices.

After all, soundness of these arguments cannot assume their adoption in customary international law. The latter is an issue of agency. State views and expressions matter, and this level of tenuousness is one familiar in international law. As Cassese notes:

> "The expression of legal views by a number of States and other international subjects about the binding value of a principle or rule, or the social and moral need for it is observance by states, may be held to be conducive to the formation of a principle or customary rule, even when there is no widespread and consistent State practice, or even no practice at all, to back up those legal views."[165]

[165] Cassese, *International Law*, 161.

Should states pursue these arguments, and exercise these rights, this sort of analysis would provide the basis for them to do so. Meanwhile, the ambiguities and lack of development in the *jus ad bellum* will provide the counterpoints and rejoinders. At that time, the subject will be ripe for further analysis, adopting not an analogical methodology, but one based upon discrete case studies and state justification. Until then, the *jus ad bellum* offers a strong basis for a regulative regime on cyberattacks, but the demonstration of which is impossible.

Applying this regulative regime to cyberattacks is a promising means for its restraint, but it is by no means last word on the subject. Particularly given uncertainties in the law and its interpretation, states' rationalist and normative-regulative judgments will factor substantially into whether and how this regime functions. Chapter 2 examined the prospects for the former. The following chapter considers the latter.

Chapter 4:

Cyberattacks and the *Jus in Bello*

TABLE OF CONTENTS

Do cyberattacks violate the humanitarian 'laws of war?' Are they disproportionate or indiscriminate, and thus might international law regard them as inherently problematic? If so, are they functionally 'unusable' to states concerned with their status within international society?

Questions like these perennially accompany new military innovations, and with good reason: the regulation of warfare itself is a curious but powerful force in international relations. Shared understandings about 'acceptable' means of coercion, and the canon of international law they undergird, are central to state decisions about the means and methods of warfare they undertake.

As outlined earlier in this study, the international status of cyberattacks remains deeply unsettled from the standpoint of rationalist deterrence calculations (Chapter 2), and largely unconsidered from the standpoint of international law under the *jus ad bellum* (Chapter 3). States' reticence to claim credit for individual cyberattacks may also be connected to their questionable status within the ethical and humanitarian principles of just conduct in war.

As a practical matter, a state's options in applying force are not unlimited. In most circumstances, they are substantially informed by international law and practice, which prohibits a number of general categories of activity as well as certain specific types of weaponry. It is an important feature of international relations that certain weapons do not easily comply with that law: consider the special status reserved for chemical and biological weapons, land mines, and poison bullets, to name only a few examples. It is no coincidence that those tools, functionally proscribed by the law, are rarely used in international conflict. It may be equally true that if cyberattacks inherently violate the *jus in bello*, states could find it difficult to justify their use. The result could be a strong force of restraint on cyberattacks even when, like poison gas in World War II, or nuclear weapons in the first Gulf War, the tool could be of substantial utility.

This chapter considers the legal case for restraint on 'humanitarian' grounds. It examines the evidence that cyberattacks might violate the *jus in bello,* and accordingly whether or not these laws are a potential restraint on state decision-making. Informed by the conclusions of prior chapters, it begins by noting that tenuous legal status may underpin states' reluctance to claim responsibility for cyberattacks, as argued in Chapter 2. It then argues that cyberattacks inherently violate the two core tenets of international law governing the conduct of hostilities, proportionality and distinction. As such, cyberattacks' incompatibility with the *jus in bello* offers meaningful prospects for restraint, given most states ready acknowledgment that their choices are bound by that existing canon of law.

Explaining the 'Cyberattack Anxiety'

Prior chapters have pointed out an apparent paradox in states' relationship to their own cyberattack capabilities. Many states have publicly created new military units devoted to cyberattack planning and execution, and furthermore have made clear their willingness to respond in-kind to a cyberattack. At the same time, states exhibit a strong aversion to admitting participation in any particular episode. No state has yet publicly claimed responsibility for the use of cyberattack tools on any scale, large or small. Russia never openly admitted any involvement in the attacks on Estonia nor, more surprisingly, as part of its invasion of Georgia. China has never admitted, and in fact publicly denied, conducting any cyber operations, despite widespread reporting to the contrary. Israel has never addressed the rumors that it disabled radar systems prior to its attack on Syria's nuclear site. North Korea has never made public its involvement in the July 4, 2007 denial of service attacks on South Korea. And the United States has neither confirmed nor denied involvement in *Stuxnet*. Regardless of their actual complicity, states are silent on these issues.

This incongruity is notable, and the reasons for it are worth exploring. If states are so publicly formulating deterrence postures, it seems curious that they would dodge responsibility for individual acts, especially when doing so risks creating a reputation for poor cyberattack capabilities. As a general matter, states' denial of involvement might be explained in terms of their limited deterrence value (as Chapter 2 outlined). With respect to attacks already executed though, surely there must be value in conditioning adversaries to the potential of a repeat action. This deterrence approach, therefore, only partially explains the present and uneasy relationship between states and the public attribution of cyberattacks.

The conclusions of prior chapters suggest a more compelling explanation for this reticence — that international law might not just condemn cyberattacks as a use of force, but on humanitarian grounds as well.

The *jus in bello*, governing all aspects of conduct in times of hostilities, is uniquely powerful. Because it is international in origin, it is regarded as universal in scope. It also places the burden of proof on parties that might be seen as out of alignment with its precepts in the use of a novel weapon.[1] The result is a canon of law with not only notable history and recognition, but general applicability to state behavior in the use of new technologies.

History suggests that this concern may have played an important part in what little we know about state decision-making on the issue. Cyberattacks have, from their first availability in warfare (usually considered the 1994 Gulf War), elicited strong concerns among policymakers, international lawyers, and military ethicists alike.[2] As early as the 1990s, senior officials of the Russian Federation proposed segregating cyberattacks into a legal and normative category reserved for ‘heinous’

[1] Ingrid Detter, *The Law of War*, 2nd ed. (Cambridge: Cambridge University Press), 154.

[2] Markoff and Shanker, "Halted ’03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk."

weapons of war and, specifically, “weapons of mass destruction.”[3] Even a decade on, contemporary expert reports prepared for the United States government openly question whether cyberattacks offer any ethical advantage to traditional weaponry, and raise serious questions (but offer few answers) on their compliance with the spirit and letter of the *jus in bello*.[4]

States’ curious silence on their involvement in cyberattacks might be attributable to concerns that they violate the *jus in bello*. If, as Ward Thomas argues, “power relies upon a sense of legitimacy” that is in turn deeply bound up with states’ behavior in wartime, cyberattacks’ questionable usability according to the *jus in bello* may well explain states’ silence on the issue.[5] The question that frames this chapter, then, is whether such an explanation is legally sound, and by extension, if the *jus in bello* could explain not just silence, but restraint.

Outline of Argument

The following section (4.1) introduces the concept of legal restraints on conduct in warfare, introducing the *jus in bello*, and explaining why this body of law is a particularly strong and relevant framework for analysis of novel weaponry. The subsequent two sections consider whether cyberattacks indeed violate the *jus in bello*’s core provisions. The first (4.2) argues that cyberattacks could potentially violate the requirement of proportionality because their unpredictable effects make

[3] "Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General."

[4] “Cyberattacks cannot be regarded as a more ‘benign’ form of warfare…simply because a cyberattack targets computers or networks.” United States National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. p. 251. Hereafter, NRC.

[5] Ward Thomas, *The Ethics of Destruction: Norms and Force in International Relations* (Ithaca: Cornell University Press), 11.

them difficult to limit. The second (4.3) concludes on numerous grounds, including violation of neutrality and non-combatant immunity, that they almost certainly violate the requirement for distinction. The result is a strong basis for the *jus in bello* to discourage state use of cyberattacks.

4.1 Studying Limitations on Warfare

This section provides a brief overview of the canon of law governing the conduct of warfare, and why it is particularly applicable to cyberattacks. It first covers the premise of the *jus in bello* and its historical origins; then covers the sources of law that make it up; and concludes with a brief discussion of the methodology which the balance of the chapters uses to consider cyberattacks in that context.

Overview of the **Jus in Bello**

The *jus in bello* clearly delineates the responsibility of states toward one another, and with respect to non-participants, during conflict. It is particularly powerful because of its universal applicability: its most basic provisions are held to apply to all states, regardless of a declaration or recognition of war, and to all combatants "irrespective of the justice of their cause."[6] Should cyberattacks inherently violate its provisions, history suggests some level of state restraint could form against their use — a fate that befell chemical weapons, biological weapons, and

[6] Sir Adam Roberts, "The Equal Application of the Laws of War: A Principle under Pressure," *International Review of the Red Cross* 90, no. 872 (2008): 936-7, 41.

antipersonnel land mines.[7] While the operation of the law is imperfect, its letter is clear: the right to injure is "not unlimited."[8]

There is little question within international law that states are bound by a variety of obligations to evaluate cyberattacks' lawfulness within the *jus in bello,* but they have yet to do so publicly. Article 36 of the 1977 Geneva Protocol I is as equally applicable to cyberattacks as any novel weapon of uncertain international status:

> "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contract Party."[9]

Accepting the analysis of the preceding chapter, any state contemplating a cyberattack would need to ensure the "means or method" does not categorically — nor is substantially predisposed to — run afoul of the *jus in bello*.

Such analysis is important, rare, and lacking in the context of cyberattacks. It is important as a lens through which to assess future state claims about the legality of their actions in context. Responsibility for the commission of war crimes, or other gross international misconduct, is often highly context-dependent; firmly establishing the abstract legality of an action can help inform whether the subject should have known its status. It is rare for reasons of pragmatism. One can understand the

[7] See: Kim Coleman, *A History of Chemical Warfare* (New York: Palgrave Macmillan, 2005); Joshua Lederberg, *Biological Weapons: Limiting the Threat* (Cambridge, MA: MIT Press, 1999); Maxwell A. Cameron, Brian W. Tomlin, and Robert J. Lawson, eds., *To Walk without Fear: The Global Movement to Ban Landmines* (Oxford: Oxford University Press, 1998).

[8] Sir Adam Roberts and Richard Guelff, *Documents on the Laws of War*, 3rd ed. (Oxford: Oxford University Press), 9; International Committee of the Red Cross (ICRC), *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)* (Geneva), Article 35(1). International Conferences (The Hague), *Hague Convention (II) with Respect to the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land* (The Hague), Article 22.

[9] International Committee of the Red Cross (ICRC), *Additional Protocol I (1977)*, Article 36.

reluctance of a state, seeking to deploy a novel weapon, to identify how it might comply with the law absent a particular use case. To do so would be to invite liability and pre-emptive limitations on its use. Finally, it may well be lacking for the reasons forgoing, and based on the novelty of the issue. It therefore creates a lacuna within both the policy and legal literature worthy of dedicated focus.

The lack of military conclusions about cyberattacks' place within the *jus in bello* is particularly notable, and perhaps alarming, when one considers the consensus that any major conflict among military powers will have a cyberattack component.[10] A recent and comprehensive report of the U.S. National Academies, one of the very few of its kind to specifically consider strategic *and* ethical issues that cyberattacks implicate, concludes little beyond the issue mattering for military planners.[11] There is evidence that this is not a novel conclusion, and that the issue has gone largely undeveloped for over a decade. A 1999 U.S. Department of Defense report concluded "[t]he magnitude, scale, and nature of a cyberattack's effects, both direct and indirect, have to be taken into account in ascertaining its significance, and it is not simply the modality of the attack that matters."[12] In avoiding the question, let alone the answer on their legality, states suggest there may be much about cyberattacks that run afoul of even the basic premises of the *jus in bello* to which nearly all states would identify themselves as bound.

[10] Select Committee on Intelligence, United States Senate, *Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community*, 31 January 2013, 1-2.

[11] United States National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*.

[12] NRC, *citing* United States Department of Defense, *An Assessment of International Legal Issues in Information Operations*, ed. Office of the General Counsel, 2nd ed. (Washington: U.S. Department of Defense, 1999).

While the sources of the *jus in bello* are diverse and historically rich — as subsequent sections will document in part — much of the relevant law spanning the late nineteenth century to the present converges around two premises: proportionality and distinction. Both those measures of law aiming to regularize conflict, and the far more numerous provisions seeking more explicitly humanitarian aims of limiting undue suffering, reflect one or both premises. It is as true of regulations on specific weaponry, from the Hague Declarations of 1899 to the 1997 Ottawa Convention on land mines, as it is for general diktats on conduct in war, from the Hague Conventions of 1907 to the more recent Geneva Protocols of 1977.

In the absence of *lex specialis* pertaining to cyberattacks, this chapter applies the *lex generalis* of the *jus in bello* — the cornerstones of which are the principles of proportionality and distinction — to consider the acceptability of their use. Following a brief methodological and sourcing note, the next section considers proportionality; the subsequent section examines distinction.[13]

Sources, Methodology, Scope

Sources. As in the last chapter, the sources of law cited in this chapter are consistent with the traditional sources of customary international law. In the context of warfare generally, these include international treaties[14] (both the *lex generalis* asserting principles like non-combatant immunity and *lex specialis* covering proscribed means and methods); a limited set of relevant case law; the writings of

[13] Most legal scholars use the phrase ‘distinction’ and ‘discrimination’ interchangeably; to minimize confusion with the dual political meaning of the latter, this study favours the former.

[14] Adopting a shorthand also employed by Roberts, this chapter will refer specifically to ‘treaties,’ encompassing positive law, convention, declaration, protocol, procés-verbal, or statute. See: Roberts and Guelff, *Documents on the Laws of War*, 5.

legal specialists; resolutions of international bodies; and national manuals guiding state behavior. In the specific context of cyberattacks, as previously documented, only the latter three exist at the time of writing, and even then are limited to two U.N. Group of Governmental Expert Reports, a handful of annual General Assembly resolutions, and national policy guides that are almost categorically military rather than international-legal in character. Therefore, beyond straightforward analysis of the normative and legal applicability of general principles like proportionality, an analogical methodology is again the best way to contextualize cyberattacks.

Scope. This chapter, while focused on laws with an ethical orientation, is not focused on the assignment of ethical value to one outcome or the other, nor does it evaluate the ethical weight of any existing normative regime. As McMahan aptly notes, "the morality of war and the laws of war are utterly different," but "this is not to say…the *content* of morality and law must be utterly different."[15] This chapter continues to be motivated, as this study has been throughout, by the notion that limiting cyberattacks is a project with great potential to improve international security and reduce undue suffering and destruction of value. Whether one deems this an ethical or political imperative affects the analysis and outcome very little. Even in the neoliberal and English School approaches, the tendency to limit conduct in war flows directly from those seeking to limit recourse to force, which in turn stems from the need to order and derive long-term benefit from an 'international society.'[16] Thus the

[15] Jeff McMahan, "Laws of War," in *The Philosophy of International Law*, ed. Samantha Besson and John Tasioulas (Oxford: Oxford University Press), 497.

[16] Hedley Bull and Adam Watson, eds., *The Expansion of International Society* (Oxford: Oxford University Press), 3. See also: Hedley Bull, *The Anarchical Society*, 3rd ed. (New York: Columbia University Press, 2002 [first published 1977]); Martin Wight, *Systems of States* (Leicester: Leicester University Press, 1977); Andrew Hurrell, *On Global Order: Power, Values and the Constitution of International Society* (Oxford: Oxford University Press, 2007). For the context of Bull's work, see

need for certain actions to be ‘off limits’ endures with either an ethical/humanitarian or neoliberal frame of reference, the latter of which this chapter maintains.

4.2 *Jus in Bello* Proportionality

The principle of proportionality requires first that in armed conflict, states’ actions do not substantially exceed the injustice the war aims to correct, and second that ‘retributive’ actions do not cause undue or inhumane suffering to the opposing party. State respect for some version of proportionality is apparent in choices made during many limited wars and punitive military strikes of the last few decades, though this principle is paradoxically less developed in positive law than the principle of distinction. This section first explains the origins and meaning of the concept, and then explores whether cyberattacks *prima facie* violate the principle by being either inherently escalatory, or uncontrollable in their effect.

The Concept of Proportionality

Proportionality, as a general matter, represents a requirement that the response needed to cease or correct a breach (usually a violation of law, like the use of force) not overwhelm the initial act in aggregate damage or suffering inflicted. Enshrined in custom and referenced in some of the seminal documents of the *jus in bello*, proportionality requirements are deeply ingrained in military doctrine and practice. This section briefly traces the principle of proportionality’s development and disaggregates it from other relevant contexts of law, such as in the *jus ad bellum*.

Hurrell’s introduction to the 3rd Edition of The Anarchical Society, esp. vii-xii. On the relationship of the concept to state interest and norm formation, see: Martha Finnemore, *National Interests and International Society* (Ithaca: Cornell University Press, 1996).

The limitation on conflict now deemed ‘proportionality’ long predates formal international law governing the conduct of hostilities, and its content and context have changed considerably over time. Proportionality in the eighteenth century was more a descriptive feature than a positive requirement of warfare. In that era of ‘limited wars,’ the conduct of European war was structured around certain political aims, well-understood tactics, and predictable weaponry. James Turner Johnson, in his inquiry into the historical and ethical aspects of restraints on war, summarized the result to be “a style of warfare defined by limited goals, limited destructiveness to property, relatively little dislocation of the normal life in the belligerent states, and a relatively low cost to human injury and death.”[17] Without implying that the wars of the era were without human toll, as they assuredly came at substantial cost, the scale of destruction was notably circumscribed in comparison to conflicts of the nineteenth century and beyond.

An international legal *requirement* of proportionality is best understood as a product of its era, as the changing character of war in the nineteenth and early twentieth century drove it from a ‘self-limited’ contest of armies to an unlimited clash of populations. Wars of the nineteenth century were notable for their infusion of ideological and nationalistic aims; a shift from political control over territory to destruction of opposing forces, and the mobilization of national economies, and the *levée on masse*.[18] The changing definition of victory, now tallied by the number of enemy soldiers killed, units destroyed, and civilian force support depleted, was

[17] James Turner Johnson, *Just War Tradition and the Restraint of War* (Princeton, NJ: Princeton University Press, 1981), 821-3.

[18] *Ibid*., 282-3.

compounded by an increase in the scale — but not accuracy — of armaments.[19] The result was an unprecedented humanitarian catastrophe. The circumstances set ethicists and officials in search of a canon of law applicable to just conduct in war, leading scholars like Helleck and Lieber to predecessors like Vattel and Van Bynkershoek in developing the foundation of the modern canon of the *jus in bello*. Surrounded by the reality of wars with 'unlimited aims,' the need to impose specific limits on that practice was, if not immediately obvious, increasingly clear over the decades leading up to the 1899 Hague Convention. The First and Second World Wars crossed all such boundaries and marked the apogee of the trend, giving birth to the United Nations Charter and Geneva Conventions designed to preclude similar horrors.[20] As the *jus in bello* evolved, it has consistently reaffirmed that states must observe in their conduct limitations on the use of even 'permissible' force, whether individual or collective self-defense, or individual or collective humanitarian intervention.[21]

What is meant today by proportionality within international law must be read in the historical context of both eras, when it served first an 'organizational,' and subsequently a 'humanitarian' purpose. *In bello* proportionality shares a similar ethical orientation to its *ad bellum* counterpart; both are concerned with limiting undue suffering, though the former is concerned with conduct, and the latter recourse

[19] *Ibid.*

[20] A. J. Coates, *The Ethics of War* (Manchester: Manchester University Press, 1997), 214-20..

[21] Most notably in Geneva Protocol I. International Committee of the Red Cross (ICRC), *Additional Protocol I (1977)*, Art. 35. On the U.N. Charter, see: Jochen Frowein, "Article 41," in *The Charter of the United Nations: A Commentary*, ed. Bruno Simma (Munich: C.H. Beck, 1995), 631. On intervention, see: Claude H. M. Waldock, "The Regulation of the Use of Force by Individual States in International Law," *Recueil des Cours de l'Academie de Droit International (RCADI)* 81 (1952): 464.

more generally. There is an important and relevant debate in the literature over the divergence in meaning here. In essence, it is an argument over the scope of suffering the *jus in bello* proportionality seeks to prevent: whether it pertains only to combatants, to populations, or to the international community more broadly. Some, for instance, have attacked the premise of *in bello* proportionality entirely, declaring it an imprecise application of a concept reserved for another context.[22] This extreme view is moderated somewhat by scholars like Gardam, who argue that proportionality in the *jus in bello* is principally humanitarian in character and concerned specifically with individual combatants (lest it collapse into a separate requirement, distinction).[23] This more limited perspective is understandable in the context of proportionality's most recent history, but ignores the fact that *in bello* restraint can meaningfully limit belligerence to the smallest possible number of *states*. Thus, the exercise of proportionality as a tactical tradition, as in every state-based naval battle since the Second World War, has also helped prevent drawing other neutral vessels and their governments.[24]

A few tests of proportionality validate this more holistic view: that proportionality aims to limit the suffering of both combatants and would-be combatants in otherwise neutral states. For instance, in evaluating the proportionality of an act, scholars like Bowett weigh it against the "danger" created by the prior act of

[22] Henri Meyrowitz, *The Principle of Superfluous Injury or Unnecessary Suffering: From the Declaration of St. Petersburg of 1868 to Additional Protocol I of 1977* (Geneva: International Committee of the Red Cross, 1994), 109-10.

[23] Judith Gardam, "The Contribution of the International Court of Justice to International Humanitarian Law," *Leiden Journal of International Law* 14, no. 2 (2001): 349.

[24] D.P. O'Connell, *The International Law of the Sea*, ed. I.A Schearer (New York: Clarendon Press, 1983), 1096.

force; Waldock weighs whether the action is required for achieving the objective (if lawful); and Higgins weighs the act against the injury inflicted.[25] In each case, not only would an act by one combatant against another violate the premise, but so too would an act by a combatant that escalates, draws in more combatants or belligerents, or runs the inherent risk of doing so. Such an act would necessarily outweigh the 'danger' created; diminish the prospects of achieving the lawful objective (peace); and outstrip the injury inflicted.

For the purposes of this analysis then, an act is proportionate within the *jus in bello* if its effects — on both opposing combatants and the universe of potential belligerents — cause neither undue suffering nor undue escalation of the conflict (compounding the suffering). For an act to meet that criteria, it must be circumscribed in area and effect, and, crucially, *knowable* in its extent of each.[26]

An act cannot be proportionate if there is no action, short of existential threat, to which it is a proportionate response. There are two characteristics that, individually or combined, would render a weapon *prima facie* non-compliant with this provision. First, weapons might, by their very nature, be *inherently escalatory* to any action to which it might be leveled in response, and so only usable under existential threat. Second, it might be *variable and unpredictable* in the scale of its effect, meaning a state using it would be effectively rejecting the premise by

[25] Bowett, *Self-Defence in International Law*, 269; Waldock, "The Regulation of the Use of Force by Individual States in International Law," 463-4; Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Oxford: Oxford University Press, 1995), 231.

[26] From a humanitarian standpoint, this condition holds in all cases except the 'existential' one. Wars for survival — which is to say armed conflicts in which not just the state, but the lives of every citizen therein are under threat of extinguishment — negate the premise of proportional response. The escalation of conflict to such a point renders theorizing on some aspects normative restraint, and certainly on proportionality, impractical.

executing such an attack in the first place. This section considers each in turn, and concludes by recognizing the challenges of deeming an act 'unusable' on the primary basis of it being disproportionate.

Escalation

If an action were 'superlatively destructive,' it would be an escalation to any action antecedent to it; thus it could not be proportional, nor permissible, under the *jus in bello*. Cyberattacks are often alleged to possess such 'uniquely damaging' qualities. Top Russian officials have repeatedly likened the use of cyberattacks to weapons of mass destruction, and specifically nuclear weapons, as did the Estonian Defence Minister following the attack on his country.[27]

As a grounding analogy, a nuclear attack is the emblematic case of an act so superlatively escalatory that it seems patently incompatible with the *jus in bello*. Pound-for-pound, nuclear weapons are generally understood to be the most destructive capability in military possession. Spectacularly on display in Hiroshima and Nagasaki, and throughout the nuclear tests that became symbolic of the Cold War, military planners have long wrestled with and failed to construct a proportionate nuclear response to a nonnuclear act.[28] This is the conclusion generally reached by the international legal community, excepting the case of a response to prior use of nuclear weapons.[29]

[27] *Op. cit.* p. 68 footnote 119; p. 7 footnote 3.

[28] See, e.g., the United States' deliberations relating to Quemoy and Matsu: Bundy, *Danger and Survival*, 273-87.

[29] See: Ian Brownlie, "Some Legal Aspects of the Use of Nuclear Weapons," *International and Comparative Law Quarterly* 14, no. 2 (1965): 15; Georg Schwarzenberger, *The Legality of Nuclear Weapons* (London: Stevens & Sons, 1958), 40.

Destructiveness is, however, a function of time as well as effect. The net effect of conventional bombing can easily surpass both in destructiveness and casualties caused a single nuclear strike, the firebombing of Tokyo in World War II being an oft-cited and relevant example. What distinguishes nuclear weapons in this respect, then, is that the action is singular and spectacular, rather than cumulative and cascading.

When compared with the immediate, direct, and 'superlative' destruction of a nuclear weapon, it is clear that cyberattacks are not inherently escalatory. Cyberattacks can be disruptive and destructive, but they are not inherent escalations from any aggressive act coming before. In fact, one can envision circumstances in which an act causing physical harm were countered by a cyberattack, and regarded by the initial attacker as de-escalation. Any number of traditional military actions that might be *more* disruptive, destructive, or illegal than a cyberattack itself, and thus responding with a cyberattack would not itself by unconscionable escalation. Cyberattacks are also not categorically (by purposeful design, rather than effect) causal to specific losses of human life or utter destruction in the vein of, for instance, a nuclear weapon. Destruction is indirect and would appear to civilian populations cumulative, seemingly more akin to repeated bombing than a single, spectacular act. Cyberattacks also possess a quality not true of all weapons: they might be reversible, at least in some measure.[30] This makes their proportionality also variable, rather than

[30] Some commentators (notably Schmidt) argue that *reversibility* might re-designate cyberattacks as weapons of war to lesser tools of influence, like economic sanctions. Even with the arguments of the prior chapters notwithstanding, that argument is suspect. Weaponized germs are still bacteriological warfare, and their instruments biological weapons, even if there exists an antidote or likelihood many individuals will recover from illness on their own.

the irreversible and categorical effect that defines weapons so disproportionate they cannot possibly comply with the *jus in bello*.

There exists a scale of disruption that might take place, dependent in no small part on the state's level of technological dependency. One can envisage a cyberattack that, in overloading electricity grids, disrupting dams and water supplies, and interfering with air-traffic control, creates high losses of life. However that same cyberattack, which had an utter and devastating effect on one state, could have a minimal effect on another due to the latter's lack of dependency on information systems. Therefore, until such a time that a preponderance of states (i.e. sufficient number to create a widely shared understanding of a norm) are so dependent as to render disruption universally recognizable and substantial, cyberattacks are unlikely to be subject to categorical proscription solely because they are superlatively destructive or inherently escalatory, and therefore disproportionate.

Uncontrollable Effect

To ensure a particular action is proportionate, a state must also know the upper and lower bounds of its likely effect, and be able to narrow it according to the threat at hand.[31] Biological warfare, specifically the weaponization of viruses or bacteria that spread through human contact, are an example of actions that most likely violate this aspect of the *jus in bello*.[32] The conditions under which an agent would have greater or lesser effect would be uncontrollable, and perhaps even unknowable, to the state deploying it.

[31] United States Air Force, *Commander's Handbook on the Law of Armed Conflict 6-2* (Washington: U.S. Department of Defense, 1980), 1-6.

[32] Biological warfare also violates notions of discrimination discussed in the following section.

Cyberattacks do have a kind of unpredictability that might run afoul of the *jus in bello*. The study's introduction outlined how cyberattacks, in frequently targeting shared information infrastructure, can have cascading effects across multiple interconnected systems. The reality, also explored in prior chapters, is that those effects are not entirely knowable. The more an attacker targets interconnected infrastructure, the less predictable those effects are.

This is not to say that there is no predicting the effect of any offensive activity in cyberspace. A virus can be programmed to attack only a single machine, and the known extent of that machine's operation could render the effects extremely limited. Cyberattacks in the most relevant interstate context are defined in part by targeting shared information infrastructure that is inherently prone to cascading effects, knowable and otherwise. So while a single offensive action (implanting a virus) might be wholly predictable, the full effects of a cyberattack of meaningful concern in international security are difficult if not impossible to fully anticipate.

This observation suggests a preliminary way that a cyberattack might *prima facie* run afoul of proportionality provisions: the more complex the critical infrastructure it targets, the less knowable all collateral effects are, and the less likely proportionality can be intentionally integrated into attack planning. The fact that this cascading effect is knowable is legally relevant, thus imperiling cyberattacks' 'usability' in general terms.

Implications

Though grounds exist to suspect cyberattacks may be somewhat disproportionate, they are less than sufficient to render the tool patently 'unusable' according to the *jus in bello.* Proportionality is fundamentally a relative and reactive quality: relative, in that is must be judged against the perceived or real wrong (presumably a violation of international law and/or the victim states' interests), and reactive in that without the antecedent act, the question becomes moot. In this respect proportionality is, almost by definition, context-dependent, and while "the requirements of proportionality *in a given instance* may be debated at great length," when systematized, those debates tend to end "inconclusively."[33] This fact frustrates attempts to categorize a weapon as 'unusable' under the *jus in bello* solely on this basis.

The second conceptual difficulty, related to the first, is that evaluating proportionality depends on notions of both perception and subjectivity.[34] One can envisage numerous scenarios in which third-party observers might disagree on the proportionality of a particular retributive response. Consider, for instance, the two 'wrongs' discussed previously — a violation of international law, and a violation of interests. An aggressor state might use chemical weapons, but with little effect to the victim (no real deaths). Some states might consider a grave and forceful response warranted (say, cruise missile attacks on military compounds), given the strength of the chemical weapons taboo. Others might, however, see that approach as undue, given the absent loss of life. A similar disagreement might break out over an aggressor states' forceful denial of an adversary's access to a rare mineral essential to the latter's economy. The conditions created may not be ones of even gross illegality, but the flexible concept of interest renders the notion of proportionality subjective at the very least. It is also subject to 'tampering' of sorts, as a state might claim exceptional collateral effect (like destruction of billions of dollars of economic value)

[33] Johnson, *Just War Tradition and the Restraint of War*, 196.

[34] *Ibid.*, 205.

to justify a more powerful response, particularly because it is difficult to externally measure.[35] International legal consensus on adjudicating specific cases of proportionality is elusive, and as demonstrated, state consensus even less so.

In summary, the principle of proportionality is unlikely to, in and of itself, provide overwhelming basis for cyberattacks to violate the *jus in bello*. While elements of the act itself do raise questions about how predictably proportionate a cyberattack can be to a perceived wrong, its method is not so obviously destructive as to be disproportionate to any precipitating act. Since proportionality is both context-dependent and lacking an adjudicatory consensus, it is a complementary, not dispositive basis for judging a weapon within the *jus in bello*.

4.3 *Jus in Bello* Distinction

The principle of distinction is far more promising in this respect. Distinction is, generally, the principle that not all objects of value to the opposing party are legitimate victims of coercion in an interstate dispute. If proportionality is the general limitation on intensity, distinction is the general limitation on scope of a conflict.

Relative to proportionality, distinction is a notably more robust, historically grounded element of the *jus in bello*. It has pervaded the practice of interstate conduct since before the existence of the modern state system. It also enjoys far greater elaboration in positive international law.[36] Some theorists, as well, argue that

[35] United States National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, 264.

[36] For example, the 1899 Hague Convention II; 1907 Hague Convention V; four 1949 Geneva Conventions; and the 1977 Geneva Protocol I all contain substantial treatments of neutral states, territory, and in some cases individuals.

distinction must be morally superior to considerations of proportionality, since the former deals in protection of the innocent from suffering, whereas the latter absent the content of the former exists only as a means for conditioning state conflict.[37]

This section first traces that long lineage, then outlines two overarching grounds on which cyberattacks could, by their very nature, run afoul of the principle of distinction: by violating the neutral rights of states, and by lacking the ability to distinguish its effects between combatants and noncombatants. It argues cyberattacks may well interfere with aspects of the former, and almost certainly run afoul of the latter — invoking numerous precedents of specifically proscribed means and methods of war.

Historical Grounding

Distinction is a particularly powerful and longstanding principle within the *jus in bello*. By most accounts, the norm of distinction within the *jus in bello* extends to the earliest records of organized warfare, and even its positive incarnation in proto-international law far predates the Westphalian state system itself. The Greeks and Romans observed principles of order and restraint in their armed hostilities through a series of "unwritten conventions," amounting to "socially constructed and socially maintained rules of war" that were in turn reflected in epic accounts of great battles and reinforced by that same mythology.[38] Those same traditions — variously justified as matters of divine decree, honor, chivalry, or 'humanity' — all contained

[37] Paul Ramsey, *War and the Christian Conscience: How Shall Modern War Be Conducted Justly?* (Durham, NC: Duke University Press, 1961).

[38] Josiah Ober, "Classical Greek Times," in *The Laws of War: Constraints on Warfare in the Western World*, ed. Michael Howard, George J. Andreopoulos, and Mark R. Schulman (New Haven: Yale University Press, 1997), 13, 17.

some element distinguishing non-combatants or protected classes, informing more theologically grounded guidance recognized, if not always practiced, by European soldiery centuries hence.

Among the earliest codifications of the norm was the 989 A.D. 'Peace of God,' declared between the Archbishop of Aquitania and warring nobility, which laid out clear protected classes from warfare that included women, children, church property, and rudimentary forms of neutral non-combatants and commerce.[39] Raymond of Peñafort's 1234 *Summa de casibus poenitentiae*, intended as a guide for confessors, was oft-cited after its publication and made clear requirements of, *inter alia, jus in bello* proportionality and distinction between "offenders and the innocent."[40] In the Middle Ages, rules of engagement and chivalry were used to discipline armies and regularize the conduct of hostilities — including drawing in turn on rigorous social distinctions between the armed *nobilis* and the "unarmed, vulgar herd of common humanity," in what became a rudimentary form of distinction.[41] In the seventeenth century, practice and certain limited treaties also sought to protect innocents caught in armed struggle, permitting the release of women and certain children free of ransom.[42] Similar concepts can also be found in Gustavus Adolphus' 1621 Articles of War drawn up for soldiers departing to fight Russia in the Baltics.[43]

[39] R.G.D. Laffan, ed. *Select Documents of European History, 800-1482* (New York: Henry Holt), 94. in Gregory M. Reichberg, Henrik Syse, and Endre Begby, eds., *The Ethics of War: Classic and Contemporary Readings* (Oxford: Blackwell Publishing, 1929), 94-5.

[40] Laffan, *Select Documents of European History, 800-1482*, 133.

[41] Robert C. Stacey, "The Age of Chivalry," in Howard (ed.), *ibid.,* 29. See also: Maurice Keen, *Chivalry* (New Haven: Yale University Press, 1984); *The Law of War in the Late Middle Ages* (New York: Routledge & K. Paul, 1965).

[42] Detter, *The Law of War*, 152.

[43] Roberts and Guelff, *Documents on the Laws of War*, 3.

Clearly distinction has been embedded in the conduct of states since their earliest interactions; from early modern Europe on, the *jus in bello* came to represent "a powerful combination of natural and divine law, ecclesiastical precepts, military law, common custom, and self-interest," imbuing it with "new and enduring consistency."[44] By the end of the seventeenth century — well before most recognized international law had taken shape — England, Switzerland, Sweden, and Germany had all developed codes of conduct for their armed forces that at a high level sought to protect civilians from marauding and other misdeeds. Following the transition from the limited wars of nobles and kings to the 'wars of nations' synonymous with eighteenth and nineteenth century Europe emerged a "passion for codification," which Adam Roberts describes as starting with the 1856 Paris Declaration on Maritime Law and leading to the 1868 Saint Petersburg Declaration's famous decree "that the only legitimate object which states should endeavor to accomplish during war is to weaken the military forces of the enemy."[45] An ocean away, the first comprehensive and modern attempt to distill these traditions as guidelines for soldiers was ventured by the aforementioned American lawyer Lieber, and codified by American President Lincoln to guide the conduct of his troops during the Civil War.[46] The 'Lieber Code,' centrally focused on distinction, was later adopted as the basis for similar guidelines by over a half-dozen powers in the period 1870-1893.[47] It is no coincidence that the

[44] Geoffrey Parker, "Early Modern Europe," in Howard (ed.), *ibid.,* 42.

[45] Sir Adam Roberts, "Land Warfare: From Hague to Nuremberg," *ibid*., 119.

[46] Instructions for the Government of Armies of the United States in the Field, General Orders, No. 100, 24 April 1863. See also: Baxter, The first modern codification of the law of armed conflict, International Review of the Red Cross, 29 (1963).

[47] These included Prussia in 1870; the Netherlands in 1871; France in 1877; Russia in 1877 and 1904; Serbia in 1878; Argentina in 1881; Great Britain in 1883 and 1904; and Spain in 1893. See: Green, 37;

International Red Cross, devoted to the alleviation of suffering in war, was founded in 1870.[48]

Thus the 1899 and 1907 Hague conferences that gave International Relations its most famous examples of positive law restraining warfare were, notably, a reflection not of security in the march of ideals and restraint but a genuine terror of new weaponry and war.[49] The Conventions they produced, particularly on the Laws and Customs of War on Land, remain among a handful of the most widely recognized and durable aspects of the positive law of war.[50] Today, they serve as the basis for the modern understanding of distinction as applied both to states, in the form of 'neutral rights and obligations,' and the more familiar version applied to 'non-combatant' individuals.

Neutrality

States not participating in a declared armed conflict, as well as states without any direct standing to be implicated in hostilities, are non-combatant entities said to be 'neutral' to it — a condition that carries with it certain rights and duties.[51] As a phenomenon in international relations, neutrality is a concept as old as the notion of

Thomas Erskine Holland, *The Laws of War on Land (written and unwritten)*, (Oxford: Oxford University Press, 1908) 71-3.

[48] David P. Forsythe, *The Humanitarians: The International Committee of the Red Cross* (Cambridge: Cambridge University Press, 2005).

[49] Roberts, "Land Warfare: From Hague to Nuremberg," 120.

[50] A 1993 report by the U.N. Secretary-General to the Security Council reaffirmed this notion, citing only four documents that comprise "the part of conventional international humanitarian law which has beyond doubt become part of" customary international law: this 1907 Hague Convention IV, the four 1949 Geneva Conventions, the 1948 Genocide Convention and the 1945 Charter of the International Military Tribunal at Nuremberg. See: United Nations Secretary-General, *Report of the Secretary-General Pursuant to Paragraph 2 of Security Council Resolution 808* (New York: United Nations, 1993).

[51] Detter, *The Law of War*, 171.

interstate war, as any state not party to a conflict was, by definition, neutral. Modern neutrality was particularly influential in maritime practice, providing a means to prevent a belligerent from interfering with vital interstate trade.[52] The constituent ideas of this principle are straightforward enough: namely, that there is collective benefit in keeping armed disputes limited to belligerents, and that the codification of certain rights guaranteed to those outside conflict would in turn help limit undue spread of war.

Over the last three centuries, these ideas crystallized into more specific customs. Those customs were, in turn, sufficiently common as to form the basis of positive legal obligations viewed for over a century as reflecting customary international law. After the first codification in the 1899 Hague Convention II, the 1907 Hague Convention V on *Respecting the Rights and Duties of Neutral Powers and Parties in the Case of War on Land* remains the foundational, systematic articulation of these rights and duties.[53] In tracing these principles — still operative in decision-making today — Hague V in particular provides a useful template to test whether a certain means or method of warfare might be partially incompatible with the principle of distinction.

[52] Roberts and Guelff, *Documents on the Laws of War*, 85-7. Terminologically, Roberts notes that the terms 'neutral,' 'non-belligerent,' and 'other states not Parties to the conflict' are effectively synonymous, with the same laws applying to all; the only distinction may come in the marginal case of a party that seeks to favour one party above another, while still acting short of participation in the conflict itself. (*Ibid.*, 86).

[53] International Conferences (The Hague), *Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land* (The Hague). Additional mention of neutral obligations can be found in the Geneva Conventions as well, specifically: International Committee of the Red Cross (ICRC), *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention)* (Geneva), Article 11.

The first obligation of neutrality falls to belligerents, to treat "the territory of neutral powers" as "inviolable," and not to transit their territory in the movement "of troops or convoys of either munitions of war or supplies."[54] Two aspects of present-day cyberattacks might violate neutral territory by analogy: first, an attackers' data transiting of third-country networks en route to the target network, and second, the use of a neutral states' 'network resources' (i.e. machines) to carry out an attack.

Whether or not an attacker violates sovereign neutrality rests on whether a country's digital networks are more closely analogized to its territory, its territorial waters, or its radio-airspace.[55] Does a 'packet' of data transiting fiber-optic cables resident within one states' borders for a matter of milliseconds constitute an incursion? That claim seems far-fetched, thus either of the latter two comparisons is appealing. States have revocable obligations to permit 'innocent passage' through their territorial waters. But that passage seems hardly innocent when the data in question is instrumental in a cyberattack. Likewise, states are under no international legal obligations to carry even 'innocent' data traffic across their borders in the way they are maritime traffic; they do so for matters of efficiency.[56] Therefore, reviewing the letter of the law in the specific *jus in bello* context, the analogy to a state's radio-airspace seems most apt. Notably, Hague V explicitly and presciently clarifies, states are "not called upon to forbid or restrict the use on behalf of the belligerents of

[54] International Conferences (The Hague), *Hague V (1907)*, Article 1.

[55] The latter refers to airspace not conventionally controlled (as it is with the passage of air traffic), but which a country could without violating international law limit third-party transmissions through. In this respect, radio-airspace differs from territorial waters, another potential analogy, since there is no international-legal guarantee of innocent passage through radio-airspace.

[56] There is great debate, for instance, as to whether or not the U.S. President needs the domestic authority to unilaterally deny passage to foreign data for national security reasons. See: Declan Mccullagh, "Renewed Push to Give Obama an Internet 'Kill Switch'," *CBSNews*, 24 January.

telegraph or telephone cables or of *wireless telegraphy apparatus* belonging to it *or to companies* or private individuals."[57] Today's network cables and switches fall well within that same definition. The data used in a cyberattack is, fundamentally, a series of signals on telecommunications cables, sometimes sent wirelessly, and over infrastructure belonging in most cases to private companies. Straightforwardly, this analogy holds.

However given the *jus in bello*'s broader intent of the maintenance of limited conflict, there is reason to reconsider whether the letter of the law matches its spirit. The basis for the protection afforded to neutral states is a desire to exclude them from unwarranted injury from a conflict in which they have no precipitating role. The prohibition on troops transiting neutral territory serves not to inconvenience belligerents; its basis lies in protecting those on sovereign territory from shouldering the burden of those assets or attack for which they bear no responsibility.

Extending the analogy to cyberattacks then, it is more than plausible that a cyberattack, the transiting of a neutral party's network, could result in undue harm to that neutral state. It is true that any network-based attack would transit third parties to reach its destination by virtue of the Internet's basic operation. However, by virtue of that same architecture, the attack would appear to be 'emanating' from the neutral state's territory. If a victim state sought a 'counterforce' attack, and to strike the source of inbound fire, absent better intelligence about the source, it may well target networks in the neutral third state. This would be precisely the kind of delimitation of

[57] International Conferences (The Hague), *Hague V (1907)*, Section 5, Article 8. Emphasis added.

territory that the principle of distinction necessarily creates, and so much of the law of war seeks to reinforce.[58]

Consider also if an attacker were to co-opt infrastructure residing within a state's borders, for instance, by building malware on an infected machine in a neutral state before infecting the target computer. Doing so would not just run afoul of both the *jus in bello* premise of neutral distinction (by inviting counterattack), but also Hague V's clear prohibition on belligerents "erect[ing] on the territory of a neutral power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces."[59] Even more obviously prohibited would be recruiting from a third state so-called 'patriotic hackers' of the sort purportedly a part of the Russian campaign against Georgia. For the same principle of not drawing others unduly into conflict, Hague V explicitly prohibits the formation of "corps of combatants" and "recruiting agencies…to assist the belligerents."[60]

A final rejoinder might claim that transiting a neutral state's networks, as many do, is a low-impact but essential act of tactical subterfuge, a 'ruse' of warfare long held to be both necessary and permitted in armed conflict.[61] It may be tactically advantageous, but the permission of rouses must be read in conjunction with broader affirmative obligations on identification of combatants, on which the rule is predicated and to which this chapter will turn shortly. Therein lies the obligation to

[58] Detter, *The Law of War*, 168.

[59] International Conferences (The Hague), *Hague V (1907)*, Article 3.

[60] *Ibid.*, Art. 4.

[61] *Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land* (The Hague), Annex, Chapter 2, Article 24.

affix emblems to all lawful combatants, lest the soldier be treated as a spy (and be afforded no protections of the law), or the state be guilty of perfidy (as a later section will explore). In the absence of this counterweight, the legality of rouses is highly suspect.

The conclusion here is that, when read in a certain context, many cyberattacks will certainly violate the principle underlying *jus in bello*'s neutral guarantees. In the interest of their own self-defense, such perceived violations might provide states a first basis to question the permissibility of the practice itself. The conclusion does not render cyberattacks utterly unusable, but does suggest a clear state interest in their circumscription, regulation, or proscription.

Indiscriminate Attack

The *jus in bello* also holds that attacks which are indiscriminate in nature — and thus cannot be reliably deployed against a designated target — violate the principle of distinction. Recognized since before the First World War in both the 1899 Hague Convention II and the 1908 Hague Convention IV,[62] Article 51(4) of the 1977 Geneva Protocol (Protocol I) enumerates the premise clearly in a more modern context:

> Indiscriminate attacks are prohibited. Indiscriminate attacks are:
> (a) those which are not directed at a specific military objective;
> (b) those which employ a method of means of combat which cannot be directed at a specific military objective; or
> (c) those which employ a method or means of combat the effects of which cannot be limited as required by this protocol;

[62] *Hague II* (1899), Article 22-8; *Hague IV* (1907).

> and consequently, in each case, are of a nature to strike military objective and civilians or civilian objects without distinction.[63]

Uniting these proscriptions are three premises of control: over an attack's effects; over those subject to its effects; and over the timeframe during which its effects are felt. If a tactic or weapon cannot be meaningfully brought under all three forms of control, it fails to comply with this provision of the *jus in bello*. Since the first premise, control over effects, mirrors the provision of proportionality just discussed, the latter two are the most relevant areas to consider here.

Control over victims. Weapons that expose vast areas or categories of targets to their effects, without regard to military effectiveness, violate this requirement. Here three well-known categories of weapons — nuclear arms, antipersonnel mines, and cluster munitions — all highlight the premise and provide a point of comparison for cyberattacks.

The principle of distinction weighs heavily on the use of nuclear weapons, narrowing to nearly non-existent their permissible practical uses. They possess exceptional explosive power and intense heat, dispersed over a relatively large radius. Additional nuclear fallout affects all people equally, and due to environmental factors, cannot be largely contained to a small blast radius. It is likewise difficult to execute a nuclear blast that minimizes the effects to protected classes, such as hospitals, churches, or areas of cultural and historical value. The result is a weapon that cannot, in most practical instances, be contained to limited targets of military value (the exception being Operation Desert Storm, where even utility of the weapon was

[63] International Committee of the Red Cross (ICRC), *Additional Protocol I (1977)*, Article 51(4).

outweighed by the precedential argument against its use in non-existential circumstances).[64]

Antipersonnel (AP) mines have also been subject to longstanding scrutiny on these grounds. In the United States Civil War even General Sherman — the originator of the well-known phrase “war is hell” — condemned the American Confederacy’s use of hidden land mines as “not war, but murder.”[65] While AP mines have for most of their history been subject to no special scrutiny in international affairs, it is also impossible to ignore the success transnational civil society has had isolating their use as inhumane on precisely the grounds that victims cannot be sufficiently controlled.[66] The origins of that historical antipathy and modern codification are worth scouring for analogy to cyberattacks.

Likewise, the notable but nominally less-successful effort to marginalize cluster munitions was built atop their inability to control targets. Critics note they “fall into a special category due to the sheer number of explosive sub-munitions that are delivered over a wide area,” while the Convention on Cluster Munitions itself notes that due to the imprecision and non-immediacy of detonations, the weapons “obstruct economic and social development…[and] impede post-conflict rehabilitation and reconstruction.”[67] These two components of distinction were

[64] Tannenwald, *Nuclear Taboo*, 294. See also: McGeorge Bundy, "Nuclear Weapons and the Gulf," *Foreign Affairs*, Fall 1991.

[65]Thomas, *The Ethics of Destruction: Norms and Force in International Relations*, 2. Quoting William T. Sherman, *Memoirs of General William T. Sherma*n, vol. 2 (New York: D. Appleton and Company, 1875), p.194.

[66] Richard Price, "Reversing the Gun Sights: Transnational Civil Society Targets Land Mines," *International Organization* 52, no. 3: 617.

[67] Alexander Breitegger, *Cluster Munitions and International Law* (New York: Routledge, 2012), 44, 229.

essential in both transnational advocacy against the weapon, and in the considerations of those negotiating the ban.[68]

By comparison then, cyberattacks possess some similar qualities of indiscriminateness, though less categorically than the aforementioned examples. Narrowing a cyberattack's aperture would be more technically plausible than with the destructive blast of a nuclear weapon — though likely in direct proportion to its disruptiveness. It is possible to carry out some reconnaissance on a state's digital networks, perhaps to understand whether or not certain protected targets, like a city's hospitals, rely upon certain information infrastructure. As previously articulated though, doing so is not strictly reliable, and the spread of certain cyberattack tools beyond the anticipated area of operation can further compound the problem.[69] By definition, cyberattacks target underlying infrastructure that is, in the modern age, substantially interconnected. The result is that the large-scale cyberattacks described in this study do not offer the kind of strict control that might render them in full compliance with this requirement of the *jus in bello*. Normalization of cyberattacks within warfare would be subject to this powerful critique.

Duration of conflict. An act can violate distinction not just by who it targets, but when. This premise is a helpful, additional means to determine if a particular act may run afoul of the *jus in bello.* Recall that a key principle of the *jus in bello* is the circumscription of conflict. The simplest manifestation of the principle is the 'spatial' application of the law of war, which would protect neutral states and the innocents

[68] *Ibid.*, 51.

[69] The tools that made up *Stuxnet,* for instance, appear to have inadvertently spread beyond their expected area of operation.

there-within, and non-combatants, through positive and negative obligations of soldiers.[70] A 'temporal' application of the law is, however, equally applicable. At their conclusion, whether a conflict ends in surrender, cessation, or other mutual peace, there can by definition no longer be permissible targets. The conclusion of hostilities grants all citizens non-combatant status, so time-delayed attacks, regardless of who they target, would necessarily run afoul of the principles of the *jus in bello*.

For this reason, obligations regarding the conclusion of hostilities abound, and 'traps' or other devices that might extend conflict beyond settlement of the peace fall well outside those strictures.[71] Therefore as a general matter, weapons whose effects cannot be felt, or by construction are likely to extend beyond the timescale of the conflict itself, are predisposed to violate this aspect of *in bello* distinction. They were also enshrined in the 1981 Conventional Weapons Convention emerging from the Lucerne and Lugarno Conferences, and specifically in Protocol II on Treacherous Weapons, Article 4, which highlights delayed-action devices.[72]

This prohibition is not just legally grounded, but operationalized within international practice. The emblematic case is again AP mines. Through the vivid illustration of post-conflict maiming of civilian populations and destruction of property, advocates helped create a reputation for land mines as extending the effects of conflict beyond what was lawfully permissible under the *jus in bello*. Land mines

[70] Detter, *The Law of War*, 168.

[71] Roberts and Guelff, *Documents on the Laws of War*, 517.

[72] United Nations, *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (and Protocols) (as Amended on 21 December 2001)* (Geneva: 1980), Article 4. See also: International Committee of the Red Cross (ICRC), *Conference of Government Experts on the Use of Certain Conventional Weapons* (Geneva: 1976), 51.

were thus uncontrollable in a temporal sense, indiscriminate, and unusable.[73] Nuclear weapons, against which another powerful taboo emerged over the last half-century, possess similar qualities. Both Wittner and Tannenwald note the importance of long-term radioactive fallout's civilian effects, in rendering Hiroshima and Nagasaki uninhabitable, and in civilian illness and death from subsequent nuclear tests in the 1950s, as significant in the legal and ethical opprobrium heaped on the potential for nuclear first-use.[74]

There are grounds for arguing this same premise — that the human toll caused by weapons that unduly extend the duration of hostilities is unacceptable — would apply to the tools essential to many cyberattacks. While not necessarily part of a cyberattack by definition, most successful cyberattack scenarios using present technology involve the advance installation of malicious software or hardware in anticipation of later activation. In essence, this malware is a kind of booby trap on a digital system — awaiting the right trigger to activate and cause damage. If preparations for conflict involve pre-positioning these destructive tools on systems, it would seemingly take an affirmative action to 'clear' the systems of those tools after a conflict concluded. Analogically, this obligation clearly exists under present international law. However as a strict matter, there is no such affirmative obligation, and it seems unlikely that former belligerents would allow each other access to their networks subsequent to a conflict. The result is preemptively-placed destructive mechanisms would likely abound following any conflict, and might easily

[73] Price, "Land Mines," 631-9.

[74] Tannenwald, *Nuclear Taboo*, 157; Lawrence S. Wittner, *Resisting the Bomb: A History of the World Nuclear Disarmament Movement, 1954-1970* (Stanford: Stanford University Press, 1998), 3-9.

malfunction or be unintentionally triggered to cause subsequent damage. Even more relevant and disruptive in the digital environment, fear of their persistence could cause significant economic harm, as loss of public faith in digital systems could chill e-commerce and electronic transactions generally. The tactic seems exceptionally illegal within the broader scope of a cyberattack. In fact, without judging its motives, this is one of the few areas where countries have voiced a particular concern and interest in an affirmative commitment to mitigate it.[75] So while not all cyberattacks would extend harm beyond the duration of a conflict, certain basic tools of a present-day cyberattack would almost certainly do so.

Conclusions on indiscriminateness. In targeting shared critical information infrastructure, cyberattacks run substantially afoul of the *jus in bello*. Less categorically, the popular cyberattack tool of installing malicious backdoors in critical infrastructure to enable later disruption seems highly susceptible to the same criticisms about unintentional activation to which AP mines are subject. The latter would be a prohibited method of using such a weapon, but would not necessarily designate cyberattacks writ large a prohibited means of warfare under the law.

For some, the attractiveness of a large-scale cyberattack is in the interconnection between multiple nexuses of an enemy state and society: military communications, but also utilities, banking, and government services. Such often-commercial shared information infrastructure is commonly the weakest link in the chain of military command and control, making it an attractive target. Using the case of the United States, networks that carry military or otherwise strategic

[75] Chinese foreign ministry officials have publicly called for commitments not to engage in activity to install destructive 'backdoors' into critical information infrastructure. See: PRC Submission to the 2010 U.N. Group of Governmental Experts on Information Security, *op. cit.*

communications do so incidentally relative to the overall traffic thereupon: perhaps with a ratio of one-million-to-one, or less. By disrupting the infrastructure, one disrupts all such traffic, strategic and otherwise. The result is that in only the narrow exceptional case — where the attack is surgical in approach, small in footprint, but exceptionally disruptive of sensitive systems — would the principle of distinction not cast serious doubt on the permissibility of a cyberattack.

Military strategists might argue this requirement is altogether too stringent. They might argue that in disrupting a state's core networks via a cyberattack, the attacker achieved a military aim (such as interrupting military logistics) on a network known to carry military traffic, justifying the military action to disrupt it. This logic functions only in the abstract. As a practical matter, with the multi-purpose and global networks of the present day, the requirements of distinction are likely still to be unmet.

Non-Combatant Immunity

Cyberattacks pose equally profound questions in the context of the second and even better-known variant of the principle of distinction: between combatant and non-combatant individuals, often referred to as 'non-combatant immunity.' It is, in short, the foundation of what many regard as the *jus in bello*, and is thus accorded special legal status. Coates, for instance, regards it as "not some abstract and *a priori* moral norm devised by moral theorists in the teeth of moral experience. Rather, it enshrines the moral convictions and understanding of past generations."[76] Its status is not entirely uncontroversial. Roberts regards it, at least as late as the end of the Second

[76] Coates, *The Ethics of War*, 263.

World War, as "crucial," but "also tenuous" after such gross violation therein.[77] Yet despite tribulation, "the idea that certain people are entitled to a degree of protection and that this should be codified has refused to die," conveyed clearly in the 1907 Hague Conventions on land war, and "confirmed" by the adoption of four new Geneva Conventions in 1949 "focused entirely on the protection of victims of war."[78] With such repeated reference throughout the legal, ethical, and operational writings on interstate conflict, cyberattacks clearly must comply with its provisions to be permissible under the *jus in bello*.

The essential premise of non-combatant immunity is that only targets, individuals, and objectives offering distinct military advantage are ethically appropriate subjects of belligerence. As the prior section outlined, some version of this premise goes back as far as any proto-international law covering conflict. These principles' early incarnations, and in turn their present-day form, fall into three rough categories. The first category of principles focuses on combatants themselves, levying certain obligations such as wearing uniform or bearing distinctive emblems in order to regularize combat and simplify distinction. A second category focuses on enumerating specific protected classes, such as the Peace of God movement's prohibition on injuring 'the weak' who themselves pose no threat to combatants.[79] A third category seeks a more ambitious goal: to create systemic protections or general exemptions, such as the early Greek custom that eschewed strategies targeting the

[77] Roberts, "Land Warfare: From Hague to Nuremberg," 136.

[78] *Ibid.*, 136.

[79] Geoffrey Parker, "Early Modern Europe," *ibid.*, 41.

enemy's social and economic system.[80] Each offers a distinct but relevant basis for questioning cyberattacks' usability.

Obligation to identify. To comply with the *jus in bello*, perhaps the most specific obligation of a combatant for the purposes of distinction is self-identification, or declaration – in other words, making clear the individual is not a civilian. Much of the functioning of the law of war, particularly land war, is contingent upon this basic requirement. Its history and present-day status attest to its near-universal recognition. In the chivalric code, the rule served to distinguish knights (of rarefied social class who were in turn to be held for ransom) from armed commoners (whose slaughter was generally permitted), but over hundreds of years it permuted from expedient to custom to obligation of uniformed soldiery by the time European powers organized professional standing armies.[81] The Annex to the Hague Convention IV (1907) offers the clearest articulation of combatant obligations still in general operation today: that a state's belligerents must "have a fixed distinctive emblem," must "carry arms openly," and must "conduct their operations in accordance with the laws and customs of war."[82] The requirement can be summarized as 'declaration,' but it reflects a concept already common in this study: attribution. The notion that the agents of belligerence must themselves be attributed is almost universally respected among regular forces today, and enduringly enshrined even by their 1907 codification, "apply also to militia and volunteer corps" — the irregular forces of the era.[83]

[80] Josiah Ober, "Classical Greek Times," *ibid.*, 18; *Mass and Elite in Democratic Athens: Rhetoric, Ideology, and the Power of the People* (Princeton, NJ: Princeton University Press), 53-95.

[81] Keen, *Chivalry*, 175; Stacey, "The Age of Chivalry," 36.

[82] International Conferences (The Hague), *Hague IV (1907)*, Annex, Article 1.

[83] *Ibid.*, Annex, Preamble.

If declaration is a prerequisite for a permissible belligerent, a state's cyberattackers surely must face the same requirement. Doing so is, however, practically challenging. The emblems on a cyberattacker's uniform, at a distance of several thousand miles, offer little to the victim state. In fact, the characteristics of the individual responsible for the attack are not instrumental to the law having its intended effect, since it is unlikely that undue harm would come of a person mistaken to be the operator of a cyberattack. A rough analogy might be possible, since a pilot is not only clad in uniform, but the aircraft she flies also has affixed to it certain emblems distinguishing it from civilian aircraft. The line between belligerent agent and instrumentality is, however, not perfectly clear. Pilots and planes carry emblems, as do inter-continental ballistic missiles, but artillery shells do not. As a particular matter, there is no such thing as a non-combatant artillery shell. There is no civilian object against which to distinguish. This argument is stronger than, for instance, than the supposition that only those belligerent instrumentalities carrying human persons need carry emblems (to distinguish civilians therein). The former argument further explains why unmanned instrumentalities, like drones and ballistic missiles, carry such emblems.

Rather than focus on identification of the individual, the law seemingly demands identification of the instrumentality itself — a missile or, in the case of a cyberattack, the computer of origin or data-stream that constitutes the 'delivery means.' Since computers, networks, and the human processes upon which they rely might be subject to collateral damage of retribution, *something* recognizable to the victim must distinguish a cyberattacker at the time of execution.

The current practice certainly suggests that cyberattacks have difficulty complying with the requirement. As of this writing, no acts approximating cyberattacks carried the kind of identification clearly required by international norm. The present condition is one in which states have chosen to hide behind the realities of the technology and undertake those actions more covertly — perhaps as a means to exempt them from compliance with these strictures. At issue is whether in so doing they are acting in accordance with the most reasonable or practical interpretation of this rule as it applies to cyberattacks, or whether they actually reinforce the case that the act itself may well be legally impermissible.

It is not, as a general matter, impossible for cyberattackers to distinguish themselves or their instrumentalities as belligerent; it is simply inconvenient to do so, and technologically simple to do otherwise. Conversely though, cyberattacks are not in all instrumentalities, in all technological scenarios, anonymous operations. Though much ink has been spilled decrying the permanent anonymity of the cyberattacker, and the impossibility of assigning that individual to any one state, this is a period-specific prognosis. Methods of obfuscation will continue to be available, just as covert commandos and apparently merchant vessels laden with explosive remain available to conventional militaries. Not atypically, the question of compliance with the law has some inverse relationship to efficacy, surprise, and deniability. The most relevant legal question is whether the obfuscation common today is a derogation of either the affirmative obligation to identify, or the negative one against perfidy.[84]

[84] Affirmations of the prohibition on perfidy include Article 16 of the *Lieber Code*; Article 37 of the 1977 *Geneva Protocol*; Article 17 of the 1954 *Hague Convention for the Protection of Cultural Property*; and Protocol II of the 1980 *U.N. Convention on Prohibitions or Restrictions on the Use of Certain Chemical Weapons*.

Noting this concern, a few commentators have implied a solution of ensuring every 'packet' of data be authoritatively identified with a 'national marker.'[85] That solution is legalistically attractive but, at least given today's technology, rather impractical.[86] This study will not dwell on the technical design of a regime that would suffice, particularly given the numerous and changing vectors for executing a cyberattack. Regardless, the difficulty of solution does not obviate the clarity of requirement, and the simplicity of dodging it does not from a legal (or ethical) standpoint excuse attackers making such a choice.

When protection of innocents demands identification of belligerents, states make certain concessions of covertness. Cyberattacks are not legally questionable because they are so often anonymous. Rather, interstate actors carrying them out are legally suspect in leveraging technology to obfuscate their responsibility. So long as this practice of de-identification remains custom, cyberattacks will as a matter of law carry the stigma associated with violating this most basic provision of the *jus in bello*.

The undefended. Cyberattacks also raise substantial questions about the feasibility of meaningful defense, another important and longstanding criterion in the *jus in bello*. Some of the earliest codifications of the law, including 1874 Declaration of Brussels, included the notion that "fortified places are alone liable to be besieged.

[85] See, for example, John E. Savage and Melissa E. Hathaway, "Stewardship of Cyberspace: Duties for Internet Service Providers," in *Cyber Dialogue: What is Stewardship in Cyberspace?* (University of Toronto, Munk School of Global Affairs: University of Toronto, 2011). John E. Savage and Les Bloom, "On Cyber Peace," in *Reports of the Cyber Statecraft Initiative* (Washington: The Atlantic Council, 2011).

[86] It may also be self-defeating. If a 'network signature' were to identify military origin and likely the country thereof, as befits distinct emblems, doing so may well compromise the efficacy of the attack itself. It may be tantamount not to wearing a patch on a battlefield, but to revealing the location of combatants awaiting a surprise attack. The practical (i.e. political) opposition to complying with this norm is likely to be profound.

Open towns, agglomerations of dwellings, villages, which are not defended can neither be attacked nor bombarded."[87] Similar protections against the undefended can be found in Hague II and Protocol I.[88] As a matter of land warfare this requirement is straightforward, but the principle underlying it — the common thread throughout these laws — excludes undefended populations from the equivalent of siege.

This principle has factored into recent considerations on nuclear weapons, with some instructive points for cyberattacks. For instance, one of the earliest sources of public panic of nuclear weapons was the inability of states to defend against them, a premise that carries more relevance to cyberattacks than has been given credit. Memorialized by Stanley Baldwin's famous adage, 'the bomber will always get through,' and further by the advent of supersonic delivery mechanisms like the ballistic missile, truly reliable defense against a nuclear weapon was for much of their history a matter of strict deterrence.[89] Neither Reagan's pursuit of the Strategic Defense Initiative nor modern-day anti-ballistic missile interceptors have permanently eroded that anxiety. With an arsenal of sufficient size, nuclear defense absent deterrence, dissuasion, or counterattack capability remains a largely hollow concept.

Cyberattacks also raise substantial, though not necessarily permanent challenges of defense. As a technical matter, a state can defend against a cyberattack through effective cybersecurity practices. For every vulnerability in a digital system, there exists a means to secure it by 'patching' software, closing network connections,

[87] "Project of an International Declaration Concerning the Laws and Customs of War," (Brussels), Article 15-17.

[88] International Conferences (The Hague), *Hague II (1899)*, Article 25.

[89] For more systematic analysis, see: Giulio Douhet, *Command of the Air*, trans. Dino Ferrari (New York: Coward-McCann, 1942).

or reengineering how the affected device communicates with other devices. In this respect, falling victim to a major cyberattack can be attributed in part to poor planning and defense, rather than the awesome existential power of the destructive capability. Concerns about the impossibility of effective cyber-defense and associated suggestions about illegality on those grounds seem misplaced and more akin to the bomber panic accompanying the advent of air war.[90]

The analogy to nuclear defense is, however, more useful than might seem, and there is a reasonable analogy that modern, interconnected societies might form an undefended enclave of the sort protected by the *jus in bello*. Cyberattacks target a persistent reality about digital networks: that to be globally and technologically interoperable, they remain pervasively insecure. This is a vulnerability that as a general matter is shared by all countries that use the technology. Much as nuclear defense is *technically* possible with a perfectly functioning anti-ballistic missile shield and air defenses, perfect cybersecurity is also possible but impractical. In their present constitution, networks are inherently too insecure to be entirely impregnable to cyberattack; to make them so would be to upend much of their value to economies, societies, and even militaries. This sunk cost in interoperable hardware, software, and the underlying protocols of the Internet upon which they run suggest this permeability will remain the case for the near future. Accepting, as many technical experts do, that networks will in aggregate and for the foreseeable future remain utterly insecure,

[90] See: Pape Jr., *Bombing to Win*, 60-1. The concept is best memorialized in history by Stanley Baldwin in his 1932 speech to the British Parliament claiming, “the bomber will always get through” — itself reflecting the strategic philosophy of Giulio Douhet.

there seems cause for similar public anxiety.[91] Accepting the present state of interoperable technology, then, cyberattacks seem incommensurate with protections for the undefended, providing further potential evidence they violate the *jus in bello*.

Other protected classes. Particularly strong norms and explicit laws reflecting them also protect certain classes of target from attack in unexceptional circumstances in conflict. These classes are known well beyond those versed in international law: clear rules bar attacks on hospitals, for instance.[92] The same holds true for churches, shrines, schools, museums, national monuments, and historical and cultural sites not otherwise related to or co-opted by the opposing force to advance its military aims.[93] This relatively straightforward distinction is designed to exempt certain 'helpless' targets either incapable of rendering harm to an attacker, or the targeting of which would cause undue suffering for another protected subclass (e.g. the wounded, clergy, or children).

Considering only this first, most well-recognized protected class, cyberattacks do not *inherently* target any one intentionally or disproportionately. Whether or not they do is a function of the configuration of any particular state and its infrastructure. As previously discussed, knowing how a cyberattack might affect members of a protected class (i.e. assessing collateral damage) may be difficult given the complexity of interconnection, causing some reason or pause. In this context

[91] James Kaplan, Shantnu Sharma, and Allen Weinberg, "Meeting the Cybersecurity Challenge," *McKinsey Quarterly* (2011): 3.

[92] See, e.g., International Committee of the Red Cross (ICRC), *Geneva Convention IV (1949)*, Articles 14-22.

[93] With respect to objects of cultural value, for example, see: Howard M. Hensel, "The Protection of Cultural Objects During Armed Conflicts," in *The Law of Armed Conflict: Constraints on the Contemporary Use of Military Force*, ed. Howard M. Hensel (Hampshire: Ashgate, 2006).

however, ethicists like Coates have argued compellingly for non-combatant immunity as a strategic (vice tactical) consideration, and that moral adjudication of such acts is more useful as a matter of intention (vice consequence).[94] Satisfaction of due diligence must factor into evaluation of the act, but aiming at a lawful target to achieve a military objective, incidentally yet unavoidably interfering with a protected class, is not grounds for categorical rejection of the aim. Here also, any legal suspicion would be appropriately directed at the state choosing the manner of cyberattack, not the choice to use the means itself.

More recent treaty law has extended the categories of protected classes beyond these obviously 'helpless' targets, suggesting a more fruitful line of inquiry in the case of cyberattacks. For instance, the 1977 Geneva Protocol I extends protections to "works and installations containing dangerous forces" — including dams and nuclear plants.[95] The pervasive interconnection of these facilities to Internet infrastructure suggests the latter may qualify for similar protections, if its disruption were reliably known to cause failure of their safeties. Somewhat less compelling but relevant in the long-term might also be the Protocol's protections of "objects indispensable to the survival of the civilian population," which aims to safeguard food supply and distribution, but which in many countries is increasingly reliant on the reliable operation of digital systems.[96] As civilian practice develops, even these more-specific applications of the principle of distinction may have bearing on the usability of cyberattacks.

[94] Coates, *The Ethics of War*, 259.

[95] International Committee of the Red Cross (ICRC), *Additional Protocol I (1977)*, Article 56.

[96] *Ibid.*, Article 54.

Systematic protections. A related and interesting question might be raised about whether those engaged in neutral commerce constitute a protected class. Protection or respect for civilian property is a recurring reference throughout the *jus in bello* in law and practice. Certainly, maritime law affords such commercial agents protections, pursuant to certain requirements.[97] Provisions of this sort would fall at the intersection of those protecting certain defenseless classes, and those aiming to insulate the operations of civilian life from the conduct of organized war. The modern premise is simple and consistent with the overall premise of non-combatant immunity described herein: that in selecting targets for attack, those with no direct military value are theoretically immune from attack.

Provisions like these remain far more controversial, and generally less observed, than those protecting specific classes. Spectacular violations of such 'systematic protections' have taken place in most large-scale conflicts. At one end of the spectrum then would be the urban bombing campaigns of World War II, noted for exceptionally high casualty count and explicitly intended to bring about a weakening of civilian will in victim states.[98] Nonetheless, these systematic protections persist in various aspects of the *jus in bello*. From an ethical standpoint, the operation of these norms is essential, for instance, to avoid a "dehumanized view of war according to which war is seen as an industrial and mechanical process in which the distinction

[97] See, most recently: United Nations General Assembly, *Convention on the Law of the Sea* (Montego Bay, Jamaica: United Nations, 1982), Art. 3(A). For a general overview, see: Edward Elliott, "The Freedom of Neutral Commerce," *California Law Review* 3, no. 4 (1915); J. Ashley Roach, "The Law of Naval Warfare at the Turn of the Two Centuries," *American Journal of International Law* 94 (2000): 107.

[98] Pape Jr., *Bombing to Win*, 318-26.

between the human and the material element is systemically suppressed."[99] Therefore, at the other end of the spectrum, one might contrast the rules of engagement given to U.S. soldiers during Operation Desert Storm, which called on them not only to "avoid harming civilians unless necessary to save U.S. lives," but to "avoid harming civilian property…do not attack traditional civilian objects such as houses…treat all civilians and their property with respect," and even not to requisition civilian property "without giving a receipt."[100] That document summed up the principles of discrimination clearly: to "Fight only combatants. Attack only military targets. Spare civilian persons and objects."[101] Considering this state of the art, civilian property and trade, when unrelated to conflict in question, is a proscribed target (either strictly, as a protected class, or more generally, as part of a broader systematic protections).

The status of the law providing systematic protections to commercial objects and interests distinct from the war effort is generally sound, and while adherence may be not universal, the underlying premise is worth considering given the relevance to cyberattacks. It is incontrovertible that a growing portion of the global economy is directly attributable to the Internet, directly accounting for 3.4% of GDP in a survey of both mature and fastest-growing economies, and 21% of GDP growth in those countries over the last five years.[102] In the United Kingdom, it directly accounts for

[99] Coates, *The Ethics of War*, 220.

[100] United States Army, *Operational Law Handbook*, ed. International & Operational Law Department (Charlottesville, VA: Judge Advocate General's School, 1995). Reproduced in Roberts and Guelff, *Documents on the Laws of War*, 562-3.

[101] United States Army, *Operational Law Handbook*, 8-8.

[102] McKinsey Global Institute, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity* (New York: McKinsey & Company, 2011), iv.

over 5% of GDP.[103] Far more importantly though, the Internet's reach is far greater than just the information sector; over 75% of the Internet's economic impact arises from traditional (non-technology) industries, and a majority of participants in OECD countries' economies rely upon the Internet and its infrastructure for some aspect of their livelihood.[104] The same is true for basic government functions, with countries like Estonia leading the way in provision of all civic services including taxation, benefits, and licensing taking place online. In the milieu of popular cybersecurity panic, it is all too easy to ignore that the percentage of global Internet traffic directed at peaceful commerce and communication is even greater than the percentage of global land put to civilian purposes. For that reason then, a fair analogy can be drawn to the notion of 'innocent passage' and 'neutral commerce' — that digital systems and traffic that do not constitute a legitimate military aim and are owed protections as civilian objects. That premise is not, of course, guaranteed by international law in the direct manner that seaborne commerce enjoys. Nonetheless, considering the potential for wide-scale commercial harm, particularly given the shared use of infrastructure between military and civilian systems, this protection seems plausible.

Conclusions Applying the **Jus in Bello**

Using the guide of other prohibited means of warfare, cyberattacks raise many of the same legal (and ethical) issues that helped inform those specific bans. In descending order of significance, cyberattacks are almost certainly indiscriminate; they evade obligations to identify belligerents; run high risk of implicating neutral

[103] *Ibid.*, 40.

[104] *Ibid.*, 22; Organisation for Economic Cooperation and Development, "Measuring the Internet Economy," in *OECD Digital Economy Papers* (Paris: OECD Publishing, 2013), 51; "The Impact of Internet in OECD Countries," in *OECD Digital Economy Papers* (Paris: OECD Publishing, 2012), 5.

third parties; and exploit common vulnerabilities that are difficult to defend against. To the extent that certain qualities serve as the basis for rending them 'unusable' to states concerned with their standing in international society, these are the strongest and most relevant. Additionally, should cyberattack tools create a long-term a liability for the security of networks and faith therein, there may be further basis to develop a *lex specialis* within the *jus in bello* restricting their use.

If states obscure their cyberattack activities, they may well do so to avoid confronting the hard questions the *jus in bello* presents. There seems ample basis to regard cyberattacks as incommensurate with the key principles of the law*,* at least as much if not more than weapons subject to specific bans, such as land mines or cluster munitions.

The gulf between analysis and state restraint is determined by how widely this interpretation of the law is shared, recognized, and most powerfully, further codified into *lex specialis* pertaining to cyberattacks. Historically, patent incompatibility with the *jus in bello* has been a prerequisite for a weapon becoming 'unusable.' This criterion is necessary, but insufficient to restrain states reliably. The *jus in bello* does not have the same remedial procedures as the *jus ad bellum.* Instead, one might consider the remedial *jus in bello* to be the formation and maintenance of international norms. Punishment for transgressions comes not from a formal legal regime, but from overlapping influences of international opprobrium, military intervention, and in the most extreme cases, individual criminal responsibility for 'grave breaches' of the law.[105] Combined, these are powerful forces of restraint on state behavior. As the

[105] "Grave breaches" are defined variously by the four Geneva Conventions of 1949 and Additional Protocols of 1977: International Committee of the Red Cross (ICRC), *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva*

last two chapters have shown, existing international law clearly renders cyberattacks outside the realm of peaceful and just interstate conduct in peace as well as in war.

Convention) (Geneva: 1949), Article 50; *Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention)* (Geneva: 1949), Article 51; *Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention)* (Geneva: 1949), Article 130; *Geneva Convention IV (1949)*, Article 147; *Additional Protocol I (1977)*, Articles 11, 85.

Conclusion:

What Will Restrain Cyberattacks?

Every weapon of war is subject to at least some form of restraint, yet none are under full and irrevocable control. As this study has shown, cyberattacks are no exception. States will seek to deter one another with them, but they do so with little prospect of imposing the sort of restraint that prevented a nuclear catastrophe during the Cold War. In the absence of recognizable deterrence, states are turning to an alternative: competing strategies of structural deterrence hoping to shape the international custom over the permissible response to a cyberattack. As they do, those states rely on international law tilting in their favor, but thus far have offered only sweeping claims and little underlying analysis to support their respective cases.

The latter parts of this study critically evaluated the claims upon which these deterrence strategies are based, conducting the legal analysis that has been heretofore lacking both in state policy and the academic literature. Its findings were overwhelming. Cyberattacks are certainly subject to the letter and regime of international law restraining the recourse to force, as well as the laws setting the boundaries of 'permissible' and 'humane' conflict. Under analysis, they violate both.

All states are bound by the U.N. Charter regime, but its real restraining influence varies state-to-state. For some states, illegality itself may suffice. For others, the potential a victim might be granted the right to use retributive force — for which there is clearly legal basis — may create strong disincentive. Still others, though, will respond only to custom, and it is clear that such a custom of states taking strong, self-defensive action to a cyberattack has not taken hold. Herein lies the distinction between the letter of the law and imposition of a rule in international relations — the basis for that custom exists, but its operation depends on agency.

Separately, many states — particularly given historical evidence from the 1990s — might hold back from a cyberattack for fear it violates the *jus in bello.* This canon of law has a humanitarian basis, but also a crucial reputational function. While it lacks the remedial regime of the *jus ad bellum*, the stakes are in some respects higher. Some states may already be reflecting this view in their preference for covert deployment of cyberattack tools, refusing to admit their involvement in attacks so successful, deterrence might suggest great power in doing so. Therein again lies the legal basis, and potential state practice, for cyberattacks to remain an exceptional weapon subject to considerable restraining influence.

These restraining forces are up against a considerable draw, which may be more significant for some states than others. Which specific countries might specifically observe or be resistant such restraint, based on their history and politics, could form an important subject for further study. It may be particularly notable given that cyberattack capabilities do not necessarily map onto traditional notions of military advantage. Cyberattacks might, given uneven restraint, have the ability to reconfigure distributions of power in the international system — especially since their disruptive potential is unlikely to help incumbent powers preserve their status. Countries can buy their way into the club of those with some cyberattack capabilities, but they cannot with the same ease bring down the technological dependence that renders them vulnerable. Thus the archetypical state with the most to gain from a cyberattack capability is one with little technological dependence itself, but a large military and an adversary whose economy and armed forces are highly dependent on modern computing. This is notable asymmetry that some states are bound to exploit, if unrestrained. These circumstances form the basis for the need articulated just prior: to consider the potential for a specific norm prohibiting cyberattacks in international practice.

A Norm Barring Cyberattacks?

Even stronger forces within international relations might act on states to restrain the use of cyberattacks, but extended study of them is somewhat premature. Consider, for instance, the outcome of the structural deterrence process described in Chapter 2. That outcome is not necessarily a collective restraint; indeed, the success of the West's structural deterrence strategy could see the regularization of cyberattacks in war. What structural deterrence does invite, however, is the habituation of state conduct in the event of a cyberattack. It communicates expectations about how cyberattacks are to be understood and reacted to, and is aimed at sharing that expectation as broadly as possible. The next step in structural deterrence, then, is the formation of a norm — specifically, a norm governing state response (and eventually recourse) to a cyberattack.

Likewise, there are stronger grounds for the *jus ad bellum* to restrain cyberattacks than many states let on in their public statements today — but that fact runs the risk of becoming dead letter in the absence of consensus and custom. Even among international law's most ardent defenders, it is "fundamentally misguided to attribute to [it] an exclusive role in controlling state behavior."[1] Here again, the regimes of international relations tilt toward restraint of cyberattacks, but demand agents within the international system to make it so. Without a tradition or norm of

[1] Gray, *International Law and the Use of Force*, 4.

nonuse built atop this solid legal foundation, it is unfair to assume that restraint will necessarily take hold in the defense policies of most states.

Finally cyberattacks, like many explicitly proscribed means and methods of war, seem potentially disproportionate and almost certainly indiscriminate. They may, as a result, earn an international status of being 'unusable.' Incompatibility with existing law is necessary but not sufficient for a norm against cyberattacks to take hold. Restraint in warfare is far from a strictly legal matter. Nearly every scholar commenting on the *jus in bello*, for instance, notes at some point the endless pattern of advances in military technology followed by outcry and moral disdain. Yet only a small number of weapons that cause legal or ethical anxiety end up earning the category of 'unusable.' Thus, even legal analysis as conclusive as in the preceding chapters forms an incomplete picture of whether a prohibitive norm might take hold. After all, in most cases, outcry over military innovation is quickly followed by regularization — not prohibition. The harshest critics of the *jus in bello* regard its provisions as either ethically bankrupt for baldly reflecting power relations, or dysfunctional for only limiting military instruments of minor impact. How then, one might ask, can it serve as the basis for a norm against cyberattacks?

Reading in concert the three preceding chapters, it is clear that for the purposes of restraining cyberattacks, the normative whole may be greater than the sum of its rationalist and regulative parts. There may not be the evidence to trace a norm proscribing cyberattacks, but this analysis shows there may well be a clear path for one to take shape. The conclusions of the prior two chapters provide at the very least a basis for a norm proscribing cyberattacks.

The development and operation of such a norm also does not depend on full restraint or categorical non-use. Take, for example, the nuclear taboo or the chemical weapons ban. Both technologies have been used, and each instance only strengthened opprobrium on the user and the norm against their non-use, particularly in the latter case. Thus, as Kratochwil and Ruggie note, even were there an established and widely recognized norm, "[t]he violation of a norm does not mean it no longer exists or that it ceases to have an impact on social behavior; what matters is how the violation is interpreted by others and what subsequent practices serve to rehabilitate or undercut the norm."[2] When they are used, communicative dynamics of rationale, justification, pleas for understanding, and admissions of guilt, are all "communicative dynamics" which can "tell us far more about how robust a regime is than overt behavior alone."[3]

The other common criticism of the formation and value of a norm built atop the laws of war is that it would limit the wrong objects and "[refrain] from imposing restraints on the most dangerous forms of armed violence."[4] It is hard to argue that the nuclear taboo does not hold at bay a dangerous form of violence, and so, too, with chemical weapons. More comprehensive evidence also comes from detailed studies of the formation of specific norms, such as Price's on chemical weapons and land mines and Tannenwald's on the "nuclear taboo."[5] These studies effectively undercut the argument that the operation of these norms is explainable strictly as a function of power-based interests that would exclude only asymmetric tools. Thus, leaving aside

[2] Friedrich Kratochwil and John Gerard Ruggie, "International Organization: A State of the Art on the Art of the State," *International Organization* 40, no. 4 (1986).

[3] *Ibid.*, 768.

[4] Cassese, *International Law*, 399.

[5] Price, "Land Mines."; Richard M. Price, *The Chemical Weapons Taboo* (Ithaca: Cornell University Press, 1997); Tannenwald, *Nuclear Taboo*; Richard Price and Nina Tannenwald, "Norms and Deterrence: The Nuclear and Chemical Weapons Taboos," in *The Culture of National Security*, ed. Peter Katzenstein (New York: Columbia University Press, 1996).

purely ethical issues parenthetical to this study (such as whether the *jus in bello* sufficiently addresses cases of civil war and genocide), the demonstrated ability of such norms to meaningfully limit states' recourse to otherwise effective weapons illustrates the practical and normative importance of the enterprise.

The prior chapters have found that not only are several such norms highly applicable to cyberattacks, but those same critiques also apply to a number of specific weapons against which a norm has taken hold. Upon this basis, the balance of the section considers the pathways that such a specific norm against cyberattacks, derivative of the *jus ad bellum* and *jus in bello*, might take to form.

Pathways to the norm

With a solid foundation, it is possible to posit a number of ways that the norm might come into practical effect. The most powerful 'normative pathway' would be a systemic one, drawing coherence between a hypothetical, counter-cyberattack norm and existing prohibitive international norms. The arguments of the preceding chapters have provided the basis for such an argument. As a practical matter, that pathway would be based on numerous, powerful governments building consensus for the clear coherence between a norm against cyberattacks and existing norms governing recourse to and use of force.[6] Yet, like the legal analysis itself, coherence does not yield a robust norm and, rather, is a passive pathway that lends legitimacy to more active advocacy. To be fully operationalized, those advocating for a norm

[6] See: Ann Florini, "The Evolution of International Norms," *International Studies Quarterly* 40 (1996); David Lumsdaine, *Moral Vision in International Politics* (Princeton, NJ: Princeton University Press, 1993); Neta Crawford, "Decolonization as an Internatoinal Norm," in *Emerging Norms of Justified Intervention*, ed. Laura Reed and Carl Kaysen (Cambridge, MA: American Academy of Sciences, 1993).

would need to engage in a process that Price refers to as 'grafting.'[7] In this approach, norm entrepreneurs appropriate the genealogical heritage of associated norms in the germination of a new one. As this and prior chapters have shown, it would be straightforward to graft a norm against cyberattacks onto the *jus ad bellum* and *jus in bello,* giving this pathway notably strong potential.

But can a norm proscribing cyberattacks take hold given the potential utility of cyberattacks, and in the absence of a strong civil society that was so instrumental in the ban on land mines? One does not have to accept an ethical or humanitarian imperative to limit cyberattacks to see a future for a norm proscribing them. A confluence of immediate state interest, and preponderant power, could well still regulate cyberattacks. Consider that, today, only a handful of states are exceptionally vulnerable to a cyberattack. They are exclusively developed economies with considerable (and collectively preeminent) militaries. Those aspiring to such status are, at the pace of their rise, also growing in vulnerability. The result is that the United States, Australia, Canada, Japan, South Korea, and most of Western Europe would all be the greatest beneficiaries of a system in which large-scale cyberattacks were prohibited in wartime and outside of it. Obliquely, this may be the underpinning of the Western structural deterrence posture outlined in Chapter 2 — but for the reasons outlined in that chapter, that policy is highly contested, and it is on its own no guarantee of legitimacy.

Some commentators (and in particular neorealists) would argue that this vulnerability provides precisely the opportunity for aspiring powers to exploit it, either directly by attacking or indirectly by creating an environment accepting of its

[7] Price, "Land Mines," 617.

use. Yet, if anything, aspirants like China and a re-emerging Russia are seeking *greater* overt regulation of cyberattacks than their Western counterparts. That preference might have strategic origins, but its outcome is the same. There is surprising, if as yet unrealized, alignment in efforts to normatively prohibit large-scale cyberattacks.

Adding to this coherence pathway, other, systemic sources of norm development could play an important role, including identity, reputation, and hegemonic influence. The former sources are generally straightforward: embedded within norms prohibiting certain methods of warfare are constitutive notions of humanitarianism and civility, with origins both expedient and existential. The community judging comportment with those norms also develops notions of collective identity that in turn create attraction to the norm. This, in turn, can create a feedback effect, where the germination of a norm among a particular community can grow the community of adherents and, in turn, strengthen the norm itself. Given the well-documented public anxiety of government officials about their cybersecurity vulnerabilities, it is easy to imagine the appeal of a community defined by reducing that threat and marginalizing those who would exploit it.

This systemic pathway is particularly powerful when one considers that the structural deterrence efforts documented in Chapter 2 inevitably have such a normative effect — while seeking to legitimize retributive force to a cyberattack, they simultaneously aim to delegitimize the act itself. The countries advocating for such a position, particularly the United States and its allies, could plausibly be in a position to impose such a hegemonic consensus for this view. The effect, which strong evidence suggests is already taking place, is a sort of 'forced grafting,' where all three of these systemic pathways to norm formation combine to create a particularly fertile ground for a norm against cyberattacks to take root.

This international discourse also does not occur in a vacuum, nor it is even specific to cyberattacks. There may be an additive influence of 'societal diffusion' — the interface between domestic and international norms — in such a proscription taking hold. Consider, for instance, that such a norm would resonate with emerging domestic norms against disruptive cyberattack activity. On the general topic, scholars like Lumsdaine, Cortell, Davis, and on more specific topics, Crawford (on decolonization), and Klotz (on apartheid) have all shown the influence of this force in other areas.[8] With regard to cyberattacks, most states with even rudimentary digital economies possess some form of anti-cybercrime law outlawing disruption of digital systems. Prosecutorial imperative also drove the need for an international instrument, the *Budapest Convention on Cybercrime*, to harmonize those laws. The coherence of the subject matter is difficult to ignore; here a domestic norm, codified into domestic law, has diffused into an international norm and ultimately positive international law. *Budapest* does not itself constitute the kind of norm under discussion here, but it is notable as a pathway and source of influence.

A final pathway, less compelling but nevertheless worth noting given substantial policy attention paid to it, would leverage the bureaucratic power of entrepreneurs interested in the issue. The most obvious example would be the interest of various United Nations figures, notably the Secretary-General of the International

[8] See: Lumsdaine, *Moral Vision in International Politics*; Andrew Cortell and James Davis, "How Do International Institutions Matter? The Domestic Impact of International Rules and Norms," *International Studies Quarterly* 40 (1996); Crawford, "Decolonization as an Internatoinal Norm."; Audie Klotz, *Norms and International Relations: The Struggle against Apartheid* (Ithaca: Cornell University Press, 1995).

Telecommunications Union, placing the question on agendas for state dialogue and research programs within that system.[9] There is also evidence undercutting the influence of this pathway; despite Russian-sponsored resolutions with a clear aim at 'cyber-disarmament' appearing on the agenda for over a decade, there are few indications that discourse has shifted as a result.[10] This fact suggests that the influence of individuals such as ITU Secretary-General Touré is a function of, but also limited by, their bureaucratic ability to force otherwise recalcitrant states to entertain dialogue on the issue. It seems, in the present case of cyberattacks, to bode poorly for the influence of the kind of personal advocacy effects emphasized in other contexts by Nadelmann and McElroy.[11]

It is likely that coherence would be the strongest pathway for such a norm to develop given present practice, but it is far too early to rule any out. The efforts of government leaders, transnational civil society, issue advocates, and multilateral institutions in advocating for such this norm are likely to be enduring and rich subjects for study. In an analysis so dependent on agency, the mere basis for a norm to take hold is itself a powerful conclusion — not only the strongest presently available, but also one that cannot be claimed for the vast majority of novel weapons.

[9] Agence France-Presse, "U.N. Chief Calls for Treaty to Prevent Cyber War," 30 Jan 2010. Touré's efforts are also evident in the efforts of U.N. programs like the United Nations Institute for Disarmament Research (UNIDIR) on the issue.

[10] *Op cit.* p. 80 footnote 11.

[11] Ethan Nadelmann, "Global Prohibition Regimes: The Evolution of Norms in International Society," *International Organization* 44 (1990); Robert McElroy, *Morality and American Foreign Policy* (Princeton, NJ: Princeton University Press, 1992).

Challenges and Opportunities in the Study of Cyberattacks

An enduring challenge in the study of cyberattacks is framing meaningful analysis on a subject so fast-moving. International relations' most prized insights earn that status as a function of their durability, and many of its deepest analyses have been conducted with the luxury of decades of hindsight. Afflicted by proximity, the primary challenge in the case of studying cyberattacks is ensuring that it is not robbed of the quality of durability. There are also real limits to what scholarship on a topic as contemporary as cyberattacks can achieve in the present day without greater hindsight and state practice from which to draw. Here, the comparison with nuclear weapons is instructive. There remains insufficient history of state decision-making to write a historical account like Bundy's, a normative study like Tannenwald's, or even a strategic analysis of the sort produced by RAND in the 1960s.

Nonetheless, this study attempted to meet that challenge in several ways. The first was to avoid fixation on any single case study. In the absence of much international custom of cyberattacks, and the lack of a 'full demonstration' of capabilities of the sort witnessed with nuclear technology at Hiroshima, such instances may actually prove of little explanatory value. While there may be a tendency in the present and future scholarship to fix predictions about state practice around single case studies, doing so runs similar risks to predicting nuclear practice in the Cold War from the vantage of 1951. With that perspective, as Tannenwald points out, one could just as easily have assumed a nuclear strike would become a commonplace tactic for any nation advanced enough to possess them.[12] Yet by 1970, that future failed to materialize. Analysis on this topic cannot be frozen in time, and

[12] Tannenwald, *Nuclear Taboo*, 181-9.

in the absence of a repeated and specific precedent, international law and the context of other advances in weaponry remain the strongest predictors of the shape of things to come.

In the same vein, a privilege of a study this length is to examine a range of competing explanations and frameworks, rather than focus narrowly on — and potentially overemphasize fit with — any single regime or force in international politics. With very few exceptions, the last few years' scholarly literature on the issue of cyberattacks remains in disciplinary silos. This study also worked to connect those analyses, bringing disparate strains of thought together in an integrative project for which the discipline of international relations is uniquely well-suited to support. As scholarship on the topic matures, it will continue to benefit from work on other fast-developing areas at the intersection of international law, emerging state custom, and advances in technology. Among these, the lessons of space law, the law of the sea, and the evolution of conventional arms control regimes seem natural candidates for later cross-pollination.

The meaningful contemporary study of cyberattacks in international relations is still far from exhausted. For instance, ripe for analysis and heretofore largely neglected, one could examine in-depth the philosophical and ethical implications of cyberattacks. These two projects are indeed related: this study accepted a certain general perspective on the issue, but did not attempt a systematic philosophical inquiry into the subject. The field would benefit from such an analysis — a continuation of the sort of work undertaken generally by scholars like Rodin and specifically by Lucas in the context of cyberattacks.[13]

Likewise, the discipline of international security is increasingly engaging with new questions, both narrowing its focus to consider low-intensity conflict, and broadening it to examine concepts of human security.[14] With this in mind, a meaningful line of inquiry might come from applying those insights to smaller-scale cyber incidents, specifically those not rising to the level of damage considered by this study. To the former, do the Syrian Electronic Army or Anonymous collectives suggest there such thing as a *cyber* insurgency? How would counter-insurgency operations regard and internalize this concept? The effects of cyberattacks on livelihood or access to basic goods, and even the evolving concept of a 'right to Internet access,' could form another line of analysis.[15]

Relatedly, a dedicated study of the human rights implications of cyberattacks would be meaningful and timely, as digital disruptions of civil society protests in Iran, Syria, and elsewhere are of great importance to popular movements therein. As a legal and precedential matter, those disruptions involve deprivation of freedoms guaranteed by the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights, which might be rewarding to further explore. Finally, scholars of comparative government may find rich source materials in the ever-

[13] David Rodin, *War & Self-Defense*, Reprint ed. (Oxford: Oxford University Press, 2010 (first published 2002)); Lucas, "Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets."

[14] David Kilcullen, "Counter-Insurgency *Redux*," *Survival* 48, no. 4 (2006); S. Neil MacFarlane and Yuen Foong Khong, *Human Security and the UN: A Critical History* (Indianapolis, IN: Indiana University Press, 2006).

[15] Frank La Rue, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression," (Geneva: United Nations Human Rights Council, 2011).

growing number of national cybersecurity strategies — largely without international policy treatments, but important for the overall shape of cybersecurity issues to come.[16] These are but a few of the many directions in which future scholarship might head, and for which this study might serve as a preliminary guide.

Conclusion

Some of the most durable conclusions of this study are also important validation of both regimes of international law and the explanatory power of international relations more generally. Even when confronted with a practice as novel and complex as cyberattacks, the phenomenon can still be understood within the existing regimes and customs of international relations. This is, after all, not the first time the field has been influenced by changes in technology. Indeed, innovations in war have long been a crucial force challenging law and reconfiguring power dynamics. In a period of immense geopolitical change, though, the need for context in how states might use these tools remains constant. Cyberattacks are an emblematic case: they are a practice best understood within and not distinct from contemporary international relations.

The discipline, and particularly international security within it, is perhaps underappreciated for its ability to evolve with and be driven forward by such change. Since Westphalia, the story of the international system has been one of external and internal pressure, evolution, and dynamism. Technology is one of many important factors that can accelerate those changes — whether in distributions of power or configurations of politics with which states identify. New weaponry can be an abrupt

[16] *Op cit.* p. 41 footnote 88.

marshal of change. From the longbow at Agincourt to the atomic bomb at Hiroshima, coercive novelties impose a punctuated equilibrium on the evolution of international relations politics. It is straightforward that the states' accumulation of cyberattack capabilities will have some clear effects on their international relations. The tectonic question for international security more broadly is whether their use is regular or rare. Some policy-focused studies have begun to posit and even adopt the former as a starting premise, but that conclusion is premature. After all, cyberattack capabilities are available to members of various unstable dyads, like India and Pakistan, yet their use is hardly widespread.

Precedent is a powerful template. A select category of weapons are today 'unusable,' even when militarily advantageous — a practice variously imposed by political leadership and armed forces themselves. Nuclear weapons are the most notable example. Other means, like chemical weapons and AP mines, awakened a collective conscience only after use on a certain scale. In rare instances, the international community has even united to preclude weapons that have not yet materialized, such as Rule 79 of the 1980 Conventional Weapons Convention outlawing projectiles of undetectable fragments — a whole genre of feared but not developed weapons.[17]

One conclusion of this study is that, taken together, the basis for such a norm clearly exists. Evidence even points to a norm with a promising legal foundation and more than one discernable pathway to take shape. While I argue that coherence is the most powerful factor at play, there is no doubt that numerous other factors will

[17] Price, *Chemical Weapons*, 67-8, 167-9; "Protocol on Non-Detectable Fragments (Protocol I)," in *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions, and Other Documents*, ed. Dietrich Schindler and Jiří Toman (Geneva: Henry Dunant Institute, M. Nijhoff).

influence the potential formation of such a norm. If it does take hold, it will likely proceed on what Price called a “haphazard combination” of normative pathways, shaped equally importantly by the “contingencies of history.”[18]

A norm against cyberattacks is a high standard, but one that has been achieved in the context of chemical weapons and anti-personnel landmines. Restraint will not be automatic. In fact, the paths on which some key states have set themselves might undermine broader efforts at restraint in the near-term. Those states that possess a foreign policy aimed at reducing cyberattacks work across one another’s, and at times even their own purposes. For instance, the one side’s efforts at structural deterrence serve only its short-term interests by normalizing cyberattacks within conventional conflict, since to pursue a more far-reaching norm against cyberattacks would be to concede the other bloc’s core arguments about a special status for the capability. For the West, short-term defense imperative clouds long-term normative progress, while for the East, decades of investment in a groundless effort for new international law have invited politics to stand athwart consensus on normative principle.

Many weapons, once used, have proven too militarily powerful and with too few disincentives to resist. The machine gun replaced the musket, and today, all advanced militaries possess air forces. So too did many develop nuclear and chemical capabilities, only to abstain from their use or liquidate stockpiles in their entirety.

With history as precedent and the law on its side, forbearance from cyberattacks is eminently possible. Whether or not states observe it is a matter of custom and a project for advocacy. This study offered a template for how that custom might take shape.

[18] Price, "Land Mines," 616.

Bibliography

Works Cited

Adee, Sally. "The Hunt for the Kill Switch." *IEEE Spectrum*, 1 May 2008.

Agence France-Presse. "Growing Threat from Cyber Attacks: U.S. General." 7 April 2009.

———. "U.N. Chief Calls for Treaty to Prevent Cyber War." 30 Jan 2010.

Agence Nationale de la Sécurité des Systèmes d'Information, France. *Information Systems Defence and Security: France's Strategy*. Paris: 2011.

Alberts, Davis, and Richard Hayes. *Power to the Edge: Command...Control...In the Information Age*. Washington: DoD Command and Control Research Program, 2005.

Committee on Armed Services, United States Senate. *Hearing to Consider the Nomination of Lt. Gen. Keith B. Alexander to Commander, U.S. Cybercommand*, 15 April 2010.

Committee on Armed Services, United States House of Representatives. *Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force, Hearing before the Subcommittee on Intelligence, Emerging Threats and Capabilities*, 14 March 2013.

Alger, John. "Introduction to Information Warfare." In *Information Warfare: Chaos on the Electronic Superhighway*, edited by Winn Schwartau. New York: Thunder Mouth Press, 1994.

Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. Indianapolis, IN: Wiley & Sons, 2008.

Andress, Jason, and Steve Winterfeld. *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners*. Oxford: Syngress, 2011.

Annan, Kofi. *Address of the Secretary-General to the General Assembly (23 September)*. New York: United Nations, 2003.

———. *In Larger Freedom: Towards Development, Security, and Human Rights for All*. New York: United Nations, 2005.

Aréchaga, E. Jiménez de. "International Law in the Past Third of a Century." *Recueil des Cours de l'Academie de Droit International (RCADI)* 59, no. 1 (1978).

Arend, Anthony Clark, and Robert J. Beck. *International Law and the Use of Force*. New York: Routledge, 1993.

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo V. Uganda), Judgment, ICJ Reports 168 (2005).

Arquilla, John, and David Ronfeldt. "Emergence and Influence of the Zapatista Social Netwar." In *Networks and Netwars*, edited by John Arquilla and David Ronfeldt. Santa Monica: RAND, 2001.

———, eds. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND, 2001.

Associated Press. "Iran's Nuclear Agency Trying to Stop Computer Worm." *The Independent*, 25 September 2010.

Association of Southeast Asian Nations (ASEAN) Regional Forum. *Statement by the Ministers of Foreign Affairs of the ASEAN Regional Forum Participating States on Cooperation in Ensuring International Information Security*. Bandar Seri Begawan, Brunei: ASEAN, 2010.

Attorney General's Department, Australia. *E-Security Review*. Canberra: 2008.

Attorney General’s Department, Australia. *Cyber Security Strategy*. Canberra: 2009.

Barnes, Julian E. "Cyber-Attack on Defense Department Computers Raises Concerns." *Los Angeles Times*, 28 November 2008.

BBC News. "China Confirms Satellite Downed." 23 January 2007.

———. "Concern over China's Missile Test." 19 January 2007.

———. "Estonia Hit by ‘Moscow Cyber War’." 17 May 2007.

———. "Interview with Prime Minister Gordon Brown: 'We Must Not Be Victims'." 25 June 2009.

———. "New 'Cyber Attacks' Hit S Korea." 9 July 2009.

———. "South Korea Blames North for Bank and TV Cyber-Attacks." 10 April 2013.

———. "Stuxnet Virus Targets and Spread Revealed." 15 February 2011.

———. "Stuxnet Worm Hits Iran Nuclear Plant Staff Computers." 26 September 2010.

———. "US Cyber War Defences 'Very Thin', Pentagon Warns." 16 March 2011.

Betz, David J., and Timothy C. Stevens, eds. *Cyberspace and the State: Towards a Strategy for Cyberpower (Adelphi Series)*. London: Routledge, 2012.

Biddle, Stephen. *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton, NJ: Princeton University Press, 2004.

Black, Max. *Models and Metaphors*. Ithaca: Cornell University Press, 1962.

———. "More About Metaphor." In *Metaphor and Thought*, edited by Andrew Ortony. Cambridge: Cambridge University Press, 1979.

Select Committee on Intelligence, United States Senate. *Annual Threat Assessment of the US Intelligence Community, Unclassified (Testimony of Adm. Dennis C. Blair)*, 2010.

Borg, Scott. *The Cyber Defense Revolution: A Synthesis (Presentation of the U.S. Cyber Consequences Unit)*. Tallinn, Estonia: NATO CCD-COE, 2009.

Bowett, D.W. *Self-Defence in International Law*. New York: Praeger, 1958.

Breitegger, Alexander. *Cluster Munitions and International Law*. New York: Routledge, 2012.

Brennan, John O. *Remarks at the Launch of the U.S. International Strategy for Cyberspace*. Washington: The White House, 2011.

Brenner, Joel. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin, 2011.

———. *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World*. Reprint ed. New York: Penguin, 2013.

Brodie, Bernard. *Strategy in the Missile Age*. Princeton, NJ: Princeton University Press, 1959.

Brownlie, Ian. *International Law and the Use of Force by States*. Oxford: Oxford University Press, 1963.

———. "Some Legal Aspects of the Use of Nuclear Weapons." *International and Comparative Law Quarterly* 14, no. 2 (April 1965): 437-51.

Brunnée, Jutta, and Stephen J. Toope. "The Use of Force: International Law after Iraq." *International and Comparative Law Quarterly* 53, no. 4 (2004): 785-806.

Bryan-Low, Cassell. "British Spy Chief Breaks Agency's History of Silence." *The Wall Street Journal*, 29 October 2010.

Bull, Hedley. *The Anarchical Society*. 3rd ed. New York: Columbia University Press, 2002, first published 1977.

Bull, Hedley, and Adam Watson, eds. *The Expansion of International Society*. Oxford: Oxford University Press, 1984.

Bundy, McGeorge. *Danger and Survival: Choices About the Bomb in the First Fifty Years*. New York: Random House, 1988.

———. "Nuclear Weapons and the Gulf." *Foreign Affairs*, Fall 1991.

Bush, George W. *Remarks by the President on Iraq (Cincinnati, Ohio)*. Washington: U.S. Government Printing Office, 2002.

Buzan, Barry, Ole Waever, and Jaap de Wilde, eds. *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers, 1998.

Cabinet Office, United Kingdom. *Keeping the UK Safe in Cyberspace*. Edited by Cabinet Office of Cybersecurity. London: The Stationary Office, HMG, 2013.

Cameron, David. *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*. Edited by Cabinet Office. London: The Stationary Office, HMG, 2010.

Cameron, Maxwell A., Brian W. Tomlin, and Robert J. Lawson, eds. *To Walk without Fear: The Global Movement to Ban Landmines*. Oxford: Oxford University Press, 1998.

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media, 2009.

Cassese, Antonio. *International Law*. 2nd ed. Oxford: Oxford University Press, 2005.

Centre for the Protection of National Infrastructure (United Kingdom). *Process Control and SCADA Security*. London: CPNI, 2008.

Cho, Jong Ik. "Ha Tae Kyoung Interview on the Growing Cyber-Terrorism Threat from North Korea and the South's Response." *NK Vision*, 15 May 2013.

Church, William. "Information Operations Violates Protocol I." *InfoWar Monitor*, 9 April 1999.

Select Committee on Intelligence, United States Senate. *Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community*, 31 January 2013.

Select Committee on Intelligence, United States Senate. *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community*, 31 January 2012.

Clark, David D., and Susan Landau. "Untangling Attribution." In *Proceedings of a Workshop on Deterring Cyberattacks*, edited by Herbert Lin. Washington: National Academies Press, 2010.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2010.

Clinton, Hillary Rodham. *Remarks at the Launch of the U.S. International Strategy for Cyberspace*. Washington: The White House, 2011.

Coates, A. J. *The Ethics of War*. Manchester: Manchester University Press, 1997.

Coleman, Kim. *A History of Chemical Warfare*. New York: Palgrave Macmillan, 2005.

Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies. *Securing Cyberspace for the 44th Presidency*. Edited by James Lewis. Washington: CSIS, 2008.

Congressional Research Service, United States. *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*. Washington: Congressional Printing Office, 2003.

———. *Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues*. Washington: Congressional Printing Office, 2013.

———. *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*. Washington: Congressional Printing Office, 2005.

———. *Critical Infrastructure: Control Systems and the Terrorist Threat*. Washington: Congressional Printing Office, 2003.

———. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*. Washington: Congressional Printing Office, 2007.

"Constitution of the International Telecommunications Union." In *Constitution and Convention of the International Telecommunications Union*. S. Treaty Doc. No. 104-34, 21, 2010.

Corrin, Amber. "Cyber Executive Order Close, Napolitano Says." *Federal Computer Weekly*, 28 September 2012.

Cortell, Andrew, and James Davis. "How Do International Institutions Matter? The Domestic Impact of International Rules and Norms." *International Studies Quarterly* 40 (1996): 451-78.

Crawford, Neta. "Decolonization as an Internatoinal Norm." In *Emerging Norms of Justified Intervention*, edited by Laura Reed and Carl Kaysen, 37-61. Cambridge, MA: American Academy of Sciences, 1993.

D'Amato, Anthony. "International Law, Cybernetics, and Cyberspace." In *Computer Network Attack and International Law*, edited by Michael Schmitt and Brian O'Donnell, 59-72. Newport, RI: Naval War College, 2002.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired*, 21 August 2007.

Davis, Lance, and Stanley Engerman. *Naval Blockades in Peace and War*. Cambridge: Cambridge University Press, 2006.

Denning, Dorothy. *Information Warfare and Security*. Reading: Addison-Wesley, 1999.

Department of Defense, United States *An Assessment of International Legal Issues in Information Operations*. Edited by Office of the General Counsel. 2nd ed. Washington: U.S. Department of Defense, 1999.

Department of Foreign Affairs and Trade, Australia. *AUSMIN 2011: Transcript of Joint Press Conference with Defence Minister Stephen Smith, US Secretary of State Hillary Clinton and US Secretary of Defense Leon Panetta (15 September)*. Canberra: 2011.

Department of Homeland Security, United States. *Alert: Increasing Threat to Industrial Control Systems*. Edited by Industrial Control Systems Cyber Emergency Response Team. Washington: Department of Homeland Security, 2012.

Detter, Ingrid. *The Law of War*. 2nd ed. Cambridge: Cambridge University Press, 2000.

Dinstein, Yoram. "Computer Network Attacks and Self-Defense." In *Computer Network Attack and International Law*, edited by Michael Schmitt and Brian O'Donnell, 99-120. Newport, RI: Naval War College, 2002.

———. "International Law as a Primitive Legal System." *NYU Journal of International Law and Policy* 19, no. 1 (1986-1987).

———. *War, Aggression and Self-Defence*. 4th ed. Cambridge: Cambridge University Press, 2005.

Douhet, Giulio. *Command of the Air*. Translated by Dino Ferrari. New York: Coward-McCann, 1942.

Dunlap Jr., Charles J. "Meeting the Challenge of Cyberterrorism." In *Computer Network Attack and International Law*, edited by Michael Schmitt and Brian O'Donnell, 59-72. Newport, RI: Naval War College, 2002.

Edelman, R. David. "NATO's Cyber Decade?". In *NATO and the 21st Century: New Security Challenges*, edited by Richard Prosen. Oxford: Oxford University Press, forthcoming.

Elliott, Edward. "The Freedom of Neutral Commerce." *California Law Review* 3, no. 4 (1915): 292-99.

Evron, Gadi. "Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet Wars." *Georgetown Journal of International Affairs* (2008): 121-26.

Falliere, Nicholas. "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems." *Symantic Connect*, 6 August 2010.

Farwell, James P., and Rafal Rohozinski. "The New Reality of Cyber War." *Survival* 54, no. 4 (2012): 107-20.

Feder, Norman M. "Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack." *NYU Journal of International Law and Policy* 19 (1986-7): 395-432.

Federal Chancellery of the Republic of Austria. *Austrian Cyber Security Strategy*. Vienna: 2013.

Federal Department of Defence, Civil Protection and Sport DDPS, Switzerland. *National Strategy for the Protection of Switzerland against Cyber Risks*. Bern: 2012.

Federal Ministry of the Interior, Germany. *Cyber Security Strategy for Germany*. Berlin: February, 2011.

Finnemore, Martha. "Cultivating International Cyber Norms." In *America's Cyber Future: Security and Prosperity in the Information Age*, edited by Kristin and Travis Sharp Lord, 87-121. Washington: Center for New American Security, 2012.

———. *National Interests and International Society*. Ithaca: Cornell University Press, 1996.

Florini, Ann. "The Evolution of International Norms." *International Studies Quarterly* 40 (1996): 363-89.

Follath, Erich, and Holger Stark. "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor." *Speigel Online International*, 2 November 2009.

Forsythe, David P. *The Humanitarians: The International Committee of the Red Cross*. Cambridge: Cambridge University Press, 2005.

Franck, Thomas M. *Recourse to Force: State Action against Threats and Armed Attacks*. Cambridge: Cambridge University Press, 2002.

———. "Who Killed Article 2(4)? Or Changing Norms Governing the Use of Force by States." *American Journal of International Law* 64 (1970).

Freedman, Lawrence. *Deterrence*. Cambridge: Polity, 2004.

———. *The Evolution of Nuclear Strategy*. New York: St. Martin's Press, 1981.

———, ed. *Strategic Coercion: Concepts and Cases*. Oxford: Oxford University Press, 1998.

Friedman, Thomas L. *The World Is Flat: A Brief History of the Twenty-First Century*. 1st ed. New York: Farrar, Straus and Giroux, 2005.

Froehlich, Fritz E., and Allen Kent. *Froehlich/Kent Encyclopedia of Telecommunications*. Vol. 15, New York: Marcel Dekker, 1997.

Frowein, Jochen. "Article 41." In *The Charter of the United Nations: A Commentary*, edited by Bruno Simma, 621-8. Munich: C.H. Beck, 1995.

Fulghum, David. "Israel Used Electronic Attack in Air Strike against Syrian Mystery Target." *Aviation Week*, 8 October 2007.

Fulghum, David A., Amy Butler, and Sally Adee. "Cyber-Combat's First Shot." *Aviation Week*, 26 November 2007.

Gardam, Judith. "The Contribution of the International Court of Justice to International Humanitarian Law." *Leiden Journal of International Law* 14, no. 2 (June 2001): 349-65.

Geist, Michael. "Cyberlaw 2.0." *Boston College Law Review* 44 (2003).

General Accounting Office, United States. *Computer Security: Hackers Penetrate DOD Computer Systems*. Washington: GAO, 1991.

George, Alexander, and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice*. New York: Columbia University Press, 1974.

Georgia Tech Information Security Center. *Emerging Cyber Threat Reports, 2011*. Atlanta, GA: Georgia Institute of Technology, 2011.

Goldsmith, Jack. "Against Cyberanarchy." *University of Chicago Law Review* 65 (1998).

Goldsmith, Jack, and Tim Wu. *Who Control the Internet?: Illusions of a Borderless World*. Oxford: Oxford University Press, 2006.

Goodwin, Jacob. "FERC Seeks to Close Any Cyber-Security ‘Gaps’ at Nuclear Plants." *Government Security News*, 25 March 2009.

Gordon, Edward. "Article 2(4) in Historical Context." *Yale Journal of International Law* 10 (1985).

Gorman, Siobahn, and Julian E. Barnes. "Cyber Combat: Act of War." *Wall Street Journal*, 30 May 2011.

Graham, Bradley. "Military Grappling with Guidelines for Cyberwar." *Washington Post*, 8 November 1999, A1.

Gray, Christine D. "The Bush Doctrine Revisited: The 2006 National Security Strategy of the USA." *Chinese Journal of International Law* 5, no. 3 (2006): 555-78.

———. "The Charter Limitations on the Use of Force: Theory and Practice." In *The United Nations Security Council and War*, edited by Vaughn Lowe, Adam Roberts, Jennifer Welsh and Dominik Zaum, 86-98. Oxford: Oxford University Press, 2010.

———. *International Law and the Use of Force*. 3rd ed. Oxford: Oxford University Press, 2008.

Grotius, Hugo. *On the Law of War and Peace*. Edited by Stephen C. Neff. Cambridge: Cambridge University Press, 2012, first published 1625.

Grove, Greory D., Seymour Goodman, and Stephen Lukasik. "Cyber-Attacks and International Law." *Survival* 42, no. 3 (2000): 89-103.

Hague, William. *Foreign Secretary's Closing Remarks at the London Conference on Cyberspace*. Edited by Foreign & Commonwealth Office. London: The Stationary Office, HMG, 2011.

Hargrove, John Lawrence. "The *Nicaragua* Judgment and the Future of the Law of Force and Self-Defense." *American Journal of International Law* 81, no. 1 (January 1987): 135-43.

Harvey, Mike. "Chinese Hackers 'Using Ghost Network to Control Embassy Computers'." *The Times (London)*, 30 March 2009.

Harvey, Nick. *Armed Forces Minister - Responding to Cyber War*. Edited by UK Ministry of Defence. London: The Stationary Office, HMG, 2011.

Hathaway, Oona, and Rebecca Croontof. "The Law of Cyber-Attack." *California Law Review*, no. 817 (2012).

Hensel, Howard M. "The Protection of Cultural Objects During Armed Conflicts." In *The Law of Armed Conflict: Constraints on the Contemporary Use of Military Force*, edited by Howard M. Hensel. Hampshire: Ashgate, 2006.

Hersch, Seymour. "The Online Threat: Should We Be Worried About a Cyberwar?" *The New Yorker*, 1 November 2010.

Hesse, Mary B. *Models and Analogies in Science*. London: Sheed & Ward, 1963.

Higgins, Rosalyn. *The Development of International Law through the Political Organs of the United Nations*. Oxford: Oxford University Press, 1963.

———. *Problems and Process: International Law and How We Use It*. Oxford: Oxford University Press, 1995.

Hill, Richard. "WCIT: Failure or Success, Impasse or Way Forward?" *International Journal of Law and Information Technology* 21, no. 3 (2013).

Hobbes, Thomas. *Leviathan (with Selected Variants from the Latin Edition of 1668)*. Edited by Edwin Curley. Indianapolis, IN: Hackett, 1994, first published 1668.

Hurrell, Andrew. *On Global Order: Power, Values and the Constitution of International Society*. Oxford: Oxford University Press, 2007.

Huth, Paul, and Bruce Russett. "General Deterrence between Enduring Rivals: Testing Three Competing Models." *American Political Science Review* 87, no. 1 (1993): 61-73.

Information Security Policy Council, Japan. *Information Security Strategy for Protecting the Nation*. Tokyo: 2010.

International Cable Protection Committee. *Subsea Landslide Is Likely Cause of SE Asian Communications Failure*. London: ICPC, 2007.

International Committee of the Red Cross (ICRC). *Conference of Government Experts on the Use of Certain Conventional Weapons*. Geneva: 1976.

———. *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention)*. Geneva: 1949.

———. *Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention)*. Geneva: 1949.

———. *Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention)*. Geneva: 1949.

———. *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention)*. Geneva: 1949.

———. *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*. Geneva: 1977.

International Conferences (The Hague). *Hague Convention (II) with Respect to the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land*. The Hague: 1899.

———. *Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land*. The Hague: 1907.

———. *Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land*. The Hague: 1907.

International Law Commission. *Report of the International Law Commission to the General Assembly*. 1980.

International Telecommunications Union. *World Telecommunication/ICT Indicators Database 2010*. Geneva: 2010.

Jennings, R.Y. "The *Caroline* and McLeod Cases." *American Journal of International Law* 32, no. 1 (January 1938): 82-99.

Jervis, Robert. "Deterrence Theory Reconsidered." *World Politics* 39 (1979): 289-324.

———. *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1976.

Johnson, James Turner. *Just War Tradition and the Restraint of War*. Princeton, NJ: Princeton University Press, 1981.

Joint Chiefs of Staff, United States. *Jp1-02: Department of Defense Dictionary of Military and Associated Terms*. Washington: U.S. Department of Defense, 2001.

———. *National Military Strategy*. Washington: U.S. Department of Defense, 2008.

Kaplan, James, Shantnu Sharma, and Allen Weinberg. "Meeting the Cybersecurity Challenge." *McKinsey Quarterly* (June 2011).

Karrar, Tahani. "Third Undersea Cable Reportedly Cut between Sri Lanka, Suez." *Dow Jones Newswire*, 1 February 2008.

Kaspersky Lab. *Kaspersky Lab Identifies Operation 'Red October,' an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide*. Moscow: Kaspersky Lab, 2013.

Keen, Maurice. *Chivalry*. New Haven: Yale University Press, 1984.

———. *The Law of War in the Late Middle Ages*. New York: Routledge & K. Paul, 1965.

Kelsen, Hans. *General Theory of International Law and State*. Cambridge, MA: Harvard University Press, 1945.

Kenyon, Henry. "Work Commences on $1b NSA 'Spy' Center." *Defense Systems*, 7 January 2011.

Kerr, Donald M. *Remarks by the Principal Deputy Director of National Intelligence at the Association for Intelligence Officers Annual Intelligence Symposium*. McLean, VA: United States Office of the Director of National Intelligence, 2008.

Khalilzad, Zalmay, and John P. White, eds. *Strategic Appraisal: The Changing Role of Information in Warfare*. Santa Monica: RAND, 1999.

Kilcullen, David. "Counter-Insurgency *Redux*." *Survival* 48, no. 4 (2006): 111-30.

Kim, Kwan-jin. "Remarks at the 11th Defense Information Security Conference," news release, 2011.

Kingsbury, Alex. "In Georgia, a Parallel War Rages Online." *U.S. News & World Report*, 13 August 2008.

Kiras, James. "Irregular Warfare." In *Understanding Modern Warfare*, edited by David Jordan, 225-91. Cambridge: Cambridge University Press, 2008.

Kissinger, Henry. *Diplomacy*. New York: Simon and Schuster, 1994.

Klotz, Audie. *Norms and International Relations: The Struggle against Apartheid*. Ithaca: Cornell University Press, 1995.

Subcommittee on Technology and Innovation, Committee on Science and Technology, U.S. House of Representatives. *Untangling Attribution: Moving to Accountability in Cyberspace (Testimony of Robert Knake)*, 2010.

Komov, Sergei, ed. *International Information Security: The Diplomacy of Peace*. Moscow: Russian Federation Official Publications, 2009.

———. "Russian Federation Military Policy in the Area of International Information Security: Regional Aspect." In *International Information Security: The Diplomacy of Peace*, edited by Sergei Komov, 34-44. Moscow: Russian Federation Official Publications, 2007.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington: Potomac Books, Inc., 2009.

Kratochwil, Friedrich, and John Gerard Ruggie. "International Organization: A State of the Art on the Art of the State." *International Organization* 40, no. 4 (1986): 753-75.

Krutskikh, Andrey. "Advancement of Russian Inititaive to Ensure International Information Security (Chronicles of the Decade)." In *International Information Security: The Diplomacy of Peace*, edited by Sergei Komov, 116-41. Moscow: Russian Federation Official Publications, 2009.

———. "Information Challenges to Security (1999)." In *International Information Security: The Diplomacy of Peace*, edited by Sergei Komov. Moscow: Russian Federation Official Publications, 2009.

Kuehl, Daniel T. "China and Cybersecurity." Paper presented at the National Security Seminar, Heritage Foundation, 28 April 2010.

La Rue, Frank. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression." Geneva: United Nations Human Rights Council, 2011.

Laffan, R.G.D., ed. *Select Documents of European History, 800-1482*. New York: Henry Holt, 1929.

Lebow, Richard Ned, and Janice Gross Stein. "Rational Deterrence Theory: I Think, Therefore I Deter." *World Politics* 41, no. 2 (January 1989): 208-24.

Lederberg, Joshua. *Biological Weapons: Limiting the Threat*. Cambridge, MA: MIT Press, 1999.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, ICJ Reports 136 (2004).

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 226 (1996).

"Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General." New York: United Nations, 1998.

Lewis, James A. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington: CSIS, 2002.

———, ed. *Cyber Security: Turning National Solutions into International Cooperation*. Washington: CSIS, 2003.

———. *The Cyber War Has Not Begun*. Washington: CSIS, 2010.

Libicki, Marin C. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND, 2009.

———. "The Nature of Strategic Instability in Cyberspace." *Brown Journal of World Affairs* 18 (2011): 71-82.

Lin, Herbert. "Cyber Conflict and International Humanitarian Law." *International Review of the Red Cross* 94, no. 886 (June 2013): 515-31.

Lord, Kristin, and Travis Sharp, eds. *America's Cyber Future: Security and Prosperity in the Information Age*. Washington: Center for New American Security, 2011.

Lowe, Vaughn, Adam Roberts, Jennifer Welsh, and Dominik Zaum, eds. *The United Nations Security Council and War*. Oxford: Oxford University Press, 2010.

Lucas, George R. "Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets." In *Oxford Institute for Ethics, Law and Armed Conflict seminar series*, 2011.

Lumsdaine, David. *Moral Vision in International Politics*. Princeton, NJ: Princeton University Press, 1993.

Lynn III, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, September/October 2010.

MacFarlane, S. Neil, and Yuen Foong Khong. *Human Security and the UN: A Critical History*. Indianapolis, IN: Indiana University Press, 2006.

Mallison, William T. "Limited Naval Blockade or Quarantine-Interdiction: National and Colelctive Defense Claims Valid under International Law." *George Washington Law Review* 31 (1962).

Mann, Simon. "Cyber War Added to ANZUS Pact." *Sydney Morning Herald*, 16 September 2011.

Markoff, John. "A Silent Attack, but Not a Subtle One." *New York Times*, 26 September 2010.

Markoff, John, and Mark Lander. "Digital Fears Emerge after Data Siege in Estonia." *The New York Times*, 29 May 2007.

Markoff, John, David Sanger, and Thom Shanker. "In Digital Combat, U.S. Finds No Easy Deterrent." *The New York Times*, 25 January 2010, A1.

Markoff, John, and Thom Shanker. "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk." *The New York Times*, 1 August 2009, A1.

Markoff, Michele. "National and Global Strategies for Managing Cyberspace and Security." Paper presented at the Conference of the Atlantic Cuncil: International Engagement On Cyber: Establishing Norms And Improved Security, Washington, 30 March 2011.

Martin, Bradley K. *Under the Loving Care of the Fatherly Leader: North Korea and the Kim Dynasty*. New York: St. Martin's Griffin, 2004.

Maxwell, Stephen. *Rationality in Deterrence*. Adelphi Papers. Vol. 50. London: International Institute of Strategic Studies, 1968.

McAfee. *Global Energy Cyberattacks: 'Night Dragon'*. Santa Clara, CA: McAfee, 2011.

———. *Protecting Your Critical Assets: Lessons Learned from 'Operation Aurora'*. Santa Clara, CA: McAfee, 2010.

McAffee and Good Harbor Consulting. *Virtual Criminology Report*. Santa Clara, CA: McAfee, 2009.

McConnell, Mike. "How to Win the Cyber-War We're Losing." *The Washington Post*, 28 February 2010.

Mccullagh, Declan. "Renewed Push to Give Obama an Internet 'Kill Switch'." *CBSNews*, 24 January 2011.

McDougal, Myres S. "The Soviet-Cuban Quarantine and Self-Defense." *American Journal of International Law* 57 (1963): 597-604.

McElroy, Robert. *Morality and American Foreign Policy*. Princeton, NJ: Princeton University Press, 1992.

McKinsey Global Institute. *Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity*. New York: McKinsey & Company, 2011.

McMahan, Jeff. "Laws of War." In *The Philosophy of International Law*, edited by Samantha Besson and John Tasioulas, 492-509. Oxford: Oxford University Press, 2000.

McMillan, Robert. "Siemens: Stuxnet Worm Hit Industrial Systems." *Computerworld*, 14 September 2010.

Mearsheimer, John J. *Conventional Deterrence*. Ithaca: Cornell University Press, 1983.

Meyrowitz, Henri. *The Principle of Superfluous Injury or Unnecessary Suffering: From the Declaration of St. Petersburg of 1868 to Additional Protocol I of 1977*. Geneva: International Committee of the Red Cross, 1994.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua V. United States of America), Merits, Judgment, ICJ Reports 14 (1986).

Miller, Hunter, ed. *Treaties and Other International Acts of the United States of America*. Vol. 4 (Documents 80-121: 1836-1846). Washington: Government Printing Office, 1934.

Ministry of Administration and Digitisation, Internal Security Agency, Poland. *Cyberspace Protection Policy of the Republic of Poland*. Warsaw: 2013.

Ministry of Business, Innovation & Employment, New Zealand. *New Zealand's Cyber Security Strategy*. Wellington: 2011.

Ministry of Government Administration, Reform and Church Affairs, Norway. *Cyber Security Strategy for Norway*. Oslo: 2012.

Ministry of Transport, Maritime Affairs and Communications, Turkey. *National Cyber Security Strategy and 2013-2014 Action Plan*. Ankara: 2013.

Moir, Lindsay. *Reappraising the Resort to Force: International Law, Jus Ad Bellum, and the War on Terror*. Portland, Oregon: Hart Publishing, 2010.

Morgan, Patrick. *Deterrence Now*. Cambridge: Cambridge University Press, 2003.

———. *Deterrence: A Conceptual Analysis*. Beverly Hills, CA: Sage Publications, 1997.

Morgenthau, Hans J. *Politics among Nations: The Struggle for Power and Peace*. 5th ed. New York: Knopf, 1973.

Mueller, John. *Retreat from Doomsday: The Obsolescence of Major War*. New York: Basic Books, 1989.

"N. Korea 'Confident' in Cyber Warfare Capabilities." *Chosun Ilbo*, 8 April 2013.

Nadelmann, Ethan. "Global Prohibition Regimes: The Evolution of Norms in International Society." *International Organization* 44 (1990): 479-524.

Napolitano, Janet. *Appointment of New Deputy under Secretary for Cybersecurity*. Washington: Department of Homeland Security, 2013.

———. *Remarks at the Launch of the U.S. International Strategy for Cyberspace*. Washington: The White House, 2011.

National Coordinator for Security and Counterterrorism, The Netherlands. *National Cyber Security Strategy 2: From Awareness to Capability*. The Hague: 2013.

Nations, United. "Vienna Convention on the Law of Treaties." 1969.

Nicholson, Brendan. "World Fury at Satellite Destruction." *The Age*, 20 January 2007.

North Atlantic Treaty.

North Atlantic Treaty Organization. *Active Engagement, Modern Defence: Strategic Conept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Lisbon: NATO, 2010.

———. "Cyber Defense: Background & History."

———. *Lisbon Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Lisbon*. Lisbon: NATO, 2010.

———. "Press Conference by NATO Secretary General Anders Fogh Rasmussen Following the NATO Defence Ministers Meeting on 4 June 2013," news release, 4 June 2013.

"North Korea Launched Cyber Attacks, Says South." *Associated Press*, 11 July 2009.

Nye, Joseph. *The Future of Power*. New York: PublicAffairs, 2011.

O'Connell, D.P. *The International Law of the Sea*. Edited by I.A Schearer.New York: Clarendon Press, 1983.

Ober, Josiah. "Classical Greek Times." In *The Laws of War: Constraints on Warfare in the Western World*, edited by Michael Howard, George J. Andreopoulos and Mark R. Schulman, 12-26. New Haven: Yale University Press, 1994.

———. *Mass and Elite in Democratic Athens: Rhetoric, Ideology, and the Power of the People*. Princeton, NJ: Princeton University Press, 1989.

Office of Technology Assessment (United States). *Information Security and Privacy in Network Environments*. Washington: Government Printing Office, 1994.

Oil Platforms (Islamic Republic of Iran V. United States of America), Judgment, ICJ Reports 161 (2003).

Oppenheim, L. *International Law, a Treatise*. Vol. 2, London: Longmas, Green and Co., 1912.

Organisation for Economic Cooperation and Development. "The Impact of Internet in OECD Countries." In *OECD Digital Economy Papers*. Paris: OECD Publishing, 2012.

———. "Measuring the Internet Economy." In *OECD Digital Economy Papers*. Paris: OECD Publishing, 2013.

Organization for Security and Co-operation in Europe. "Remarks of the Coorindator for Cyber Issues, U.S. Department of State." Paper presented at the OSCE

Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Rule, Vienna, 9-10 May 2011.

Panarin, Igor. "Supremacy in Cyberspace: Obama's 'Star Wars'?" *RT*, 11 January 2012.

Armed Service Committee, United States Senate. *Hearing to Consider the Nomination of Hon. Leon E. Panetta to Be Secretary of Defense*, 2011.

Panetta, Leon. *Remarks on Defending the Nation from Cyber Attack (11 October)*. Washington: U.S. Department of Defense, 2012.

Pape Jr., Robert A. *Bombing to Win*. Ithaca: Cornell University Press, 1996.

———. "Coercion and Military Strategy: Why Denial Works and Punishment Doesn't." *Journal of Strategic Studies* 15, no. 4 (1992): 423-75.

Parker, Geoffrey. "Early Modern Europe." In *The Laws of War: Constraints on Warfare in the Western World*, edited by Michael Howard, George J. Andreopoulos and Mark R. Schulman. New Haven: Yale University Press, 1994.

Parks, W. Hays. "Operation Rolling Thunder and the Law of War." *Air University Review* (1982).

Plano, Jack, Lawrence Ziring, and Roy Olton. *International Relations: A Political Dictionary*. Santa Barbara: ABC-CLIO, 1995.

Plato. *The Republic*. Translated by Francis MacDonald Cornford. Oxford: Oxford University Press, 1964.

Powell, Robert. "Nuclear Deterrence and the Strategy of Limited Retaliation." *American Political Science Review* 83, no. 2 (1989): 503-19.

———. *Nuclear Deterrence Theory: The Search for Credibility*. Cambridge: Cambridge University Press, 1990.

Price, Richard. "Reversing the Gun Sights: Transnational Civil Society Targets Land Mines." *International Organization* 52, no. 3 (1998): 613–44.

Price, Richard M. *The Chemical Weapons Taboo*. Ithaca: Cornell University Press, 1997.

Price, Richard, and Nina Tannenwald. "Norms and Deterrence: The Nuclear and Chemical Weapons Taboos." In *The Culture of National Security*, edited by Peter Katzenstein. New York: Columbia University Press, 1996.

"Project of an International Declaration Concerning the Laws and Customs of War." Brussels, 1874.

"Protocol on Non-Detectable Fragments (Protocol I)." In *The Laws of Armed Conflicts: A Collection of Conventions, Resolutions, and Other Documents*, edited by Dietrich Schindler and Jiří Toman. Geneva: Henry Dunant Institute, 1980.

Public Safety Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada*. Ottawa: 2010.

Questor, George. *Deterrence before Hiroshima*. New York: John Wiley, 1966.

———. *The Future of Nuclear Deterrence*. Lexington, MA: Lexington Books, 1986.

Ramsey, Paul. *War and the Christian Conscience: How Shall Modern War Be Conducted Justly?* Durham, NC: Duke University Press, 1961.

Randelzhofer, Albrecht. "Article 2(4)." In *The Charter of the United Nations: A Commentary*, edited by Bruno Simma. Munich: C.H. Beck, 1995.

———. "Article 51." In *The Charter of the United Nations: A Commentary*, edited by Bruno Simma. Munich: C.H. Beck, 1995.

Rattray, Greg. *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press, 2001.

Reardon, Marguerite. "Vandals Blamed for Phone and Internet Outage." *CNet News*, 9 April 2009.

Reichberg, Gregory M., Henrik Syse, and Endre Begby, eds. *The Ethics of War: Classic and Contemporary Readings*. Oxford: Blackwell Publishing, 2006.

Reisman, Michael. "Allocating Competences to Use Coercion in the Post Cold-War World, Practices Conditions, and Prospects." In *Law and Force in the New International Order*, edited by Lori F. Damrosch and David J. Scheffer. Boulder, CO: Westview Press, 1991.

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

———. *Cyber War Will Not Take Place*. London: C Hurst & Co. Publishers, Ltd., 2013 (forthcoming).

Riley, Chris. "Interview with Toomas Hendrik Ilves: Cyber Attacks, NATO - and Angry Birds." *NATO Review Magazine*, 13 June 2013.

Roach, J. Ashley. "The Law of Naval Warfare at the Turn of the Two Centuries." *American Journal of International Law* 94 (2000): 64-77.

Roberts, Sir Adam. "The Equal Application of the Laws of War: A Principle under Pressure." *International Review of the Red Cross* 90, no. 872 (2008): 931-62.

———. "Land Warfare: From Hague to Nuremberg." In *The Laws of War: Constraints on Warfare in the Western World*, edited by Michael Howard, George J. Andreopoulos and Mark R. Schulman, 116-39. New Haven: Yale University Press, 1994.

Roberts, Sir Adam, and Richard Guelff. *Documents on the Laws of War*. 3rd ed. Oxford: Oxford University Press, 2000.

Rodin, David. *War & Self-Defense*. Reprint ed. Oxford: Oxford University Press, 2010, first published 2002.

Rogers, Clifford J. "Revolutions in Military Affairs - a Historian's Perspective." In *Toward a Revolution in Military Affairs?*, edited by Thierry Gongora and Harald Von Riekhoff. Westport: Greenwood Publishing Group, 2000.

Roscini, Marco. "Threats of Armed Force and Contemporary International Law." *Netherlands Law Review*, no. 54 (2007).

Rowe, Neil C. "Towards Reversible Cyberattacks." Consortium for Emerging Technologies, Military Operations, and National Security, 2011.

Russian Federation, People's Republic of China, Tajikistan, and Uzbekistan. "Letter to the Secretary-General on a Draft International Code of Conduct for Information Security." New York: United Nations, 2011.

Ryan, Daniel J., and Julie C. H. Ryan. "Protecting the National Information Infrastruture against Infowar." In *Information Warfare: Chaos on the Electronic Superhighway*, edited by Winn Schwartau. New York: Thunder Mouth Press, 1994.

Saul, Ben, ed. *Defining Terrorism in International Law*. Oxford: Oxford University Press, 2006.

Savage, John E., and Les Bloom. "On Cyber Peace." In *Reports of the Cyber Statecraft Initiative*. Washington: The Atlantic Council, 2011.

Savage, John E., and Melissa E. Hathaway. "Stewardship of Cyberspace: Duties for Internet Service Providers." In *Cyber Dialogue: What is Stewardship in Cyberspace?* University of Toronto, Munk School of Global Affairs: University of Toronto, 2011.

Schachter, Oscar. "In Defense of International Rules on the Use of Force." *University of Chicago Law Review* 53 (Winter 1986): 113-46.

———. "The Right of States to Use Armed Force." *Michigan Law Review* 82, no. 5/6 (April-May 1984): 1620-46.

Schelling, Thomas C. *Arms and Influence*. New Haven: Yale University Press, 1966.

———. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press, 1960.

Schmitt, Michael. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law* 37 (1999): 885-937.

———. "Cyber Operations and the Jus in Bello: Key Issues." *Naval War College International Law Studies* (March 2011).

———, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2013.

Schmitt, Michael, and Brian O'Donnell, eds. *Computer Network Attack and International Law*. Newport, RI: Naval War College, 2002.

Schwarzenberger, Georg. "The Fundamental Principles of International Law." *Recueil des Cours de l'Academie de Droit International (RCADI)* 87 (1955): 191-386.

———. *The Legality of Nuclear Weapons*. London: Stevens & Sons, 1958.

Schwebel, Stephen. "Aggression, Intervention and Self-Defense in Modern International Law." Chap. 33 In *Justice in International Law: Selected Writings of Judge Stephen M. Schwebel*, edited by Stephen Schwebel, 530-92, 1994.

SecDev Group. "Tracking Ghostnet: Investigating a Cyber Espionage Network." *Information Warfare Monitor*, 29 March 2009.

Secretariat of the Security and Defence Committee, Finland. *Finland's Cyber Security Strategy*. Helsinki: 2013.

Segall, Anna. "Economic Sanctions: Legal and Policy Constraints." *International Review of the Red Cross*, no. 836 (1999).

Shanghai Cooperation Organisation. *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security*. 2009.

Silver, Daniel B. "Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter." In *Computer Network Attack and International Law*, edited by Michael Schmitt and Brian O'Donnell, 73-98. Newport, RI: Naval War College, 2002.

Singer, Peter. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: The Penguin Press, 2009.

Snyder, Glynn. *Deterrence and Defense: Towards a Theory of National Security*. Princeton, NJ: Princeton University Press, 1961.

Sridharan, Vasudevan. "Russia Setting up Cyber Warfare Unit under Military." *International Business Times*, 2013.

Stacey, Robert C. "The Age of Chivalry." In *The Laws of War: Constraints on Warfare in the Western World*, edited by Michael Howard, George J. Andreopoulos and Mark R. Schulman, 27-39. New Haven: Yale University Press, 1994.

Stein, George J. " Information Warfare." *Airpower Journal* 9, no. 1 (1995).

Stewart, Phil. "Old Worm Won't Die after 2008 Attack on Military." *Reuters*, 16 June 2011.

Stone, Julius. *Aggression and World Order: A Critique of United Nations Theories of Aggression*. Clark, NJ: The Lawbook Exchange, Ltd., 1958.

Streltsov, Anatoly A. "International Information Security: Description and Legal Aspects." In *International Information Security: The Diplomacy of Peace*, edited by Sergei Komov, 45-57. Moscow: Russian Federation Official Publications, 2008.

Stürchler, Nikolas. *The Threat of Force in International Law*. Cambridge: Cambridge University Press, 2007.

Svensson, Peter. "Finger-Thin Undersea Cables Tie World Together." *Associated Press*, 31 January 2008.

Sydney Morning Herald. "Estonia Urges Firm EU, NATO Response to New Form of Warfare: Cyber Attacks." 16 May 2007.

Symantec. "Here Comes the CNCI, and the Era of Proactive IT Security." 28 August 2008.

Taft IV, William H. "Self-Defense and the *Oil Platforms* Decision." *Yale Journal of International Law* 29 (2004).

Talbot, David. "Russia's Cyber Security Plans: As Washington Airs Plans for a New 'Cyber Command,' a Top Russian Official Discusses the Threat of Cyberweapons." *MIT Technology Review*, 2010.

Tannenwald, Nina. *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945*. Cambridge: Cambridge University Press, 2007.

Technological Capabilities Panel, Science Advisory Committee, United States. "Meeting the Threat of Surprise Attack." The White House, 1955.

The White House. *Joint Fact Sheet: U.S. And UK Cooperation on Cyberspace*. Washington: U.S. Government Printing Office, 2011.

———. *The National Strategy to Secure Cyberspace*. Washington: U.S. Government Printing Office, 2009.

———. "U.S.-Russian Cooperation on Information and Communications Technology Security," news release, 17 June, 2013.

———. *The United States International Strategy for Cyberspace*. Washington: U.S. Government Printing Office, 2011.

———. *The United States National Security Strategy*. Washington: U.S. Government Printing Office, 2009.

Thomas, Ward. *The Ethics of Destruction: Norms and Force in International Relations*. Ithaca: Cornell University Press, 2001.

Thompson, Iain. "Russia 'Hired Botnets' for Estonia Cyber-War: Russian Authorities Accused of Collusion with Botnet Owners." *Computing (UK)*, 31 May 2007.

Tikk, Eneken, ed. *Frameworks for International Cyber Security: Legal and Policy Instruments.* Vol. 1. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2010.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International Cyber Incidents: Legal Considerations*. Edited by Eneken Tikk. Tallinn, Estonia: NATO Cooperative Cyber Defence-Centre of Excellence, 2010.

Tiyagi, Amit Kumar, and G. Aghila. "A Wide Scale Survey on Botnet." *International Journal of Computer Applications* 34, no. 9 (2011): 9-22.

Trend Micro. "Russian Underground 101." Cupertino, CA: Trend Micro, 2012.

Tubbs, David, Perry G. Luzwick, and Walter Gary Sharp. "Technology and Law: The Evolution of Digital Warfare." In *Computer Network Attack and International Law*, edited by Michael Schmitt and Brian O'Donnell. Newport, RI: Naval War College, 2002.

United Nations. *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (and Protocols) (as Amended on 21 December 2001)*. Geneva: 1980.

———. *Statute of the International Court of Justice*. 1946.

United Nations General Assembly. *Definition of Aggression (A/RES/3314 [XXIX])*. 1974.

———. *Convention on the Law of the Sea*. Montego Bay, Jamaica: 1982.

United Nations Group of Governmental Experts (2008-9). *Report Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2008-9)*. Geneva: United Nations (UNIDIR), 2010.

United Nations Group of Governmental Experts (2011-12). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2011-12)*. New York: United Nations (UNIDIR), 2013.

United Nations Secretary-General. "Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General." New York: United Nations, 2011.

———. *Report of the Secretary-General Pursuant to Paragraph 2 of Security Council Resolution 808*. New York: United Nations, 1993.

United Press International. "NATO Will Lay out New Plan for Cyberwar." 10 March 2008.

United States Air Force. *Air Force Doctrine Document 2-11: Cyberspace Operations*. Washington: LeMay Center for Doctrine Development and Education, 2008.

———. *Commander's Handbook on the Law of Armed Conflict 6-2*. Washington: 1980.

United States Army. *Operational Law Handbook*. Edited by International & Operational Law Department.Charlottesville, VA: Judge Advocate General's School, 1995.

United States National Research Council. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Edited by William A. Owens and Kenneth W. Dam. Washington: National Academies Press, 2009.

Van Evera, Stephen. *Guide to Methods for Students of Political Science*. Ithaca: Cornell University Press, 1997.

Waldock, Claude H. M. "The Regulation of the Use of Force by Individual States in International Law." *Recueil des Cours de l'Academie de Droit International (RCADI)* 81 (1952): 451-517.

Walker, George K. "Information Warfare and Neutrality." *Vanderbilt Journal of Transnational Law* 33, no. 5 (November 2000): 1079-12000.

Waltz, Kenneth N. *Theory of International Politics*. Reprint ed. New York: Waveland, 2010 (first published 1979).

Walzer, Michael. *Just and Unjust Wars*. 4th ed. New York: Basic Books, 1977.

Wardrop, Murray. "William Hague: 'Britain Faces Growing Cyberspace Arms Race'." *The Telegraph*, 18 October 2011.

Wight, Martin. *Systems of States*. Leicester: Leicester University Press, 1977.

Wittner, Lawrence S. *Resisting the Bomb: A History of the World Nuclear Disarmament Movement, 1954-1970*. Stanford: Stanford University Press, 1998.

Wood, Michael. "International Law: Lecture 3." In *Hersch Lauterpacht Memorial Lectures*. Cambridge, UK: Cambridge University Press, 2006.

World Federation of Scientists Permanent Monitoring Panel on Information Security. *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*. Edited by Henning Wegener. World Federation of Scientists, 2003.

Wright, Bruce A. "Remarks before the Defense Colloquium on Information Operations." 1999.

Wu, Xu. *Chinese Cyber Nationalism*. New York: Lexington Books, 2007.

Xinhua News Agency. "U.S. Cyber Strategy Dangerous: Chinese Experts." *China Daily USA*, 2011.

Yonhap News Agency. "S. Korea to Launch Cyber Command Next Week." 8 January 2010.

Zeidanloo, Hossein Rouhani, Farhoud Hosseinpour, and Farhood Farid Etemad. "New Approach for Detection of IRC and P2P Botnets." *International Journal of Computer and Electrical Engineering* 2, no. 6 (2010).

Zissis, Carin. *Backgrounder: China's Anti-Satellite Test*. New York: Council on Foreign Relations, 2007.

Zittrain, Jonathan. *The Future of the Internet — and How to Stop It*. New Haven: Yale University Press, 2008.