2020

An Economic Analysis of Cyber Warfare Governance Models

Kevin M. Kelleher
University of Denver

An Economic Analysis of Cyber Warfare Governance Models

Abstract

Allusions to death delivered by bits and bytes have been in vogue since the Reagan administration. Yet, as the internet and its connected devices have since proliferated, cyber violence remains far more fiction than fact. Nevertheless, prominent U.S. officials have all but assured the eventuality of a devastating attack. In anticipation, political, legal, and industry experts are now seeking to codify and inculcate international norms to govern acts of war prosecuted via cyberspace. Two of the most prominent governance models to emerge are the Tallinn Manual and Microsoft's Digital Geneva Convention. The driving thesis of this research argues that within the monolith of the internet, there lie situations that can be examined through the lens of New Institutional Economics and commons governance, lending to rigorous and outcomes-based policy analysis. Through the application of Ostrom's Institutional Analysis and Development framework, this paper individually evaluates the two governance models in question and offers a theory as to the likely efficacy of each approach. This research ultimately finds that the Tallinn Manual achieves its narrow and explicit aims of demonstrating how international law applies to cyberspace while falling short of reaching its full potential as a governance institution. The Digital Geneva Convention is unlikely to meet its objective of becoming a binding international agreement, though the associated, newly founded CyberPeace Institute could breathe life into the initiative.

Document Type

Thesis

Degree Name

M.A.

Department

Josef Korbel School of International Studies

First Advisor

Deborah Avant

Second Advisor

Rachel Epstein

Third Advisor

Julia Macdonald

Keywords

Cyber warfare, Cybersecurity, Elinor Ostrom, Geneva conventions, Law of armed conflict, New institutional economics

Subject Categories

Economics | Economic Theory | International Law | International Relations | Law

An Economic Analysis of Cyber Warfare Governance Models

A Thesis

Presented to

the Faculty of the Josef Korbel School of International Studies

University of Denver

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

---

by

Kevin M. Kelleher

August 2020

Advisor: Deborah Avant, PhD

Author: Kevin M. Kelleher
Title: An Economic Analysis of Cyber Warfare Governance Models
Advisor: Deborah Avant, PhD
Degree Date: August 2020

ABSTRACT

Allusions to death delivered by bits and bytes have been in vogue since the Reagan administration. Yet, as the internet and its connected devices have since proliferated, cyber violence remains far more fiction than fact. Nevertheless, prominent U.S. officials have all but assured the eventuality of a devastating attack. In anticipation, political, legal, and industry experts are now seeking to codify and inculcate international norms to govern acts of war prosecuted via cyberspace. Two of the most prominent governance models to emerge are the Tallinn Manual and Microsoft's Digital Geneva Convention. The driving thesis of this research argues that within the monolith of the internet, there lie situations that can be examined through the lens of New Institutional Economics and commons governance, lending to rigorous and outcomes-based policy analysis. Through the application of Ostrom's Institutional Analysis and Development framework, this paper individually evaluates the two governance models in question and offers a theory as to the likely efficacy of each approach. This research ultimately finds that the Tallinn Manual achieves its narrow and explicit aims of demonstrating how international law applies to cyberspace while falling short of reaching its full potential as a governance institution. The Digital Geneva Convention is unlikely to meet its objective of becoming a binding international agreement, though the associated, newly founded CyberPeace Institute could breathe life into the initiative.

ACKNOWLEDGEMENTS

Writing this has been anything but a straightforward endeavor. Many have borne witness to my prevarications over the years and been kind enough to entertain a wide variety of potential angles and topical variations. I would like to express my profound appreciation to those who tolerated my stochastic thought process. To my advisor, Deborah Avant, as well as Rachel Epstein, Julia Macdonald, and Lisa Victoravich for their willingness to join my thesis committee and for their time and thoughtfulness throughout review and defense. Professors Avant and Epstein have been particularly instrumental in the development of my thinking about global governance issues and political economy. To Lewis Griffith for his teaching, incisive feedback, and the many valuable exchanges we shared via email and at office hours during my time at Korbel. To Ryan Mahon, for thought provoking conversations about the world around us and for offering editorial insights while steeped in his own military training. To Colonel David Wallace for his helpful feedback on one of the earliest drafts of this paper. To Winnona DeSombre for her characteristically enlightening and detailed critiques. To Wendi Peck and Bill Casey for taking a chance and giving me a completely different perspective on military leadership. To the Nobles, for being the best family I never had to ask for. To Bill and Lisa Bauman for their encouragement. And to Becca, for her love, support, and enduring faith in me and in us.

TABLE OF CONTENTS

INTRODUCTION

"At no time in the last two centuries has it been easy to predict whether a major weapon will determine the course of a coming war, let alone be employed."

-Geoffrey Blainey, The Causes of War

In the early evening hours of April 22, 1915, just north of the Belgian town of Ypres, the German Army unleashed a "strange green cloud of death,"[1] which wafted low over the Flemish countryside, choking the life out of everything in its path. The use of chlorine gas that day defied Germany's own accession to the Hague Conventions of 1899 and 1907, the former specifically banning the employment of poison and asphyxiating gases as means of injuring the enemy.[2] Such renegation quickly became the rule rather than the exception with France, Britain, and eventually most major powers relying on chemical weapons of some form or another for the remainder of the First World War. This example invites speculation as to whether or not even the most overt diplomatic actions can guarantee the cooperation of warring parties to obey limits of violence. Ever elusive, peace in our time. The world now stands at the precipice of a new era of technological weaponry —autonomous robots, malware, sophisticated cyberattacks — the costs of which are yet to be known. The question is whether or not modern diplomats can square the circle of channeling international outrages such that violence, if necessary, is directed and limited, avoiding wanton death, especially of noncombatants. At a time of

great uncertainty, two prominent models — the Tallinn Manual and the Digital Geneva Convention — now strive to codify international norms for the conduct of cyber warfare. This paper offers a view of cyber warfare as a problem of commons governance, evaluates the likely efficacy of the models in question, and seeks to advance the global conversation of how best to prevent unnecessary harm in the information age.

To date, the total number of casualties (that is, deaths or injuries) reported as a direct result of a cyberattack stands at zero.[3] The total number of cyberattacks credibly alleged to have caused physical destruction of any kind stands at two. The first such attack, referred to as Operation Olympic Games, or Stuxnet, took place in late 2009 at a uranium enrichment facility in Iran, causing breakage of nearly 1,000 industrial centrifuge cylinders.[4] The second, for which details remain extraordinarily scant, took place in 2014 at a yet unnamed steel mill in Germany, causing "massive physical damage."[5] The paucity of physical transgression (even evidence for those alleged cases) notwithstanding, cyber prognosticators warn of an increasingly dire international situation in which nation-state attacks are certain to progress in severity to the point of becoming a new kind of violent political instrument: Cyber War. Over the past 10 years, government officials, including former Defense Secretary Leon Panetta, former Homeland Security Secretary Janet Napolitano, and former head of both NSA and U.S. Cyber Command, Admiral Michael Rogers, have popularized phrases such as "Cyber Pearl Harbor" and "Cyber 9/11."[6][7][8] The analogies and coincident assurances of "*when*, not *if*" have wound their way into serious discussion, while also prompting some not-so-sotto-voce criticism.[9] The imagery is clear enough. At the highest levels of U.S. national security, the belief is that new technology

offers new ways for international political opponents to unleash unforeseen and physically devastating attacks on one another.

The luxury of relative peace has given legal, academic, military, and industry experts time to consider the consequences of cyber-physical attacks. This thinking has elicited two prominent constructs (technically, models) aiming in their own ways to deter, or at least dissuade nations from utilizing the kinds of technology and tactics, techniques, and procedures (TTPs) capable of delivering death via digital means. Those models are The Tallinn Manual and the Digital Geneva Convention (DGC). These models approach the issue of cyber warfare from different vantage points; the former a legal translation of international law as it pertains to *jus ad bellum* and *jus in bello* and the latter a private sector initiative to inculcate global norms dealing more narrowly with international humanitarian law (IHL). In that sense, the Tallinn Manual captures all that the DGC seeks to address and therefore both deal with the appropriate conduct of cyber warfare pursuant to the protection of noncombatants. With assistance from the field of New Institutional Economics (NIE), the research presented in this paper examines these governance models, taking into account their differing approaches and analyzing contextual variables, ultimately evaluating the likely efficacy of each in their IHL-related endeavors. A hopeful byproduct of this paper is to influence the ever-populating arena of would-be governors of cyber warfare in the fundamental economic question of how to efficiently allocate resources; principally now: attention.

The Tallinn Manual was first published in 2013 as the Tallinn Manual on the International Law Applicable to Cyber Warfare; the product of four years of scholarly collaboration by an International Group of Experts (IGE) led by international law scholar

Michael N. Schmitt. Its second and most recent version, superseding, while including and expanding upon and beyond the precepts of the first, was published in 2017 as the Tallinn Manual 2.0 on the Law Applicable to Cyber Operations. References throughout this paper to the "Tallinn Manual" indicate the latter version. The Tallinn Manual consists of 154 rules divided into 20 categories ranging from Sovereignty and Jurisdiction to the Law of Armed Conflict and Occupation. Each rule addresses a specific legal issue at the nexus of international law and cyber operations, then provides discussion and interpretation, commenting only on the *lex lata* and "assiduously" avoiding the *lex ferenda*.[10] A motivating example of both the structure and breadth of the manual is found in Rule 58 (a), which states that *"Cyber operations on the moon and other celestial bodies may be conducted only for peaceful purposes,"* citing Article IV of the Outer Space Treaty.[11] While assembled at the behest and published under the auspices of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence (CCD COE), the authors of the Tallinn Manual make clear it is an independent, nonbinding expression of expert opinion. It is not an official document.[12] The primary audience of the Tallinn Manual is "State legal advisors," though it does make room for broader consumption.[13]

The Digital Geneva Convention has aimed at broad consumption from the start. As presswork was underway on the second edition of the Tallinn Manual, Microsoft President Brad Smith introduced the DGC via keynote speech at RSA Conference in San Francisco. Unlike the Tallinn Manual, a concerted, long-term, international effort and evolutionary work, the DGC appeared seemingly *ex nihilo*.[14] Citing the "expansion of nation-state attacks" Smith exhorted private sector technology companies to call on governments to,

"come together, affirm international cybersecurity norms that have emerged in recent years, adopt new and binding rules, and get to work implementing them."[15] He listed six specific tenets of the proposed Digital Geneva Convention, among them: "No targeting of tech companies, private sector, or critical infrastructure," and, "Assist private sector efforts to detect, contain, respond to, and recover from events."[16] Later in 2017, Mr. Smith went to Geneva to present the DGC to the United Nations.

While critical reception for the Tallinn Manual has been generally positive, it has also generally been limited to legal and security blogs and publications. Though the *Washington Post* was quick to ask how its guidelines may apply to nations meddling in elections. the DGC was met with greater fanfare from prominent publications such as WIRED magazine, which quickly asserted "Microsoft Is Right: We Need a Digital Geneva Convention."[17] The same year, the World Economic Forum (WEF) pressed the issue with a blog entitled "Why we urgently need a Digital Geneva Convention."[18] Some, however, questioned the necessity and utility of the DGC, including the CCD COE, which called the move "both legally confusing and politically unrealistic."[19] Since announcing the DGC, Microsoft has led several tangential initiatives such as the Cybersecurity Tech Accord, the Digital Peace Now "movement," and establishment of the Geneva-based CyberPeace Institute. What Microsoft's approach to the DGC lacks in the historical foundations found in the Tallinn Manual, it attempts to make up for with the kind of rapid iteration iconic of Silicon Valley (or Redmond, as it were).

For all the ways in which the Tallinn Manual and the DGC differ in their approach, they have one significant commonality: they are both models of governance put forth by aspiring global governors. Governance scholar Deborah Avant, of the University of

Denver, defines global governors as "authorities who exercise power across borders for purposes of affecting policy."[20] This may not be clear at first due to wide variances between progenitors (a group of legal and academic experts versus the president of a tech company), development processes (heterogenous colloquia versus homogenous corporate decisioning), and explicit aims (mapping the *lex lata* to modern issues versus calling on government action). But each in its own way approximates the situation of cyber warfare, framing it with distinguishable exogenous and endogenous variables, their relationships, and expected outcomes. Here, the mere act of framing is itself an attempt to influence behavior in a particular arena, viz. international politics. It is striking to consider the different conditions under which the International Group of Experts and Microsoft simultaneously came to publish similar implicit assessments about the increasing probability of cyber warfare. The two models establish a spectrum of action ranging from promotion of messaging intended to reify and osmose international norms, to the call for an independent global governance regime to promulgate and even enforce a set of binding rules.

Governance itself tends to be a function of leadership and authority. Avant notes, "…authority [is] the ability to induce deference in others."[21] Therefore, a key component of any analysis of governance models is aptitude to induce deference. In the edited volume *Who Governs the Globe?* Avant introduces multiple types of authority — institutional, delegated, expert, principled, and capacity-based — while instructing that a combination of these is far more prevalent than any single type. Governance issues are examined in depth as part of the Analysis section of this paper, but it is useful to be aware of the types of authority implicitly exhibited by each model. The Tallinn Manual serves as a prime

example of expert authority while the Digital Geneva Convention may be seen as a delegated authority that borrows the principled authority (really, the brand) of the established Geneva Conventions. By initially framing this issue in the context of governance problems, it both motivates the desired outcome of establishing international norms and aligns with existing literature in the field of economics that enables more discrete measurement and investigation.

As is often the case with security scholarship, an overarching challenge lies in proving a negative and avoiding successful proclamations of *cum hoc ergo propter hoc*. Prediction can be a fool's errand. As the philosopher Laozi admonished, *"Those who have knowledge, don't predict. Those who predict, don't have knowledge."*[22] Fortunately, the dismal science is never afraid to play the fool. The discipline of New Institutional Economics — that which theorizes about norms and rules governing the nature of property ownership, transaction costs, and institutions themselves — and specifically the study of how to effectively govern common pool resources (CPR), offers a robust, rigorous, and roundly tested evaluative framework well suited for normalizing and analyzing these two models.

Powering the Analysis section of this paper is one of the most well-known evaluative tools to emerge from NIE scholarship dealing with CPR management: Elinor Ostrom's Institutional Analysis and Development (IAD) framework. Ostrom, whose Nobel Prize-winning academic work focused largely on the organization of governance systems for common pool resources, recognized that, *"one needs a common framework…in order to address questions of reform and transition. Particular models then help the analyst to deduce specific predictions about likely outcomes of highly simplified structures."*[23]

Without minimizing the years of work that have gone into them, both the Tallinn Manual and Digital Geneva Convention are highly simplified structures in their own ways: the Tallinn Manual a legal reference book and the DGC a confederation of speeches, policy papers, and organizations. Each model addresses issues of reform and transition. Here, reform may seek to answer questions of how best to change current legal and diplomatic constructs such that nations consciously minimize collateral damage caused by cyber warfare.[24] Transition may seek to answer questions of how to bring awareness to the nature of the changing battlefield so that nations are held accountable for actions that violate existing international law. The IAD presents a well-defined framework for normalizing and analyzing how and how well governance systems function. The ability to accurately assess preventive regimes and promulgate the kinds of institutions and norms that have the highest likelihood of reducing negative outcomes becomes more important with each passing moment that the number of cyber war casualties remains zero.

The research untaken herein is interdisciplinary by nature, with debts to the studies of international relations, international security (esp. warfare and cybersecurity), global governance, institutional economics, public policy, and international humanitarian law. However, it also strives to be as accessible as possible. Therefore, key concepts are explained throughout, with motivating examples similar to those found in this introduction. The structure of the paper is as follows: The complete set of introductory chapters consist of the preceding overview, next a review of the economic underpinnings of the research design, making the case for viewing cyberwarfare as an issue of CPR governance. With the necessary justification for invoking the Institutional Analysis and Development framework in place, the Methodology presents definitions of terms and a diagram that will

make four-star Clausewitzians swoon. It also delineates specific process steps and evaluative criteria. The subsequent section on The Evolution of Governance in Cyberspace explains how global governance works. It tours major milestones in the development of cyber governance from a matter with origins in U.S. national security to managing problems of cybercrime and now to the establishment of international norms. This leads to a section that presents more in-depth background on both the Tallinn Manual and the Digital Geneva Convention. In the Analysis section, each model is independently fitted to the IAD framework and evaluated against the criteria defined in the Methodology section. Finally, the conclusion restates the findings of the analysis and inquires as to the appropriateness of corporate involvement in global governance as it relates to warfare before offering a few final thoughts on New Institutional Economics and lessons learned from the application of the IAD.

ON THE DEVELOPMENT OF NEW INSTITUTIONAL ECONOMICS

Tragic Origins of Common Pool Resource Theory

What is a common pool resource? Why is the concept so prevalent and even at times controversial among scholars of political science and economics? Principally, the issue of what makes a CPR comes down to property ownership and rights of use. The inherent dilemma is well defined by Adam Smith, writing in *Wealth of Nations*, *"It is [every individual's] own advantage, indeed, and not that of the society, which he has in view. But the study of his own advantage naturally, or rather necessarily leads him to prefer that employment which is most advantageous to the society."*[25] Smith's positivism makes no conjecture as to the ways in which self-interest and societal good may peaceably abide. For centuries thereafter, and not until the mid-20th, the debate over allocation of resources largely remained one of private versus public interest. A house, a ship, a business, these may be understandably privately owned. Unclaimed land, navigable waterways, the high seas, domains of the public; sometimes undefined altogether. Yet, shared spaces in which competing parties seek to extract some utility have long existed, most prominently in the form of grazing land and fisheries.

The descriptive term 'commons' became popular in 1968 when ecologist Garrett Hardin wrote his now infamous *Tragedy of the Commons* for *Science* magazine. Hardin's *Tragedy* refers most directly to an economic problem related to the efficient allocation of scarce resources, especially within shared, public environments. Hardin's article deals

squarely with the most extreme kind of commons problem, viz. the Malthusian trap. The tragedy as he saw it was the harmful effect of exponential population growth on Earth's resources. His paper served to frame the problem of resource management, giving life to the concept of common pool resources as generally anarchic situations where the extraction of materials is zero-sum, and participants may not be easily excluded. Though not explicitly attributable to Hardin, *Figure 1* shows the expansion of exchange type variation that occurs between the qualities of subtractability and excludability across four categories: public goods, club/toll goods, private goods, and common pool resources. Hardin's ultimate assessment, crucial to the research that would follow, was rather dire in that common pool resources, though momentarily distinct, are destined for either government control, complete private ownership, or spiraling degradation. Hardin reveals his own extreme convictions, ultimately adjudging that "Freedom to breed will bring ruin to all"[26] before launching into a proto-Skinnerian salvo on mass coercion while making some reasonable points about the annoyance of supermarket Muzak. There's got to be a better way.

		Subtractability	
		Low	***High***
Excludability	***Low***	Public Goods	Common Pool Resources
	High	Club/Toll Goods	Private Goods

Figure 1

Figure 1 Note: It is important to recognize that this discrete representation belies the fact that massively dispersed, complex systems may at any particular time, exhibit qualities of one, more than one, or even none of the categories described.

As a brief interlude and motivating example for thinking about the categories of property interaction from the physical world (though it does offer Wi-Fi), consider the aptly named Boston Common, a 50-acre park, which sits across from the great gold-domed State House in downtown Boston, Massachusetts. Founded in 1634, it is the oldest public park in the United States. It is owned by the City of Boston and managed by the Boston Parks Department. Boston Common is generally recognized as public property. Anyone may freely enter, making it difficult to exclude any particular member of the public. And one person's enjoyment of the park does not necessarily take away from the enjoyment of anyone else. In the language of commons analysis within the school of New Institutional Economics, Boston Common would be said to exhibit low excludability and low subtractability. For some, this would end the investigation. This is clearly public property. However, the Common is technically closed between the hours of 11:00 PM and 5:00 AM and violators of those bounds may be cited for trespassing. This increases excludability and moves the Common from public property towards a club good. Yet, even during normal hours of operation, not all of Boston Common is equally desirable ground. There are two tennis courts with a fence around them that operate on a first come, first serve basis. In theory, excludability is therefore low while subtractability may be high if one is forced to wait for a court. The dynamism of economic systems and spectrum of commons analysis is a recurring theme in this paper.

Wittingly or otherwise, *The Tragedy of the Commons* threw down the gauntlet for others to find a more reasonable solution. It does so most pointedly in its restatement of Wiesner and York's assessment that the nuclear arms race posed a dilemma with "*no technical solution*."[27] Hardin defines a technical solution as "*one that requires a change only in the techniques of the natural sciences, demanding little or nothing in the way of change in human values or ideas of morality.*"[28] There are many juxtapositions that can help codify meaning behind Hardin's words. Hard versus soft sciences. Science versus art. Objective versus subjective. False dichotomies these may be, but they remain useful heuristics. Problems that lend themselves to precise control and experimentation by limitation of variables are those with technical solutions. Problems too unwieldy for the laboratory due to imperfect information, belief-based assumptions, and high variability (even given consistent application of processes) may be recognized as those without technical solutions.

Hardin illustrates the utility of thinking outside the bounds of technical solutions with an example from the game of tick-tack-toe [*sic*], offering a situation in which an opponent has perfect information about the game (i.e. total knowledge of the set and sequence of all opponent moves). He notes that, for any challenger, winning in such a case would be impossible. The opponent, having perfect information, would know exactly where to move every time in order to guarantee a win. The game would be unwinnable *unless* the challenger were to step outside the bounds of the game as it were understood and rewrite the definition of winning altogether. For a modern example, if supercomputers beat the world's best human chess players 100% of the time, then humans could simply exclude computers from competition, preserving the ability for humans to claim

dominance. Given recent advancements in artificial intelligence technology, one might see such a rule as a form of cheating, but preclusion of non-human entities from human competition is the rule rather than the exception. Deep Blue and AlphaGo are interesting modern exhibitions, but do not in any way seem to threaten the official standings of Magnus Carlsen or Tang Weixing.[29]

So, it is apparent that the class of "no technical solution" problems necessitates a sort of gamesmanship in the game making itself; certainly, with the playing. What that means for the management of common pool resources is that it may be as much an art as it is a science, echoing the Aristotelian sentiment that "*art is the study of things with starting points in the producer and not the thing being produced*."[30] Wiesner and York's challenge of understanding the atmospheric and biological effects of nuclear tests differed entirely from the development of an international system that could control the testing itself by imperfect and irrational humans. They were the first to make the case that technological solutions to this latter set of problems would spell doom. Nevertheless, it is critical to recognize that Wiesner and York ended their 1964 article on an optimistic note. They were hopeful that the partial nuclear test ban treaty would be a first step toward solving the security dilemma; international agreements offering solutions not otherwise found in the hard sciences that split the atom. Decades later, historian Richard Rhodes would call the [partial test ban treaty] and non-proliferation treaty the "most effective treaties in preventing rampant nuclear proliferation."[31] Recognizing the fear that paralyzed generations during the Cold War, the idea that treaties and similar governance models can provide viable solutions (in some cases, perhaps the only ones) to preventing international conflict is an historical lesson worth heeding.

A New Hope: Elinor Ostrom and Institutional Analysis

If *Tragedy* set out to quell the optimism of Wiesner and York, it served only to ignite interest in one young scholar in particular: Elinor Ostrom. Having received her PhD in political science from UCLA three years prior to Hardin's publication, Ostrom, along with husband Vincent, was already laying the groundwork for a way of managing the commons. A review of Ostrom's early academic interests provides insight into the evolution of her thinking in terms of organized systems, management of exchange, and how to approach common pool resources. In 1965, she published *A Behavioral Approach to the Study of Intergovernmental Relations*. In 1968, *Constitutional Decision-Making: A Logic for the Organization of Collective Enterprises*. And in 1971, *A Theory for Institutional Analysis of Common Pool Problems*. The breadth of Ostrom's research, from fisheries to forests to irrigation practices, demonstrates the prevalence of common pool resource issues as well as the applicability of the methods she devised. This quality of abstraction is perhaps best demonstrated in her work with law enforcement.

In fact, some of the earliest rudiments of what would become her Pietic contribution, the Institutional Analysis and Development framework, can be found in her 1978 work with Parks, Whitaker, and Percy, *Formation of Police and Law Enforcement Policy.*[32] Ostrom's work cast serious doubt on Hardin's tragic assertions, becoming the chief proponent for the notion that common pool resources could be sustainably managed by their own participants. The IAD framework fleshed out in the early 1980s, harmonized three key areas: common pool resource management, game theory, and collective action.[33] In 1985, Ostrom published *Formulating the Elements of Institutional Analysis* as part of a

collection of essays edited by her and Vincent, entitled *Studies in Institutional Analysis and Development*.[34] Her essay in particular makes the case for concentrated, empirical study of institutions by presenting the need to do so and supplying the foundational elements thereof (these elements are defined and described in greater technical detail in the forthcoming Methodology section of this paper). The need, according to Ostrom, centers on interdisciplinary coordination.[35]

In 1990, Ostrom published her seminal work, *Governing the Commons*. In it, she presents possible ways of overcoming the tragedy of the commons, primarily by means of self-organization and self-regulation, noting *"some individuals have created institutions, committed themselves to follow rules, and monitored their own conformance to their agreements, as well as their conformance to the rules in a CPR situation."*[36] She is explicit, however, that there are no simple, or even elegant solutions to the problem of allocating resources in a commons situation. Ostrom addresses proponents of privatization as well as those who believe in a more command economy-style approach, citing each as potential solutions within a larger set of solutions based on specific problems. In her own words, *"Instead of presuming that the individuals sharing a commons are inevitably caught in a trap from which they cannot escape. I argue that the capacity of individuals to extricate themselves from various types of dilemma situations varies from situation to situation*."[37] This should not be construed to mean that commons problems cannot be abstracted in some sense or that they are intractable. Indeed, Ostrom made significant progress in the meta-analysis of CPR research and would come to reconcile challenges of high variability within the analytical concept of polycentricity. In short, that social systems in particular tend to

be recursively nested and woven together in ways that do not comport with simplistic linear or hierarchical views.[38]

Since Ostrom's work in the 1970s and 80s, the Institutional Analysis and Development framework has become one of the central tools in the field of New Institutional Economics for understanding how institutions governing the commons can operate sustainably and efficiently. The framework is essentially similar to a mathematical function, defining the inputs, operations, and outputs of a particular governance regime. Translations to IAD terminology follow:

- Inputs
    - Biophysical/Material Characteristics
    - Attributes of the Community
    - Rules
- Operations
    - Evaluative Criteria
- Outputs
    - Patterns of Interaction
    - Outcomes

Yet the IAD goes beyond basic input/output, defining not only the function of the institution in question, but also the situation to which it is specifically tailored. In technical terms, this is referred to as the Action Arena, which is made up of Actors and Action Situations. Defining all of these attributes reduces variability, making empirical analysis

more accessible. Additionally, the IAD incorporates feedback loops making it possible to turn otherwise static governance systems into teachable institutions.

While various visual representations exist based on interpretations of Ostrom's research, this paper will rely on *Figure 2*[39] for analysis[40]:

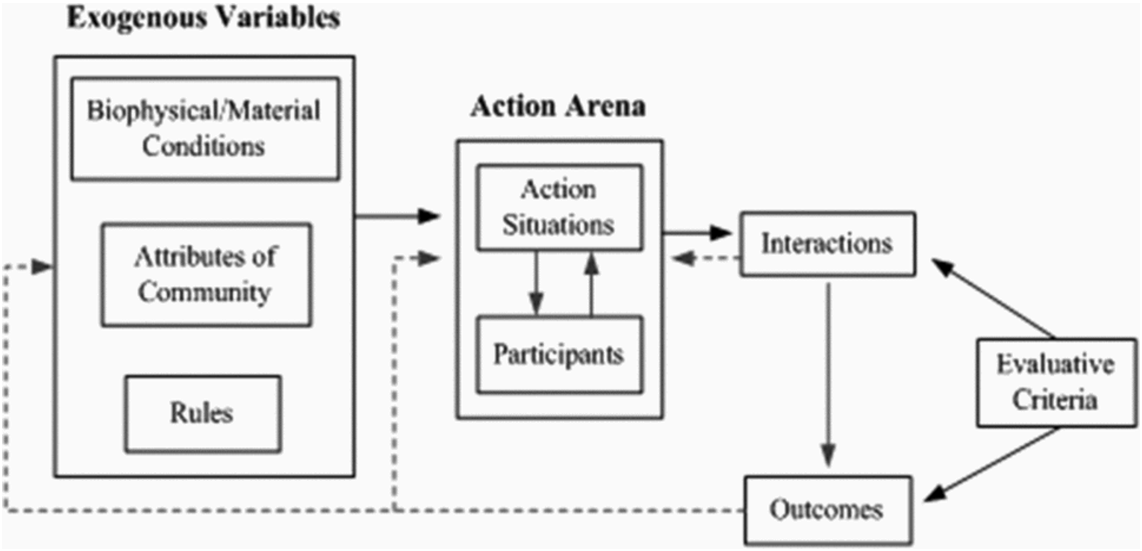

Figure 2

A brief recap of the situation thus far. For centuries, economists have attempted to understand the nature of property ownership and interactions among those who have interest in said property, viz. the extraction of some utility. Until the mid-20th century, this conversation was generally binary, explaining ownership and access as either public or private. The introduction of the commons opened the door for a more nuanced view, recognizing anarchic systems where individuals interact to gain utility but seek no private ownership, thereby ostensibly leading to greater collective benefits of use. Hardin viewed

this as necessarily destructive given man's self-serving nature and called for extreme measures to control societal behavior.

Ostrom countered this assertion, positing her own view, backed by field work, that commons can be effectively governed by their own participants. She produced the Institutional Analysis and Development framework to aid in the evaluation of economic systems (i.e. systems of exchange). It by application of the IAD that researchers can better understand and evaluate the mechanics of a particular system and predict outcomes.

The following section introduces modern research and uses reason by analogy to tie the key common pool resource concepts to problems in cyberspace, viz. cyber warfare.

Cyberspace as a Commons

A crucial point to make at this juncture is that while Ostrom's work centers on the effective management of common pool resources, the IAD is by no means limited in its applicability to a particular kind of analysis. The reason that common pool resources are interesting likely comes down to the relative novelty of CPRs in economics, their ambiguous governance logic, the Nobel Prize committee's recognition of Ostrom's work, and, realistically, Hardin's pithy phrasing. However, the IAD could reasonably be applied to any private situation, public situation, or club situation. Similarly, as will be shown in this section, some have taken to vociferously advocating or decrying the analysis of cyberspace as a function of common pool resource management. A central premise of this paper is that complex systems lend to a variety of kinds of analysis and mutual exclusion approaches Ostrom's admonishments about panacea thinking. Ultimately, the four categories in *Figure 1* are better thought of as lenses than boxes. There is a deliberate

choice here to view cyberspace through the lens of CPR governance because situations specific to cyber warfare do in certain circumstances exhibit those hallmarks of high subtractability and low excludability. Opposing views are presented here as an exercise of due diligence, but also to call attention to the problem of monolithic analysis.

In 2012, venture capitalist and former Intel executive Bill Davidow wrote a 730-word missive for the Atlantic entitled, *The Tragedy of the Internet Commons*.[41] In it, he asserts the efficiency of free markets and the surety that commons open to free markets are necessarily doomed to destruction, attempting to envision what Hardin would think about the internet. Davidow initially traverses physical and cyberspace, hypothesizing that digital retailers siphon revenue from the physical "bricks-and-mortar commons."[42] His main point, however, centers on the issue of privacy, reiterating Hardin's warning to make a point about the impossibility of self-regulation and the need for privacy laws in the United States to rival those in Europe.

Countering Davidow's arguments, Mark Raymond, writing in 2013 as a fellow at the Centre for International Governance Innovation, penned *Puncturing the Myth of the Internet as a Commons*. In it, he posits that Davidow's first point has more to do with normal business practices than destructive forces related to overuse of a commons. The point about privacy is considered moot because the mere existence of costs (as in time to filter spam) does not necessitate a commons situation. Raymond's first point makes sense. It is strange indeed to compare the cannibalism of physical retail by online shops to be in any way related to even modern interpretations of the commons. That does not necessarily exclude it from the realm of possibility, but Davidow positions it as a function of the *internet* as a commons. Davidow would find more purchase analyzing the *online retail*

function itself as a kind of commons, relying on models such as Porter's Five Forces to explain the effect of new entrants on a market. And even on that face, little purchase would the argument find, unless Davidow could demonstrate that too many entrants to the digital marketplace cause customer burnout, driving away online sales. Davidow's privacy argument is much stronger than Raymond gives credit. For one, the argument is not primarily concerned with costs incurred as a result of spam. If privacy can be unitized, then it can be measured as a function of subtractability. That would at least make it more likely to be a matter of either private property or common pool resources. From there, and well beyond the scope of this paper, one would have to determine how excludability works to increase and decrease privacy. If one feels their privacy is decreased by some online activity, does self-exclusion increase privacy? What are the systemic effects of data-as-a-service (DaaS) companies on the ability for one to manage his or her privacy? These are questions worth investigating and Davidow is clearly attempting to start the conversation (or at least he was in 2012). The most egregious error in Davidow's piece is the complete disregard of 40 years of research since Hardin's *Tragedy*.

Raymond's *Puncturing the Myth* quickly moves past Davidow, contending primarily that while a commons must exhibit rivalry (i.e. zero-sum subtractability) and excludability, the internet does neither.[43] Raymond wisely borrows from thoughts expressed by both Hardin and Ostrom about pollution, presenting the example of congestion as one way that the internet could theoretically become rivalrous. However, he offers that a simple solution may be found in building out infrastructure and generally improving technology. He goes on to point to several ways in which internet participants may be excluded from use, including the example of the so-called "Great Firewall of

China" and distributed denial of service (DDoS) attacks. Curiously, some of Raymond's arguments suit their own needs as they arise. For instance, if the solution to congestion is to simply "build more physical infrastructure,"[44] yet participants may be easily excluded from the internet through the destruction of infrastructure (as Raymond asserts[45]), then every situation has a solution and the problem loses its bounds. One arguing for thinking of the internet as a commons would be burning infrastructure to create rivalry while building it for non-excludability. One arguing against thinking about the internet as a commons would be building infrastructure for non-rivalry and burning it to keep people out. The phrase self-licking ice cream cone finally makes sense.

Raymond's contrarianism might be too quick to make a point where better framing of the issue would have improved its fidelity. His argument is correct in its focus on the language of commons analysis, where rivalry is a function of *subtractability*, positioned orthogonally to *excludability*. However, his ultimate assessment that the internet is more akin to a set of nested clubs is unnecessarily limiting. Certainly, in some aspects, the internet may exhibit qualities of clubs, and those clubs may well be nested. But as desirable as an elegant nomenclature may be, it does not accurately capture the polycentric independence of various exchanges having to do with cyberspace. The internet is a massive and unique combination of physical infrastructure, digital transmissions, personas, and abstract concepts. Analyzing it as a monolithic set in any regard is unproductive and leads, as Raymond's paper demonstrates, to recursive exceptionalism; hemming and hawing. The overwhelming majority of commons research does not examine all arable land as a commons but narrows its focus to a specific plot of land for which subtractability tends to

be high and excludability low. In fact, it was Hardin who attempted to solve for the entirety of the biosphere as a commons and it led to an appeal for forced sterilization.

The task, then, is not to answer *if* cyberspace is a commons, but to posit *when* and *where* cyberspace exhibits elements of a commons, given a particular context. When framing the internet as a domain of warfare, one focal area fits the definition of a commons exceedingly well: internet-connected industrial control systems (ICS). These systems are used around the world to automate processes in large-scale utilities, manufacturing facilities, oil & gas operations, and infrastructure controls; not to mention localized deployment in commercial transportation vehicles such as ships and airplanes. In a sense, the growing adoption of ICS, is creating a commons for nation-states to exploit. This results in a situation where any nation-state may endeavor to attack any ICS (low excludability) and the successful exploitation of an ICS results in at least the exploit (in a technical sense), but potentially the entire system, being made unavailable to other nation-states (high subtractability), most importantly the host nation. In other words, the proliferation of internet-connected ICS may be "stocking the pond" for cyber warfare.

Another example of a commons situation specific to cyberspace and cyber warfare is in the development and use of zero-day vulnerabilities (0-days). The U.S. National Institute of Standards and Technology (NIST) defines a zero-day attack as one that "exploits a previously unknown hardware, firmware, or software vulnerability." Major attacks like Stuxnet can take advantage of numerous zero-days at once, showing a propensity for some to stockpile and chain 0-days for complex operations. Of course, software vulnerabilities tend to be a rule of coding rather than an exception, and developers are regularly issuing patches so that users are guarded against flaws and exploits. However,

there are situations when an attacker is able to find a vulnerability and maintain its secrecy long enough to develop an exploit, deliver a payload, and compromise a system. Here, only upon discovery of some intrusion can a developer eventually determine that there is a vulnerability and issue an appropriate fix. The ubiquity of software makes it virtually impossible to exclude anyone from analyzing code for vulnerabilities, and the limited-use nature of 0-days gives them the quality of high subtractability. The global availability yet extremely limited use of 0-days makes them one of the truly novel issues related to cyber warfare. Imagine 20 ships enter a fishery and all 20 ships catch a single fish. They are all able to view and touch and smell the fish on their own ships. The following day, 19 ships come to find that their fish have rotted because the captain of the 20th ship had a nice, big dinner. Also, the power is now out in Ukraine. Such is the new commons of cyberspace and cyber warfare.

The point of introducing these examples is not to narrowly define a perspective that will necessarily carry across each of the governance models under review — though it is presented because it closely aligns with problems of physical aggression that concern those discussing cyber warfare. Rather, it is to demonstrate how problems related to the internet and cyber warfare can and do take on characteristics such that individual situations can reasonably be considered common pool resources. This lays an important foundation, providing specific reasoning for selection of the Institutional Analysis and Development framework. It is difficult to overstate the high degrees of complexity, variability, and subjectivity in interpreting cyber warfare as a problem of the commons. Yet, hopefully the explanations of the strategic and economic implications of ICS and 0-days removes any doubt that it is feasible. Recall Raymond's allusion to the congestion problem. This is an

often-overlooked converse perspective on the commons that strengthens the case for cyber warfare as a common pool resource issue. It was Hardin who said in *Tragedy*, *"…the air and waters surrounding us cannot readily be fenced, and so the tragedy of the commons as a cesspool must be prevented by different means, by coercive laws or taxing devices that make it cheaper for the polluter to treat his pollutants than to discharge them untreated.*[46] In international relations terms, this means that in order to prevent that most pollutinous practice of warfare, nation-states must find it less costly to resolve political matters diplomatically than to conduct violent cyberattacks.

There are three key takeaways from the preceding sections. First is that cyber warfare is worth analyzing and discussing, if not for that most important endeavor of preserving peace and human life, then because so much remains unknown even as some are attempting to establish norms and governance regimes for its proper management. Second is that certain aspects of cyberspace do comport with traditional notions of the commons and an especially relevant concept is that of subtraction by addition or pollution. Third is that the field of economics and especially the discipline concerning analysis of common pool resource management has a framework capable of analyzing the likely success and sustainability of a governance system.

METHODOLOGY

The primary objective of this research is to assess the likely effectiveness of two of the most prominent cyber warfare governance models in existence today: the Tallinn Manual and the Digital Geneva Convention. While each model will be assessed against self-stated or implied objectives, the overarching question remains one of how best to inculcate global norms of cyber warfare in order to maximize the security of noncombatants by minimizing physical injury to them.

One of the most brilliant aspects of Ostrom's work in developing the IAD is in her commitment to ensuring its broad and successful application. In addition to the establishment of the Ostrom Workshop at the University of Indiana and continuing rigorous field work throughout her life, she provided an instruction manual for how to set up a study using the IAD framework. This paper therefore adheres to this guidance, which is published as *An Institutional Framework for Policy Analysis and Design by Margaret M. Polski and Elinor Ostrom*.[47]

The research design follows seven steps:[48]

1. Define the policy analysis objective and specify the analytic approach
2. Analyze physical and material conditions
3. Analyze community attributes
4. Analyze rules

5. Integrate the analysis (in process with both Tallinn Manual and DGC)
6. Analyze patterns of interaction
7. Analyze outcomes

Each model will be independently fit to the IAD framework as shown in *Figure 2* using explicit elements from proponent discourse and implicit derivations from public exposition. To the greatest extent possible, questions posed in each step of the research design will be controlled so that analysis remains model independent. However, this is not a comparative study and the differing nature of the models may necessitate some variance in the lines of questioning.

Definitions

First and foremost, a few words on words. Arguably, the most important definition related to this research is that which forms an understanding of the term cyber warfare. Whereas definitions for framing the models in question are taken from existing IAD literature and specific technical definitions are taken from the models themselves, the notion of a cyberattack in the context of cyber warfare must be dealt with here and now. Since the DGC offers no explicit commentary on the matter and the Tallinn Manual devotes nearly six pages to the topic, the following definition applies to references made by both models:

Cyberattack (also, cyber attack) — As defined by Rule 92 in the Tallinn Manual 2.0, a [cyberattack] is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.[49]

Since there is little in the way of official definitions of cyber warfare, this research refers to such conduct as that in which one nation-state actively employs one or more cyberattacks against another nation-state in pursuit of political objectives.

The following definitions serve three purposes. The first is to clearly define each variable found within the IAD in order to establish the nodes for logically mapping attributes of each individual model. The second is to provide a greater sense of context around the variability across each variable. The third is to highlight how each variation of individual variables will be handled for the purposes of this research. In order to maintain consistency with existing literature, other than a few exceptions, the definitions below are generally attributable to the same source, viz. MD McGinnis's *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework.*[50]

Framework — Identifies, categorizes, and organizes those factors deemed most relevant to understanding some phenomenon. [51]

Theory — Posits general causal relationships among some subsets of these variables or categories of factors, designating some types of factors as especially important and others as less critical for explanatory purposes. [52]

Model — Specifies the specific functional relationships among particular variables or indicators that are hypothesized to operate in some well-defined set of conditions. [53]

Institutions — The set of working rules that are used to determine who is eligible to make decisions in some arena, what actions are allowed or constrained, what aggregation rules will be used, what procedures must be followed, what information must or must not be provided, and what payoffs will be assigned to individuals dependent on their actions.[54]

The Tallinn Manual and the DGC are best understood as models of institutions. Those institutions may be customary international law, the Geneva Conventions, governance scholarship, etc. It would be premature to say that either model is yet accepted as a set of working rules for the absent conduct of cyber warfare.

Polycentricity — a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes. [55]

Exogenous Variables — Designates variables that appear in an economic/econometric model but are not explained by that model (i.e. they are taken as given by the model).[56]

Biophysical/Material Conditions — The biophysical or material conditions denoted in each model describe the nature of the good or physical/material conditions. There are two defining characteristics of goods and services: Subtractability (i.e. Does

A's consumption of a resource lower B's potential enjoyment thereof?) and Excludability (i.e. How costly is it for A to exclude B from the resource?). These characteristics are typically viewed orthogonally to one another with subset measurements of high and low. Based on the degree of highness or lowness, entities can be categorized thusly:

- Low Subtractability and High Excludability: Public Goods
- Low Subtractability and Low Excludability: Toll or Club Goods
- High Subtractability and High Excludability: Private Goods
- High Subtractability and Low Excludability: Common Pool Resources

For each of the models, the Biophysical/Material Conditions are such that the governance of cyber warfare includes the conduct of cyber warfare, where high subtractability is evident in three key areas: physical harm to noncombatants, destruction of physical systems, and global security in general. And excludability is low given the hyperconnected nature of the internet, amplified by problems associated with attribution and non-repudiation. The exogenous nature of human life, ICS, and security become endogenous when analyzed in the context of the Action Arena.

Attributes of Community: This is a summary term used to designate all relevant aspects of the social and cultural context within which an action situation is located. Key themes are trust, reciprocity, common understanding, and social capital. [57]

Because neither the "community" nor the "attributes" thereof are explicitly defined by either model, in order to normalize analysis, this research introduces a novel and modified interpretation of the Clausewitzian Trinity[58], hereafter referred to as *Figure 3*. This modern take on an easily recognizable model serves to marry the disciplines of military strategy and economics while providing a quick reference for thinking about relationships within the relevant communities under review.

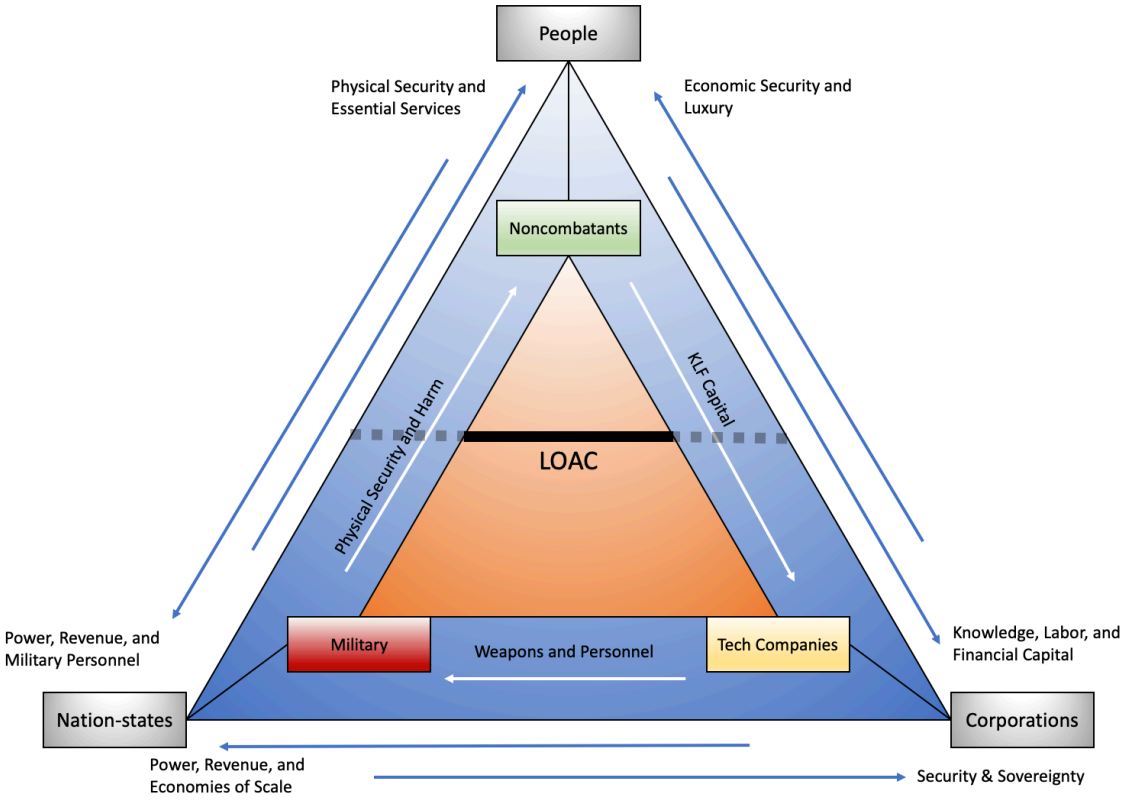

Figure 3

Rules - Rules that specify the values of the working components of an action situation. While McGinnis presents seven distinct kinds of rules, this research does not specifically address each in kind. Rather, it seeks to identify rules of each institution and

rules that come as a result of the creation of those institutions. In other words, rules for development process may be as or more important (in this anticipatory state) than rules-in-use.[59]

Action Situations – This is the core component of the IAD Framework, in which individuals (acting on their own or as agents of organizations) observe information, select actions, engage in patterns of interaction, and realize outcomes from their interaction. [60]

The Action Arena - The action situation is the "black box" where operational, collective, or constitutional choices are made. [61]

Participants – Includes the parties acting upon and constrained by the elements of excludability and subtractability. [62]

Interactions and **Outcomes** - Denotes the pattern of interactions among resource users and the particular resources upon which their livelihood relies; both the social and the ecological components of this focal action situation can be decomposed into smaller components as well as situated within the context of broader aggregations.

Evaluative Criteria - Evaluative Criteria may be used by participants or external observers to determine which aspects of the observed outcomes are deemed satisfactory and which aspects are in need of improvement. [63] Each criterion will include an

assessment of high (green), medium (yellow), low (orange-red), or NA (white), along with a brief rationale. The following chart provides an example:

Evaluative Criteria	Sample Ratings (Low, Medium, High)
Efficiency in use of resources, especially capture of economies of scale	High – Proven viable at multiple levels
Equity in distributional outcomes and processes	High – Maximizes utility of all stakeholders
Legitimacy as seen by participants in decision processes	Medium – National but not international recognition
Accountability, especially to direct users of resource	Medium – Rules in place but little enforcement
Fiscal equivalence: the extent to which the beneficiaries of a public good or service are expected to contribute towards its production	Low – Undue fiscal strain on unrelated parties
Consistency with the moral values prevalent in that community	Low – Values are at odds with affected community
Robustness or resiliency	NA – Not enough data to evaluate

Limitations

This research is subject at least to the following limitations, biases, and assumptions:

- **Faulty premise** - This research assumes that cyber warfare is a possibility. If Johns Hopkins Professor Thomas Rid is correct, then *Cyber War Will Not Take Place*.[64] Dr. Rid is not alone in his assertion, buffeted by Gartzke's *The Myth of Cyberwar*.[65] If this is the case, then developing rules to prevent cyber war would be a waste of time and this analysis would be an even greater waste of time.

- **Many rivers to the sea** - The Institutional Analysis and Development framework is not a guarantor of success any more than a historically successful business model or war strategy is a guarantor of success. Instead, it is to be understood as a guide for delineating the various parts of systems that tend to fall into particular categories, enabling some degree of rigorous analysis. Nevertheless, there are bound to be those who misinterpret the evaluation as in some way definitive. The best that this research can ever do is to gently guide the conversation.
- **The recursive prison of polycentricity** – Drawing conclusions about interconnected social systems necessarily calls for a kind of hypervariate analysis that could go on without terminus. Where termini exist in this research, they have been placed either by the analyst or that most joyous constraint of time.
- **No one asked for this** - Neither the Tallinn Manual nor the Digital Geneva Convention makes any reference to development using the IAD framework as a guide. Therefore, fitting these governance frameworks to the IAD is necessarily deductive and will require some degree of subjective assessment and good judgment. That judgment is and ought to be open to interpretation, and the research welcomes disconfirmation.
- **Post hoc cum/ergo propter hoc** – So long as nation-state behavior aligns with explicit norms, it can be difficult to disprove success of those norms. Dangers of correlation, causation, etc. This does not necessarily mean that the norms earn the benefit of the doubt, but it does call for additional theorizing about the causes of peace when war is an option.

- **High degree of subjectivity** – The IAD requires some degree of artistry in application. That, combined with the complexity of global governance issues and the uncertain of what the future will bring, increase the chance of bias affecting interpretations or findings.

GOVERNANCE AND ITS APPLICATIONS IN CYBERSPACE

One of the major areas of study within New Institutional Economics is the interplay between institutions (formal and informal rules) and the individuals, organizations, and interactions that they govern. A key takeaway from Ostrom's research is that commons can be effectively governed while maintaining the attributes that make them a commons in the first place. She uses the entirety of the third chapter of *Governing the Commons* to demonstrate situations of successful and sustainable self-governance. This is encouraging for local problems as those principles of success may be applicable on a global scale. This section provides a brief overview of the concept of governance as understood within the discipline of international relations. Though, the interdisciplinary leap isn't as great as it may at first appear. There are important points from IR scholarship that are useful for thinking about applying Ostrom's local economic success stories to interactions between nation-states, including the conduct of war.

Global governance can be defined as "the collective effort to identify, understand, and address worldwide problems that are beyond the capacity of individual states."[66] Perhaps one of the best examples of polycentricity as it relates to governance is found in the introduction to Ann-Marie Slaughter's *A New World Order.* There, she describes an ideal in which global governments would be interconnected in a latticework that would look like the globe atop Lee Lawrie's *Atlas* sculpture in Rockefeller Center. She describes this as a "world of government networks" with the promise of greater

effectiveness and justice than "a set of global institutions perched above nation-states enforc[ing] global rules."[67] It can be easy to think of governance purely as a function of the state; however, states are not alone in the development, proliferation, or even enforcement of governance mechanisms.[68] Non-governmental Organizations (NGOs), think tanks, academic institutions, corporations, and individuals are all potential participants. Citing Martin Shapiro, Slaughter discusses the presumptive duty of private actors in upholding the public trust as new members of global policymaking. Shapiro himself states that moving from govern*ment* to govern*ance* can erode boundaries between what is in and outside of government.[69]

Consider the deployment of far-reaching standards such as the fifth generation of wireless technology. Deployment of 5G networks has necessarily been a joint effort between corporations responding to consumer demands, governments responding to the desires of their constituents (along with the promise of increased soft power), and international alliances that manage the use of 5G networks across borders to comport with differing legal requirements. The case of Huawei and Euro-American adoption of 5G is instructive as to how even low-level international conflict can influence governance decisions and project onto private industry the politics of the state.

The Evolution of Governance in Cyberspace

The purpose of this section is to provide a brief review of how governance has evolved in cyberspace, from notional circumstances supported by concerns over U.S. national security to an international, polycentric practice covering topics ranging from physical hardware to intellectual property theft. Interestingly, the current focus on cyber

warfare brings governance full circle, even as it has expanded in scope. Technological advancement pairs neatly with matters of global governance. There is perhaps no better example of this than the internet. What began under the auspices of the United States Department of Defense through its Advanced Research Projects Agency and relying upon connections between the University of California, Los Angeles and the non-profit Scientific Research Institute (SRI) International, now connects tens of billions of devices in every country on earth.

Initially, governing the internet was a largely technical matter, the responsibility for which lay with its creators and early adopters in government and academia. True codification of standards began in 1986 with the forming of the Internet Engineering Task Force (IETF), followed in 1988 by the Internet Assigned Numbers Authority (IANA), and most prominently in 1998 by the Internet Corporation for the Assignment of Names and Numbers (ICANN). On the last point, former U.S national security official Richard Clarke has shared his skepticism that, "*ICANN demonstrates [a] vulnerability of the Internet, which is governance, or the lack thereof. No one is really in charge.*"[70] Yet even ICANN boasts four advisory committees, including internet users and governments. All of these organizations have focused on establishing technical norms to increase international adoption. They were not, however, built to address rising issues of nefarious use of the internet. The vast majority of governance in cyberspace has thus far been legislative.

The earliest attempts to govern the use computer systems predate even webpages. In the United States, the Computer Fraud and Abuse Act of 1986 (CFAA) classified for the first time computer crime as separate and distinct from mail and wire fraud. The

nuanced nature of and capabilities afforded by interconnected computers required new and specific kinds of regulation. It is nevertheless important to remember that the CFAA arose not out of an immediate need to address any particular problem, but in reaction to a Hollywood film. Fred Kaplan opens his book Dark Territory with the story of how, in 1984, President Reagan was compelled by the movie WarGames to ask about information systems and associated threats to national security. Understandably, the president was concerned that a hacker could launch an ICBM with the stroke of a key. Then-Chairman of the Joint Chiefs of Staff, General John Vessey, reported back to the president that the "problem is much worse than you think."[71] Soon thereafter, on September 17, 1984, the Reagan Administration published the National Policy on Telecommunications and Automated Information Systems Security or National Security Decision Directive Number 145 (NSDD-145). The document laid the foundation for what would become the CFAA. Since the time it was signed into law, the CFAA has been amended no fewer than nine times to extend its reach. New provisions have included extended protection for the financial sector, elimination of the need for intent in the use of classified information, new definitions of "damage," increased penalties for state computer crimes, expanded protection to "extraterritorial" computer systems, and even broader coverage in the private sector, among others.[72]

Over the same time period, other nations have sought to enact similar laws governing the use of computers and access of systems via the internet. The United Kingdom passed the Computer Misuse Act of 1990, which, like the CFAA, is regularly amended. Singapore has its own Computer Misuse Act, first passed in 1993. In 1997, China enacted the Computer Information Network and Internet Security Protection and

Management Regulations. And in 2007, the Council of Europe (CoE) hosted the Budapest Convention, which produced the first international treaty to bring concordance to the many individual national laws that had emerged over the interceding decades. The treaty was successful not only in its acceptance and ratification by European Council members (inclusive of many nations not otherwise members of the European Union), but also by prominent non-CoE states such as Australia, Canada, Israel, Japan, and the United States. These individual and collective efforts have made abstract concepts like cybercrime more tangible in the minds of political leaders, law enforcement officials, and individuals alike. However, an unintended consequence has been the implicit and deepening commingling of cybercrime with broader national defense and acts of war.

Use of the CFAA to prosecute both civilians committing petty crime and representatives of nation states attempting to breach government networks illustrates a kind of legal scope creep that opens wide the interpretation for oft-misunderstood actions. One of the most infamous and controversial cases involving the CFAA was the 2011 prosecution of Aaron Swartz, a software developer and co-founder of the popular news and culture website Reddit. That year, Swartz was caught downloading academic articles using the network at the Massachusetts Institute of Technology (MIT). Prosecutors assumed that his intention was to distribute the articles for free via peer-to-peer networks. Swartz was charged with 11 violations of the CFAA, which carried possible penalties of up to $1 million and 35 years in federal prison. Two days after being denied a plea bargain in the case, Swartz hanged himself.[73]

Many have cited the theft of intellectual property (IP) as a threat to national security.[74] In a 2019 guest post for the Council on Foreign Relations, Erica Borghard of

West Point and Shawn Lonergan of consulting firm PricewaterhouseCoopers described how the United States had recently begun offensive cyber operations designed to steal Chinese IP in retaliation for Chinese groups allegedly stealing American IP, especially that which could impact national security.[75] Borghard and Lonergan specifically cite indictments issued in 2018 by the United States government concerning the theft of information related to proprietary technology from various private firms as well as the National Aeronautics and Space Administration (NASA) and the Jet Propulsion Laboratory (JPL).[76] Many of the statutes cited in the indictment relate to Chapter 18, Section 1030 of U.S. Code, the CFAA. Not only did the indictments against the suspected Chinese hackers include language like "victim," "advanced persistent threat," and "overcoming network defenses," the U.S. Department of Justice published a press release in December 2018 emphasizing the national security implications of the alleged Chinese hackers.[77] At the time, then-director of the Defense Criminal Investigative Service, Dermot F. O'Reilly said, "The theft of sensitive defense technology and cyber intrusions are major national security concerns and top investigative priorities for the DCIS.

In the case of Aaron Swartz, no such parallels were or have since been officially drawn to the need for preventing his alleged behavior in order to preserve national security. Therefore, it is reasonable to conclude that although the CFAA may have originated out of concerns for national security, it has come to serve a dual purpose (or more accurately taken on a superseding purpose) in settling more routine criminal and civil matters. None of this is to say that the concept of national security pertains only to the prevention of physical attack by foreign adversaries. In fact, there exists a continuum by which one nation may seek to conduct espionage and escalate to more overt criminal

acts to test defenses for the sake of staging an attack. However, nations must be especially watchful when dealing with information technology and security as it tends to compound abstract concepts. When it comes to speculation about the blurring of these lines, some scholars point to more perverse motivations. Political scientist and IP scholar Debora Halbert has written that, "the focus on the theft of intellectual property as a security issue helps justify enhanced surveillance and control over the Internet and its future development."[78]

This is a critical point and one which speaks directly to aspiring governors of cyber warfare. There is a great paradox in the juxtaposition between problem identification and solutioning. That is, that one may develop an idea of some potential problem and draw logical conclusions to its eventuality. However, the time between problem identification and the testing of a solution in real-time can be vast. Without periodic application of the proposed problem-solving mechanisms, there exists a practical vacuum that governors tend to fill with analogous application. The problem then is that these interim applications result in their own effects and their immediacy necessitates change moment to moment, all while the spectre of the original problem is yet to be seen in action. By responding to these moment-to-moment needs, the tendency to stray from original aim increases, as the farther a bullet travels from the muzzle of a rifle, the more chance it will be impacted by physical forces and the surrounding environment to be knocked off course. The paradox itself is that the interim actions serve to justify functionally and economically the continuance of wayward travel and barring some Socratic effort, one with potentially infinite downside, there is no mechanism for keeping

a movement on its trajectory. The following section illuminates this paradoxical gap by condensing more than 30 years of cyber warfare into a few vignettes.

The Aeonian Dawn of Cyber-physical Attacks

To date, the number of cyberattacks known to have caused physical damage remains at one.[79] The attack in question was discovered in 2010 by Belarusian malware analyst Sergey Ulasen.[80] At the time, Ulasen had a customer in Iran reporting that computers running Microsoft Windows were unexpectedly rebooting and producing what is known as the "blue screen of death," a situation in which a computer freezes, showing only a bright blue background on the screen. The code causing the problems came to be known as Stuxnet and it would forever change how nations and individuals viewed the cyber-physical divide. In a 2011 interview, Ulasen noted, "the complexity of Stuxnet's code...led us to conclude that this malware was a fearsome beast with nothing else like it in the world."[81] Cybersecurity reporter Kim Zetter describes the attack in her groundbreaking investigation *Countdown to Zero Day*, which not only walks through the complexities of the malware in question, but also lays out a strong case for who was behind the attack amid one of the most perennially challenging issues in cybersecurity: attribution.

As no one has yet taken responsibility for Stuxnet, the public has had to rely on technical and investigative reporting to understand what happened, who did it, and why. It is now generally believed that the covert Operation Olympic Games began in 2006 under U.S. President George W. Bush. This was in response to reports that the Iranian government was planning to resume uranium enrichment at its facility in Natanz. What

allegedly ensued was a top-secret multi-year campaign orchestrated by United States and Israeli intelligence services to infiltrate Iranian networks at Natanz and hijack automation systems to damage centrifuges used in the enrichment process. Over the course of many months, Stuxnet caused intermittent changes in the rotational velocity of the centrifuges until they broke. Because of certain nuances built into the malware to obscure its presence and actions, Iranian scientists grew increasingly confused about otherwise inexplicable operations, purportedly leading to internal turmoil and further disruption.[82]

There is a broad range of opinion on the effectiveness of Stuxnet, given the implied goal of degrading Iran's ability to produce enriched uranium. Stuxnet reportedly damaged about 980 centrifuges (at the time, one-fifth of the total) at the facility in Natanz.[83] A widely promoted estimation puts the amount of time that Iran's nuclear program was set back at two years; others put the time closer to a few months.[8485] In what may be the best indicator of the operation's long-term effectiveness, a 2011 report by the IAEA states, "*[the] rate of production of 3.5% enriched uranium at Natanz has dipped slightly, but continues to be among the fastest rates documented; [it] remains almost twice as fast as pre-Stuxnet (2009-2010)*."[86]

David Sanger was one of the first journalists to tell the story of Stuxnet and although the world hasn't seen anything like it since it did its damage in Iran, Sanger chronicled recent attempts by the U.S. to cause physical damage by cyber means in a series of 2017 articles, culminating in his 2018 book *The Perfect Weapon*. Mr. Sanger details evidence that the United States government has shown interest in a "left of launch" strategy for stopping missile testing by the North Korean regime, including a detailed plan that was presented by Raytheon at the 2015 Space and Missile Defense

Symposium. The plan in question goes so far as to promise cyber means of "sabotaging [missiles] on the factory floor."[87] According to Sanger, "the idea is to strike an enemy missile before liftoff or during the first seconds of flight."[88] However, no definitive link has been made between the "left of launch" initiative and North Korea's failed missile tests.

There is another story worth mentioning if only to put to rest claims that using software to effect physical destruction long predates Stuxnet. Several prominent books engaging in purported histories of cyber war include references to what may have been the 1982 explosion of the Urengoy-Surgut-Chelyabinsk gas pipeline near Tobolsk, USSR. The story originally appeared in former U.S. Air Force Chief of Staff Thomas Reed's 2004 memoir *At the Abyss: An Insider's History of the Cold War*. In it, Reed tells a second-hand story from Gus Weiss, a National Security Council member under President Ronald Reagan. As the story goes, the Central Intelligence Agency (CIA) infected computer chips with a "trojan horse" computer program designed to cause automation systems to malfunction. The malicious software "worked," supposedly causing pressure to build up in a portion of the pipeline, resulting in an explosion estimated to have been on the order of three kilotons. For reference, that force would have been equivalent to the 1917 Halifax Explosion in Canada, which leveled the entire village of Richmond, killing 2,000, or nearly a fifth of the explosive power of the atomic bomb "Little Boy," which in 1945 the United States detonated over Hiroshima, Japan, killing as many as 150,000.[89]

The story was met with outright denial by former Komitet Gosudarstvennoy Bezopasnosti (KGB) head of the Tyumen region Vasily Pchelintsev.[90] Not to be confined

to Russian sources, Zetter allows for the story's "apocryphal" status. Thomas Rid lays out a convincing criticism of the alleged plot in *Cyber War Will Not Take Place*. In 15 years, Reed's tale has yet to be corroborated by any officials or people familiar with the matter (Rid notes this to be especially damning for the story's veracity given declassification of supposedly related documents such as the Farewell Dossier, which described Western espionage on Soviet technology). Reed himself, in a 2010 interview with Zetter, left open the possibility that he was misremembering the situation, acknowledging "*I don't know if it really happened.*"[91] Now, that's non-repudiation. Such widespread detraction has not stopped others from retelling the story as a matter of fact. Notably, Richard Clarke mentions the incident in passing as a matter of fact in his book Cyber War, with no sourcing whatsoever.[92] Thomas Aquinas offers a charitable interpretation of the motivations behind this kind of storytelling: "Because philosophy arises from awe, a philosopher is bound in his way to be a lover of myths and poetic fables."[93]

The truth is that imagination has both established and thus far ruled the cyber arena insofar as it may be considered a new domain of warfare. In many ways, cyber war appears to be a self-fulfilling prophecy, foretold since the days of dial-up and consistently reinforced over the years with increasingly urgent promises of devastation: preconceivedly infamous cyber Pearl Harbors and cyber 9/11s; matters of "when, not if" from the very leaders of agencies purportedly developing, unleashing, and at times losing track of antecedent and enabling mechanisms for those kinds of attacks. It was Admiral Michael Rogers, then director of U.S. Cyber Command (USCYBERCOM) and the National Security Agency (NSA) who stated in March of 2016, "it is only a matter of

when, not if, you are going to see a nation-state, group, or actor engage in destructive behavior against critical infrastructure in the United States."[94]

Five months after that speech, a group called the Shadow Brokers began releasing a virtual arsenal of exploits linked to the Equation Group and associated Tailored Access Operations (TAO) unit at the NSA. It turned out that the NSA had been developing and stockpiling 0-day vulnerabilities and corresponding exploits, most notably the EternalBlue exploit, which led to a serious of global cyber events. In May of 2017, WannaCry ransomware spread to computers around the world by way of EternalBlue. The cryptoworm disproportionately affected England's National Health Service, locking systems and forcing the diversion of some patients from certain hospitals. The same exploit was used in the 2017 NotPetya ransomware, which brought several global businesses, most notably shipping company Maersk, to a standstill. If those warning the general public about the dangers of cyber-physical events are the same individuals leading organizations where code capable of causing them is developed and lost, then imagination is guaranteed to become reality. Who or what, then, can truly mitigate the risk of these types of situations?

Enter the Governors of Cyber War

The Tallinn Manual

On May 14, 2008, NATO established the Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia. The decision for its location was no coincidence. Beginning April 27, 2007, Estonia experienced a series of disruptive cyber events (commonly, if colloquially, "attacks") consisting mainly of coordinated distributed

denial of service (DDoS) campaigns against popular email and banking websites. The campaigns persisted over the course of 22 days and resulted in "temporary degradation or loss of service on many commercial and government servers."[95] Many then (as now) suspected Russian involvement as a form of retaliation for Estonia's moving of a Soviet-era monument to a less public place. In 2008, CCD COE founder Dr. Rain Ottis published an analysis of the events concluding that "the event can be explained as a Russian information operation against Estonia."[96] Though, he was careful to add, "It should be noted that this analysis does not prove that there was an information operation due to lack of evidence from the Russian authorities."[97] Another testament to the challenge of attribution; in this case arousing suspicion by negation.

Months after the establishment of the CCD COE, the Centre contacted Michael N. Schmitt to request he speak at a conference. In his own words, Schmitt denied the invitation because, "at the time, lots of folks were focusing on cyber, but no one had answers."[98] He offered that if the Centre would put together a project to start answering the many questions that were out there, he would be willing to participate. It took only a few more months for the CCD COE to once again contact Schmitt, offering him "carte blanche" to start answering questions about cyber warfare.[99] Soon thereafter, as director, Schmitt brought together the first International Group of experts to start a conversation around if, how, and when international law applies to issues of cyber warfare.[100]

Schmitt had been thinking and writing about cyber warfare long before Stuxnet was even a consideration. In 1999, he wrote an article entitled *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*. It was one of the earliest expositions on the implications that *jus in bello* would ostensibly have

on violent force delivered via the internet. In that paper, he lists as hypotheticals the derailment of trains and pirating of municipal traffic controls, among other scenarios. His initial assessment was that computer network attack is "war on the cheap" where barriers to entry are low and rewards are high. His conclusions began the mapping process of cyber events to implications within international law, specifically Chapter VII of the UN Charter (*Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression*). The same year that he published *Computer Network Attack*, Schmitt led a Naval War College Symposium to broaden the discussion (published in 2002 as Computer Network Attack and International Law in the Naval War College Journal of International Law Studies. Six years later, Schmitt would go on to become project director for the group that in 2013 and again in 2017 produced the Tallinn Manual (versions 1.0 and 2.0, respectively), a comprehensive, non-binding treatise on international law as it applies to cyber warfare (version 1.0) and other cyber operations (added in version 2.0).

It is important to note that the two versions of the manual are not merely the product of updating information. Rather, the first edition maintains a narrow focus on international law as it pertains to warfare (acts of aggression) and cyber analogs thereof, while the latter broadens the scope to include more general operations in cyberspace that do not necessarily reach the threshold of being considered acts of war. Boasting more than 100 military and legal expert participants and reviewers, the Tallinn Manual remains the most compendious effort to date to map, codify, and influence international legal norms related to *jus ad bellum* and *jus in bello* in cyberspace. Though it is worth noting

that even in Tallinn 2.0, published a decade after the attacks on Estonia, Schmitt notes the lack of relevant treaties as well as "sparse" public availability of *opinio juris*.[101]

From the outset of developing the first Tallinn Manual and continuing through development of 2.0, Schmitt clearly identified the bounds of the problems at hand. Though the subject matter differs between versions, the principal question has aimed at reconciling existing international law with actions undertaken by nation-states in cyberspace. As Schmitt noted during the release event for 2.0, the process for discussing and attempting to reach consensus on these various topics has changed over time. The first Tallinn Manual relied on fewer than 50 individuals to make up the group consisting of the IGE, along with supporting legal researchers, and editors. Nearly all of these individuals represented either the United States or countries in Europe.

Tallinn Manual 2.0 more than doubled the size of the IGE and its supporting roles, and on top of refining its peer review process, instituted the so-called Hague Process. This was the result of the Dutch government approaching the IGE, asking how they could support the advancement of the group's initial findings. The addition of the Hague Process was a response to increased attention from nation-states who, after largely sitting the sidelines for 1.0, showed much greater interest in being part of the process for 2.0. The Asser Institute described the process thusly: *'The Hague Process' consists of over fifty States that attend at least one, sometimes more, of the three International Group of Experts meetings. In these meetings, States are provided with the draft texts and given the opportunity to express their views and comments on the content, an input which Prof. Schmitt described as extraordinarily useful.*[102] Or as Schmitt tells it:

> *"Nation-states originally kept us at arm's length because we were going to seize the normative landscape from them. The second round, nation-states came to them to ask how they could help. IGE committed to the principle that states and only states make international law. IGE listened to state legal advisor but reserved the right to tell states if their views were nonsense."*[103]

On February 8, 2017, the Atlantic Council hosted the launch of Tallinn Manual 2.0. After a brief overview of how the manual came into being, Schmitt made a few brief remarks before stating with hints of relief and nostalgia, "we're finished."

The Digital Geneva Convention

On a cyberdust covered content management platform tucked deep within the domain substructure of Microsoft Corporation lies a document that may be the first published reference to the technology giant's call for a digital (or electronic) Geneva Convention. Written by Corporate Vice President Scott Charney (now vice president, security policy), Rethinking the Cyber Threat is a 14-page memo that outlines threats in four main categories: cyber crime [*sic*], military espionage, economic espionage, and cyber warfare. Commenting on the asymmetric advantages of cyberspace, Charney makes the claim that, "the internet permits a potentially anonymous and untraceable individual with virtually no resources to engage a nation-state in cyber warfare."[104] He goes on to invoke the idea of an "electronic Pearl Harbor" and theorizes that "perhaps part of the response is an electronic "Geneva Convention." Charney ends his paper with a stepwise approach to governing cyber warfare:

> *To address cyber warfare issues, countries must first develop domestic positions on what the rules for this new domain should be, taking due care to recognize the shared and integrated nature of the domain. Then there must be an international dialogue designed to create international norms*

> *for cyber space behavior. Creating these norms will be as difficult as it sounds, but it is still both necessary and, ultimately, unavoidable. Absent such an agreement, unilateral and potentially unprincipled actions will lead to consequences that will be unacceptable and regrettable.*[105]

Like so many arks in so many crates, the subject of an electronic Geneva Convention was seemingly relegated to its own proverbial Hangar 51, though Microsoft would show renewed interest five years later. In November 2014, Charney published a follow-up entitled *Governments and APTs: The Need for Norms (Rethinking the Cyber Threat #2).* This document strays from the subject of warfare, mentioning it only five times in a 15-page document and focusing instead on matters of espionage; a hot topic given Edward Snowden's revelations the year prior. Charney puts up the scaffolding for the DGC, calling for a "new framework," presumably elucidated in the conclusory four stepwise points, viz.:[106]

1. Countries with espionage programs must admit they target other governments
2. Governments must discuss espionage programs that target private sector
3. Governments must agree that the doctrine of proportionality applies to attacks on civilian products, services, and infrastructures
4. Governments must accept that while private sector companies can be helpful, they cannot take sides in governmental disputes

By December 2014, things were really heating up towards a codification of what would become the Digital Geneva Convention. A team of 10 at Microsoft published the 24-page *International Cybersecurity Norms: Reducing conflict in an Internet-dependent world.* The introduction asserts that, "Cyber conflict and cyber war are not just theoretical

but are actual possibilities that need to be considered and addressed," before acknowledging how nation-states are "operationalizing" cyberspace as a "domain for conflict."[107] The report presents the chart in *Figure 4* as an explanation of various points at which an escalation in force by nation-states necessitates a particular kind of legal framework.[108] The report pays only glancing notice to Stuxnet, which by then had been widely documented.

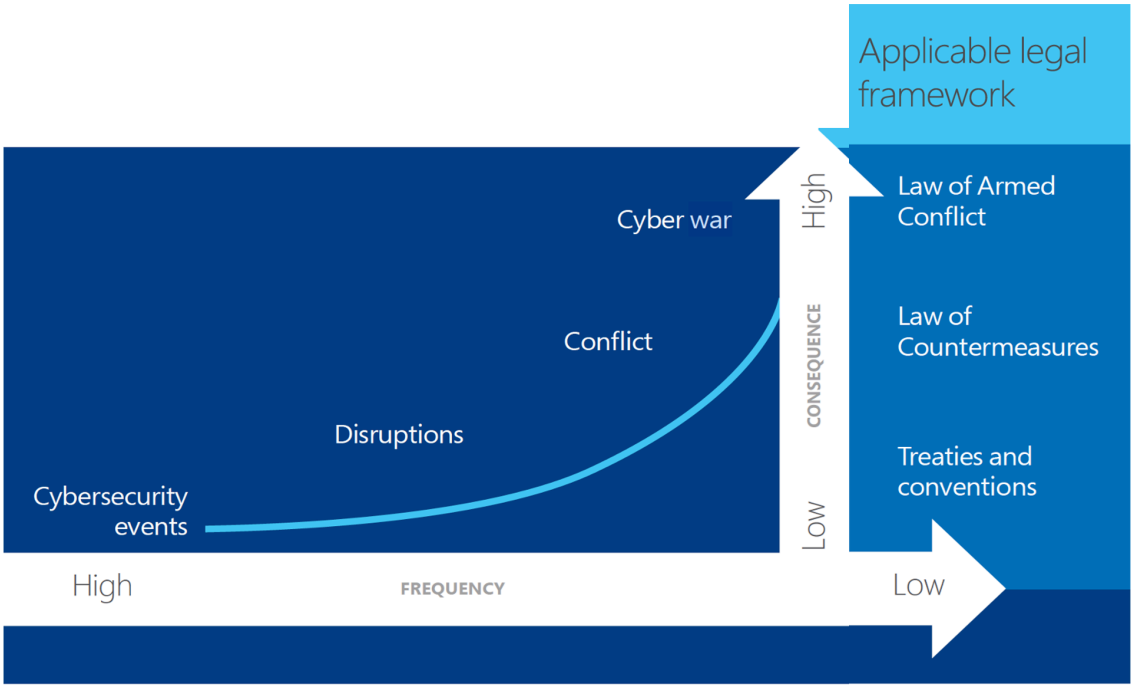

Figure 4 – Escalation of Cyber Events and Applicable Legal Framework

In addition to pointing to LOAC as the ultimate legal arbiter of cyber warfare, International Cybersecurity Norms put forth the truest DGC prototype to date in the form of six mandates for nation-states:[109]

1. States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.
2. States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
3. States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.
4. States should commit to nonproliferation activities related to cyber weapons.
5. States should limit their engagement in cyber offensive operations to avoid creating a mass event.
6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

Microsoft's penultimate policy paper in the evolution of the Digital Geneva Convention came in June 2016. Charney, leading a team of seven other Microsoft employees published *Articulation to Implementation: Enabling progress on cybersecurity norms*. Following the trend of previous publications, the topic of cyber warfare received almost no direct coverage. In fact, the only mention of the term *warfare* is in the only time any of Microsoft's DGC-related blogs mentions the Tallinn Manual. The great irony is that the citation in question pulls from the Tallinn Manual to point to six governmental proposals that are "currently driving the global dialogue on cybersecurity norms."[110]

Suffice it to say that the Digital Geneva Convention was not quite the *ex nihilo* product it may have seemed in 2017.

On February 14, 2017, one week after the launch of Tallinn Manual 2.0, Microsoft President Brad Smith took to the mainstage at RSA Conference in San Francisco to deliver the conference's keynote speech. Standing in front of a giant digital screen emblazoned with the Microsoft logo, he walked through indicators of growing threats to cyber security. He cited the fact that 74% of the world's businesses were expecting to be "hacked" over the coming year; that total economic losses to cybercrime would reach $3 trillion by 2020; that, "We've seen cyberattacks move from enthusiasts to financial thieves to now governments around the world."[111]

Smith further declared that, "cyberspace is the new battlefield," echoing the sentiments of Deputy Secretary of Defense William Lynn III, who spoke about the topic seven years earlier at the same conference. It was Lynn who at the time said, "The government cannot protect our nation alone...It is going to take a public-private partnership to secure our networks." Where Lynn's focus was on defense of national infrastructure, Smith presented his idea as a "call on the world's governments to come together." In the spirit of the successful 1949 framework designed to protect civilians during times of war, Smith proposed a new "Digital" Geneva Convention to "protect civilians on the internet in times of peace."

Smith laid out the details of the DGC as he saw it, stating, "the time has come to call on the world's governments to come together, affirm international cybersecurity

norms that have emerged in recent years, adopt new and binding rules, and get to work implementing them." The six "new and binding" rules he presented were:

1. No targeting of tech companies, private sector, or critical infrastructure;
2. Assist private sector efforts to detect, contain, respond to, and recover from events;
3. Report vulnerabilities to vendors, rather than to stockpile, sell, or exploit them;
4. Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise, and not reusable;
5. Commit to nonproliferation activities to cyberweapons; and
6. Limit offensive operation to avoid a mass event

The following section applies the information gathered for each of the aforementioned models to the Institutional Analysis and Development framework, then offers an evaluation based on Ostrom's evaluative criteria.

ANALYSIS

Define the policy analysis objective and specify the analytic approach

The primary policy analysis objective for both the Tallinn Manual and the Digital Geneva Convention is to determine current and potential effectiveness of achieving self-stated and otherwise implicit goals. A secondary analysis objective is to determine the likelihood of each model to prevent harm from befalling noncombatants in the event of cyber warfare. The analytic approach for both models and each objective is to define and map key model elements to Ostrom's Institutional Analysis and Development framework, following Polski and Ostrom's guidance for applying the IAD to policy analysis and design.

The Tallinn Manual

Mapping Model to Framework	
IAD Elements	**The Tallinn Manual 2.0**
Exogenous Variables	
Biophysical/Material Conditions	Cyber-Physical Attacks as Common Pool Resource
Attributes of Community	People: Lawyers, policy scholars, noncombatants Nation-states: Legal advisors, military strategists Corporations: Legal counsel, fiduciary responsibility
Rules	Customary International Law The Law of Armed Conflict UN Charter Geneva Conventions Case Law (*opinion juris)* Findings of the UN GGE The Schmitt Process The Hague Process The Tallinn Manual 1.0
Action Arena	
Action Situations	Cyberspace as a battlefield e.g. Stuxnet (if nation-state) e.g. Cyberattacks on ICS
Participants	People: Nation-state duty to protect noncombatants Nation-states: Must adhere to international law Corporations: No hack back
Interactions	Nation-states determining strategy and policy Nation-states consulting international law Adoption of the Tallinn Manual Nation-states consulting the Tallinn Manual Nation-states engaging in cyber warfare Nation-states impacting civilian infrastructure
Outcomes	The IGE The Tallinn Manual 2.0 The Hague Process for legal issues in cyberspace International law applies in cyberspace International influence by participation No nation-state attacks resulting in civilian harm (*PHEPH*)

Physical and material conditions

The Tallinn Manual recognizes the potential for nation-states to utilize cyber means to conduct warfare. This is explicitly defined as the use of cyber operations to inflict injury upon individuals or cause physical destruction in another state. The Tallinn Manual's emphasis on nation-state responsibility initially points to material conditions at the public property level only. However, destruction must be viewed as a pollutive act, potentially leading to permanent loss, as in death. Whether analyzing the situation as a function of security, warfare, physical well-being, or utility garnered from public infrastructure, this results in a necessarily highly subtractive environment in which it is difficult to exclude participants (i.e. nation-states on the attack).

Analyze community attributes

The genesis of the Tallinn Manual can be traced to 2009, when the NATO CCD COE agreed to sponsor the undertaking at the suggestion of Michael Schmitt. Schmitt then assembled the IGE based presumably on existing relationships, recommendations, and research based on scholarly contributions to date. The community, therefore, involves some degree of international institutionalism and civilian expertise, eventually incorporating broader individual expertise and nation-state input from top lawyers from more than 50 countries. The interactions between parties were organized around three sessions and an ongoing drafting and peer review process. Dialogue and pursuit of opinion from around the world captured one of the most vital aspects of sustainable common pool resource management: communication. It is worth noting that the IGE did

not include professionals from the cybersecurity industry (i.e. private sector). It is not entirely clear if that was intentional or, if so, why that was the case.

Only a small subset of the community under analysis is likely to be immediately impacted by the Tallinn Manual, viz. government legal advisors. Three years on from the release of the final version, the vast majority of references to the manual are in law journals and legal blogs. In order to become an effective institution, the Tallinn Manual will require advocates to ensure widespread adoption and opine periodically, in an official capacity, on real-world issues to which rules defined in the manual apply. The Tallinn Manual 2.0 analysis rests on the understanding that international law applies to cyber operations. This means that actions in cyberspace do not take place in a legal vacuum and states both have rights and bear obligations under international law.

Considering *Figure 3*, government lawyers will necessarily be responsible for educating and guiding political and military leaders on how international law applies to planned interstate action. Those leaders in turn must be willing to accept the findings of the Tallinn Manual or develop a system by which unresolved issues and concepts may be discussed. The Dutch government provided a method of bringing states together through what came to be known as the Hague Process. The community is decidedly public sector, (i.e. nation-states), with the possible addition of academics in general.

Analyze rules

There are two sets of rules requiring analysis. The first set is in the development of the Tallinn Manual itself. The rules that governed establishment of the IGE, communication between members, the peer review process (collectively, the Schmitt

Process), and eventually the Hague Process proved successful in achieving consensus on many applications of international law. This set of rules and processes (the institution of the manual compared to the manual as an institution) proved successful and scalable as many of the processes for 1.0 were transferred and improved upon for 2.0. The success of 1.0 in gaining the attention and desired participation of nation-states is another key indicator of its success. In that specific case, it demonstrates the IGE's ability to garner deference, thereby achieving some measure of authority, reinforcing its governance capacity.

The second set of rules includes those published in the manual itself. Specific to the topic of international humanitarian law, Chapter 16 on The Law of Armed Conflict Generally (Rules 80-85), but the manual is virtually exhaustive in its coverage of international law topics. Constant care (Rule 114), protection of journalists (Rule 139), protection of children (Rule 138). protection of cultural property (Rule 142). The Tallinn Manual cites case law, legal conventions, international treaties, the Geneva Conventions, ICRC opinions, the UN charter, all in addition to providing commentary and differing viewpoints of the IGE.

The Tallinn Manual can become a true institution if it can be shown that its assertions are being accepted by nation-states. This association will grow stronger as those same nation-states find themselves in states of war. For now, the manual is the most thorough legal analysis on the subject of cyber warfare and both its rigorous process and book format have the greatest potential to become global rules in use.

Analyze patterns of interaction

The question remains how much influence the manual will have on nation-state decisions in the conduct of cyber warfare. Though, this analysis adjudges the Tallinn Manual to have a high potential effect on the actions of nation-states. This is because of the authority it garners by association with established and customary international law. Furthermore, its endogenous expert authority and ties to an international defense alliance in NATO all lend to strong governance potential. However, the same association could be more of a hindrance than a help if Russia views it as adversarial. Schmitt makes clear throughout the manual's introduction that it is an independent work, but if Russia views it as an outgrowth of NATO attempts to balance regional power, then it could spell difficulty for true global adoption.

Analyze outcomes

The Tallinn Manual's book format makes it a portable and recognizable reference tool for state lawyers. During the launch event, Michael Schmitt claimed that Tallinn Manual 1.0 "probably sits in every [ministry of foreign affairs and ministry of defense] legal advisor's office in the entire world, from Washington to Beijing." If that is the case, then the same would reasonably be expected of Tallinn Manual 2.0. In fact, the Hague Process likely guarantees even broader nation-state adoption. After three years, the manual remains a relevant subject for legal research and analysis. Google Scholar shows 1,120 references to the manual since 2019 alone. One of the central tenets of successful commons governance is the importance of communication. The fact that scholars around

the world continue to discuss the Tallinn Manual bodes well for its long-term acceptance and adherence, at least among legal scholars.

A true evaluation of the strength of the Tallinn Manual in guiding states can only take place if and when a nation conducts a cyberattack. Because of how interwoven the Tallinn Manual is with existing international law, the violation thereof would be a serious indictment about the preventive capabilities of law. The study is over. The book is written. As Schmitt noted at the same launch event, “We don’t make law, but [disagreeing is] going to be a tough sell for other states.”

Evaluation

The Tallinn Manual achieves its stated aim of becoming a resource for state legal advisors in order for nation-state leaders to better understand how actions in cyberspace may be constrained by international law. The greatest question now relates to the degree to which international law itself prevents war. If international law in fact prevents warfare in any capacity, then the Tallinn Manual will be a successful model of governance for what may be termed notional or supra-arenas. The de facto nature of human reliance on law as promoter or dissuader of one action or another elevates the efficacy of the Tallinn Manual as a tool in the prevention of cyber warfare; certainly those most egregious violations of established international humanitarian law.

There do not appear to be any plans to continue to update the manual or hold additional meetings of the IGE. That leaves the door open for other institutions and organizations, including nation-states, to take the lead. The nation that sees Tallinn Manual 2.0 as a baton and takes it has the opportunity to control the conversation about

what constitutes legal and illegal action in cyberspace, especially during the prosecution of cyber warfare. Without an established governance regime to maintain the manual and continue to steward the conversation, there is some danger that what may currently be seen as a rulebook could morph into a playbook for nefarious state actors.

Evaluation Table for the Tallinn Manual 2.0

Evaluative Criteria	Tallinn Manual Rating (Low, Medium, High)
Efficiency in use of resources, especially capture of economies of scale	High – Adherence to customary international law bakes in existing attempts to preserve many types of resources, including security and physical infrastructure as CPRs
Equity in distributional outcomes and processes	High – In theory, international law applies to all nations equally; institutional attempt to include scholars from around the world for input and presumably greater distribution of message
Legitimacy as seen by participants in decision processes	High – The Tallinn Manual rests on established international law and the Schmitt and Hague Processes ensured broad discussion and review of proposed rules; Implicit NATO association
Accountability, especially to direct users of resource	Medium – Makes case for compliance with law but reliant on existing enforcement mechanisms; compellence, deterrence, etc.
Fiscal equivalence: the extent to which the beneficiaries of a public good or service are expected to contribute towards its production	NA – No calls for additional action aside from consideration by state legal advisors
Consistency with the moral values prevalent in that community	High – Comports with customary international law and took into account the many views of an international group of experts as well as >50 nation-states
Robustness or resiliency	Medium – The Tallinn Manual is only as robust as international law. It lacks the support structure necessary to carry on the conversation as a constant governor

The Digital Geneva Convention

Mapping Model to Framework	
IAD Elements	**The Digital Geneva Convention**
Exogenous Variables	
Biophysical/Material Conditions	Cyber-Physical Attacks as Common Pool Resource
Attributes of Community	People: Policy scholars, Noncombatants Nation-states: Political and military leaders Corporations: Executives, employees
Rules	1. No targeting of tech companies, private sector, or critical infrastructure; 2. Assist private sector efforts to detect, contain, respond to, and recover from events; 3. Report vulnerabilities to vendors, rather than to stockpile, sell, or exploit them; 4. Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise, and not reusable; 5. Commit to nonproliferation activities to cyberweapons; and 6. Limit offensive operation to avoid a mass event
Action Situations	
The Action Arena	Cyberspace as a battlefield
Participants	Tech sector (defense), Nation-states (offense)
Interactions	Public-private partnership
Outcomes	• Positive press reception • Friction with CCD COE • Cybersecurity Tech Accord • CyberPeace Institute • No binding international treaties • No nation-state attacks resulting in civilian harm (*PHEPH*)

Analyze physical and material conditions

Literature and speeches concerning the proposed Digital Geneva Convention recognize the potential for nation-states to utilize cyber means to conduct warfare. This is implicitly understood as the use of cyber operations to inflict injury upon individuals or

to cause physical destruction in another state. The Digital Geneva Convention's emphasis on a combination of nation-state and corporate responsibility blurs the line between public and private property. However, destruction must be viewed as a pollutive act, potentially leading to permanent loss, as in death. Whether analyzing the situation as a function of security, warfare, physical well-being, or utility garnered from public infrastructure, this results in a necessarily highly subtractive environment in which it is difficult to exclude participants

Analyze community attributes

The Digital Geneva Convention began with a policy paper by Scott Charney, writing in his capacity as a vice president at Microsoft. Charney eventually assembled a small team of other Microsoft employees who continued to expound upon his ideas with their own. These small groups of about 10 employees periodically updated the policy papers and eventually the ideas became the Digital Geneva Convention, which Microsoft President Brad Smith presented to an audience of private sector technology firms at RSA Conference. Smith shared a similar presentation to the United Nations in Geneva, Switzerland. The majority of the affected community is the private sector; however, the aim of the DGC is to impact nation-states by brokering a binding international agreement. Thus far, there is little to support the idea that the DGC has had any impact at the nation-state level, much less has it formed any basis for a binding agreement.

Analyze rules

The Digital Geneva Convention consists of six rules. Since Brad Smith's announcement in 2017, the rules have remained in their original state and may be reviewed on Microsoft's On the Issues blog. As presented, the rules appear to put forth novel concepts with no reference to existing customs, laws, norms, or best practices. All six of the rules are intended for adherence by nation-states and Smith has stated on multiple occasions his goal of achieving an international binding treaty to solidify their institutionalization. Because they are limited in number, this analysis comments on each:

1. **No targeting of tech companies, private sector, or critical infrastructure**

It is telling that the first item on the list is that nation-states should not target tech companies. The prime directive of international humanitarian law, upon which the Geneva Conventions are built, is the preservation of the lives of noncombatants. Nevertheless, rule one of the Digital Geneva Convention seems to be covered by international law concerning attacks on civilians and critical infrastructure, not to mention the fourth Geneva Convention relative to the protection of civilian persons. Though, critical definitions are missing from Microsoft's proposed rule that would strengthen its legitimacy: 1. "targeting" and 2. bounds of a "tech company" and the "private sector." Without these definitions, no further analysis can take place and the rule is determined to have low likely efficacy.

2. **Assist private sector efforts to detect, contain, respond to, and recover from events**

Here again, the ambiguity of the term "events" makes it impossible to analyze the intent of the rule. If the intent is that nation-states assist when private sector companies are the victims of cyberattacks (as defined in this paper), then that may fall within a certain duty of care. However, the threshold of compellence is not clear. The MITRE ATT&CK framework provides a popular visual representation of how cyberattacks can take place. It would be beneficial to map trigger points to some such framework. Otherwise, likely adoption of this rule and overall anticipated efficacy is low.

3. **Report vulnerabilities to vendors, rather than to stockpile, sell, or exploit them**

This rule has some novelty in the era of cyber warfare and deserves additional input from the international legal community. The NSA leak and resulting nefarious use of the EternalBlue exploit demonstrates the dangers of harboring vulnerabilities and the means to exploit them. Nevertheless, this would place a new duty on nation-states and again the threshold for compellence is unclear. If nation-states are expected to report vulnerabilities to vendors, that implies that it is within their purview to seek out vulnerabilities in the first place. This may be a reasonable action as part of a risk management and supply chain vetting strategy, but it is unclear when and why nation-states would conduct code analysis to the degree that they are finding software vulnerabilities. Likely adoption for this rule is moderate.

4. **Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise, and not reusable**
5. **Commit to nonproliferation activities to cyberweapons**
6. **Limit offensive operation to avoid a mass event**

The final three rules require greater disambiguation prior to analysis. It is not clear how the restraint in developing cyber weapons does not satisfy the commitment to nonproliferation and how that in turn does not satisfy limiting offensive operations. If a nation-state satisfies rule four, then it follows that they would satisfy rules five and six. Regardless, the same problem threads the entire needle. That is, that without clear definitions and bounds, these rules have low overall likelihood of adoption and are therefore ineffective. Ironically, the similarity of the three rules does bode well for broader adoption if a nation-state agrees to any one of them.

Integrate the analysis

The Digital Geneva Convention was conceived behind closed doors by a publicly traded, private sector technology company. In fact, it was precisely one individual who decided to write a paper and who summarily decided to update the same paper years later, leading to development of the DGC. While various Microsoft employees shared the vision along the way, there is no indication that any major international, interdisciplinary, or even intercorporate effort took place to fully assess even the need for a Digital Geneva Convention. Most baffling is that there are many recommendations for effective development of governance mechanisms in the literature. As Avant and Martha Finnemore point out almost presciently:

> "*because of its role in the enforcement of the Geneva Conventions, for example, the International Committee of the Red Cross has a unique role to play in the development of international humanitarian law (Finnemore 1996). NGOs attempting to develop a new understanding of the humanitarian effects of particular weapons, for example, are most likely to succeed if they first secure the endorsement of the ICRC Secretariat and persuade its representatives to speak out publicly on behalf of the issue.*[112]

If Microsoft has attracted the interest of the ICRC, then the two organizations are doing well to hide any endorsement. A search for the phrase "Digital Geneva Convention" on the ICRC website finds only two results, neither of which indicates any kind of partnership.

Furthermore, by the time Microsoft launched the DGC, the Tallinn Manual 1.0 had been in publication for four years, yet Smith makes no mention of the manual in either San Francisco or Geneva. In fact, as of July 2020, the only reference to the word Tallinn on the Microsoft Blog is in a late 2017 piece by Brad Smith, a rather bad faith criticism stating, *"While the Tallinn Manual 2.0 IGE made important progress in some areas, they could not reach consensus on what the U.N. Charter has to say about losses of functionality in civilian infrastructure even when nothing gets physically broken."* The emphasis on the U.N. Charter strawmans the argument, avoiding the entirety of the Tallinn Manual's work in mapping any and all relevant international law to matters in cyberspace. For the record, Rule 26 on Necessity is a good read.

The lack of attention paid to governance scholarship and existing international law, including, of all things, the Geneva Conventions, is baffling. A reasonable conclusion is that a large corporation saw an opportunity to seize on the brand recognition of a well-established international agreement and graft on a few quasi-novel, at times self-serving, rules, then present them without any external input or debate. If the

aim of the DGC is to establish a governance regime based on binding international agreements in order to protect civilians from the machinations of cyber warfare, then the initial effort leaves plenty to be desired.

Analyze outcomes

The Digital Geneva Convention was initially well received. The UN Refugee Agency (UNHCR) published an article opining on what the DGC would mean for the future of humanitarian action.[113] The World Economic Forum bolstered support with a blog entitled '*Why We Urgently Need a Digital Geneva Convention*. And several technology trade publications, including WIRED magazine published extollations.[114]

Since then, Microsoft has sponsored several initiatives to promote the DGC, including the 2018 launch of a "Cybersecurity Tech Accord" (referred to aptly confusingly as a Digital Geneva Accord by the New York Times). As of July 2020, the Accord has nearly 150 tech company signatories. Those signatories agree to uphold four principles, including the protection of "our" users and customers everywhere, opposition of cyberattacks on "innocent" citizens and enterprises, empowerment of users to strengthen protection, and partnering with one another to strengthen cybersecurity. In June 2020, Accord signatory Facebook was alleged to have helped the FBI develop a 0-day exploit for software not owned by Facebook in order to catch a child predator.[115] Facebook having reported the suspect to the FBI, determined that it could do more to help and hired a third-party firm to find a vulnerability in the operating system Tails (which none of the involved parties own). According to Facebook, the ends justified the means,

but the report highlights some of the very challenges that the DGC seeks to control, while amplifying its silence.

In September 2019, Microsoft announced the establishment of the CyberPeace Institute, headquartered in Geneva, Switzerland, asserting that, "The internet is the creation of the private sector, which is primarily responsible for its operation, evolution and security."[116] Microsoft has alluded to the need for an organization similar to the IAEA for monitoring cyber weapons. This appears to be one of the main functions of the CyberPeace Institute, which is currently in the process of hiring forensic investigators and data scientists, among other positions. It is most assuredly not merely a think tank, but a potential regulator and governor in its own right. While Brad Smith is a board member, the organization appears to aim at a more diverse approach than the Microsoft process that led to the DGC, boasting the likes of former President of Interpol Khoo Boon Hui and governance scholar Anne-Marie Slaughter. It is worth noting that Michael N. Schmitt sits on the advisory board for the CyberPeace Institute, which may indicate the potential to reconcile the models now under review.

Evaluation Table for the Digital Geneva Convention

Evaluative Criteria	DGC Rating (Low, Medium, High)
Efficiency in use of resources, especially capture of economies of scale	Medium – Financial backing of major technology firm, but lacking structure to effectively scale. Process too exclusive and rules are overly broad.
Equity in distributional outcomes and processes	Low – The initiative is led by a U.S.-based, publicly-traded firm. Rule #1 shows the emphasis for desired outcomes. No clear enforcement strategy or clear desire to adhere to international law.
Legitimacy as seen by participants in decision processes	Low – No indication that nation-states are seeking to adhere to or advance the DGC. Microsoft has not achieved a binding agreement (a goal of the DGC).
Accountability, especially to direct users of resource	Low – No clear indication of how nation-states will be held accountable.
Fiscal equivalence: the extent to which the beneficiaries of a public good or service are expected to contribute towards its production	Medium – Corporations to take responsibility but calls for increased government support.
Consistency with the moral values prevalent in that community	Medium – The aims are generally in line with existing humanitarian precepts, but there remain questions about corporate stewardship.
Robustness or resiliency	Medium – CyberPeace Institute has opportunity establish authority in international community. This could resuscitate a DGC-like model.

CONCLUSION

Understanding how governance systems work is a vital undertaking. The use of economic frameworks — in this case, the IAD — can help bound problems unique to social situations that are otherwise too highly variable to analyze. This research makes some progress in the application of the IAD to global governance systems, but far more local research is needed to disconfirm any conclusions presented here about the current state of affairs, much less any future state. Ultimately, this research assesses the Tallinn Manual to have a high likelihood of success both in longevity as a reference book for state legal advisors and as a mechanism for at very least momentary consideration prior to conduct reaching the level of cyber warfare (though, this paper is much more optimistic that the international community will heed the IGE's exercise and more readily recognize the international legal implications of cyber actions). Conversely, this research finds that the Digital Geneva Convention has low likelihood of success even if its longevity is propped up by a multibillion-dollar corporation. The lack of transparent process in its development, lack of clarity in the rules proposed, lack of open dialog and debate, and lack of formalization as either treaty or singular reference document, compounded by general eschewance of governance best practices all support this conclusion. Those supports stand on top of assertions made by those directly involved in the development of the Tallinn Manual; generally, that the DGC is a redundant work.[117] However, there is some optimism to be found in the related CyberPeace Institute, still in

its infancy. If the board of the CyberPeace Institute can maintain neutrality and begin a process similar to those utilized in the development of the Tallinn Manual, it could breathe new life into a DGC-like governance model.

In closing, I want to draw attention to the interactions exemplified in the attributes of community diagram found in *Figure 3* and associated relative distribution of power. The Tallinn Manual only ever sets out to speak to a narrow set of individuals within government and perhaps within the militaries of nation-states, viz. legal advisors. It does so from a place of explicit independence, claiming to represent no state in particular (though, it is difficult to shake the NATO associations and paucity of representation from certain "adversarial" nations). This is clearly delineated at the beginning of the manual and it stays true to its impartiality and narrow objectives. Microsoft, on the other hand, used the Digital Geneva Convention to call on nation-states and potentially private sector companies to agree to a variety of rules and ethical guidelines. By calling its project the Digital Geneva Convention it necessarily imparts a sense of care for noncombatants as well. Success of the DGC would potentiate a shift of power to the lower right corner such that nation-states would be expected to do the bidding of a single, private, American corporation in the name of preserving human life. While corporate social responsibility has gained traction in recent years and the stakeholder model has in some ways eclipsed the traditional shareholder model, this calls for much greater philosophical debate as to the appropriateness of private industry as a global governor.

One specific question is whether Microsoft or any private industry company can be trusted to supplement its fiduciary responsibility with a global responsibility for the preservation of humanitarian values. Two years after announcing the Digital Geneva

Convention, WIRED reported that since 2009, Microsoft has been helping China censor information found via Microsoft's search engine Bing as well as its professional networking platform, LinkedIn.[118] Governance scholar Dan Drezner cites an even longer time horizon for another American tech giant:

> *"In January 2006 Google agreed to create a China-based search engine that complied with the government's censorship policy. Google's acquiescence epitomizes the eagerness of multinational corporations to comply with Beijing's demands in order to access the Chinese marketplace."*[119]

A common refrain from corporate attorneys is often to effect of, "we merely abide by the laws of the countries in which we operate." If that is the case when it comes to suppression of freedom of speech, what guarantee can companies like Microsoft and Google offer that they are responsible guardians of human rights, and that those rights supersede the monetary incentives of market access? These problems approach the philosophical, but there are more local problems related to the notion of private industry playing a role in global governance and policymaking.

In fact, Charney addressed some of these issues head on in his 2014 piece, citing the difficulty of drawing "red lines" in complex environments. He posits that, *"it is arguable whether [technology] companies better promote freedoms by withdrawing from challenging markets or by spreading communications technologies."*[120] This is a formalization of the legal philosophy that one can't make an omelet without breaking a few eggs. But Charney goes on to note that, *"abandoning economic opportunities too quickly may be a breach of fiduciary responsibility."*[121] This is a difficult point with which to argue, but Charney presumes that fiduciary responsibility is a generalized normative good. It makes sense that corporations must adhere to their fiduciary

responsibility, but therein lies the precise reason why it may not be to the greatest good that those same corporations invite themselves into governing those activities which deal directly with threats to human life. The moral ambiguity is palpable. Charney offers that there are "clearly" situations in which moral questions should come before commercial interests, citing controversy related to IBM's involvement in the Holocaust, though history is doing a lot of work for Charney's surety.

Richard Clarke spends several pages in his 2010 book Cyber War cataloging Microsoft's troubling strategy and behavior within the United States government. Excerpts provided here:[122]

- P. 139 "…Microsoft the corporation has an agenda that is very clear: don't regulate security in the software industry, don't let the Pentagon stop using our software no matter how many security flaws it has, and don't say anything about software production overseas or deals with China.
- P. 139 "…Microsoft is an incredibly successful empire built on the premise of market dominance with low-quality goods."
- P. 141 "Microsoft gave me the very clear impression that if the U.S. government promoted Linux, Microsoft would stop cooperating with the U.S. government."
- P. 143 Microsoft can buy a lot of spokesmen and lobbyists for a fraction of the cost of creating more secure systems."

In fairness, these statements are both anecdotal and allegedly took place over a decade ago. Nevertheless, as those familiar with brand management can attest, perception can outweigh reality; especially when it comes to security. That is not to say that Microsoft is disqualified or irredeemable. Still, the problem of competing interests remains and

perhaps more troubling than concerns over fundamental flaws in software are those market influences that transcend the kinds of individuated rational action (in the formal sense) exhibited both in the development of the DGC and in Clarke's recounts.

Corporate influence in political decision making is hardly a new concept. The practice of lobbying is well established, and it is no secret that corporations have a vested interest in actively developing legislation that will support their business strategies. Though, special caution must be taken when business and legislation comingle on the battlefield. Again, this is a problem as old as Smedley Butler, yet it remains without a good solution. To exclude corporations from public conversation would be to ignore the massive impact and influence they have on technological development and public adoption. Cybersecurity poses the added question of responsibility for security. Herein lies the importance of calling up a perspective capable of dealing with complex economic situations. By viewing concepts like security and warfare as resources unto themselves and endeavoring to identify categories not otherwise descriptive of the kinds of public-private relationships that exist today, analysts can more accurately describe and predict for actions more or less likely to meet societal objectives, viz. peace.

Closing thoughts and next steps

A few thoughts for those endeavoring to apply the IAD for their own assessment of social systems. First is that the IAD is a framework for application, meaning that successful employment depends largely on the existence of an active action arena with discrete situations that can be observed, measured, and governed at a local level. That is not to say that there is no use for the IAD in understanding and governing global issues

such as cyber warfare (an activity whose arena remains empty). On the contrary, this research should provide some basis for future analysis in the event that a true cyberattack does take place at the nation-state level.

Second is that polycentricity opens wide the aperture of recursion. For instance, NIE theorizes that institutions are in fact the rules-in-use governing a particular arena. They may be formalized as laws, or they may arise as informal norms. Yet, it is often organizations, themselves governed by institutions, that develop those rules-in-use. As Ostrom shows, interactions that take place within arenas feed back into systems, opening the potential for externalities (from changes to exogenous rules in the interim) to affect *evaluated* outcomes. The key is to freeze a system in time rather than wrestling with time-continuous analysis, though discovery of how to reconcile the time factor would probably garner another Nobel for NIE. Those interested in the problem of cyberwarfare might be willing to analyze Stuxnet as a situation with a well-populated arena.

Another major foundational element of NIE is that certain aspects of neoclassicalism can be used to understand modern social problems dealing with rules governing behavior in particular arenas. The emphasis, however, is on the institutions themselves as opposed to rational actors. What I've found in this research is that even the most critical functions imaginable (matters of life and death) often come down to rational actor decision making. This research would benefit from careful integration of some of the principles elucidated by Graham Allison and Philip Zelikow in *Essence of Decision*, esp. regarding the Rational Actor Model. To be done effectively, this would require an profiling key actors involved to better understand their preferences and beliefs regarding risk and utility. An interesting challenge for some enterprising scholar.

ENDNOTES

[1] Pollard, A. O. Fire-Eater; the Memoirs of a V.C. London: Hutchinson, 1932.

[2] "Declaration (IV,2) Concerning Asphyxiating Gases. The Hague, 29 July 1899." Treaties, States parties, and Commentaries - Geneva Conventions of 1949 and Additional Protocols, and their Commentaries. Accessed July 25, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument.

[3] Nevertheless, specious claims abound, including a 2019 Business Insider article, which boosted a Krebs on Security article, which pointed to a study attempting to correlate cyberattacks with delayed patient care that is so convoluted and hopeful of the law of large numbers solving for ("smoothing") every nuance related to an extremely complex study, it is almost as unreliable as it is unreadable. Krebs, who is a trusted news source in the cybersecurity field, would have done well to read the findings of Ghafur et al in A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS, published a month before he declared in the same article that "not a lot of people were looking too hard for evidence" of how cyberattacks may negatively impact patients. Ghafur and colleagues found no increase in mortality as a result of WannaCry in a clear, targeted, far more methodologically sound study that still leaves space for the possibility of other patient harms. The point is, when a bomb goes off, you don't need two PhDs and an MD funded by the National Science Foundation to figure out proximal cause of casualties. In order to study cyber-physical events, causality has to become that simple.

[4] Zetter, Kim. 2014. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Crown Publishers. Prologue.

[5] Bundesamt für Sicherheit in der Informationstechnik. 2014. Die Lage der IT-Sicherheit in Deutschland 2014. 31. Retrieved online July 3, 2020. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf;jsessionid=DE5A404BE5A89777D3C819B5552BE5B0.2_cid369?__blob=publicationFile&v=2

[6] Bumiller, Elisabeth, and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." The New York Times, October 11, 2012.

[7] Charles, Deborah. "U.S. Homeland Chief: Cyber 9/11 Could Happen 'Imminently.'" Reuters. Thomson Reuters, January 24, 2013. https://www.reuters.com/article/us-usa-cyber-threat/u-s-homeland-chief-cyber-9-11-could-happen-imminently-idUSBRE90N1A320130124.

[8] Lyngaas, Sean. "NSA's Rogers Makes the Case for Cyber Norms." FCW, February 23, 2015. https://fcw.com/articles/2015/02/23/nsa-rogers-cyber-norms.aspx.

[9] Lawson, Sean, and Michael K. Middleton. 2019. "Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016. First Monday. Retrieved online July 3, 2020. https://firstmonday.org/ojs/index.php/fm/article/view/9623/7736.

[10] Schmitt, Michael N. 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, United Kingdom: Cambridge University Press.

[11] Ibid. 273.

[12] Ibid.

[13] Ibid.

[14] Patience, Microsoft. I will explain the evolution of your thinking later on.

[15] Smith, Brad. “The Need for a Digital Geneva Convention.” Microsoft on the Issues, May 15, 2018. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[16] Ibid.

[17] Tworek, Heidi. “Microsoft Is Right: We Need a Digital Geneva Convention.” Wired. Conde Nast, June 3, 2017. https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/.

[18] World Economic Forum. “Why We Urgently Need a Digital Geneva Convention.” World Economic Forum, December 29, 2017. https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention/.

[19] Minárik, Tomáš, and LTC Kris van der Meij. “Geneva Conventions Apply to Cyberspace: No Need for a 'Digital Geneva Convention'.” CCD COE, 2017. https://ccdcoe.org/news/2017/geneva-conventions-apply-to-cyberspace-no-need-for-a-digital-geneva-convention/.

[20] Avant, Deborah D., Martha Finnemore, and Susan K. Sell, et al. 2014. Who Governs the Globe? Cambridge: Cambridge University Press. 2.

[21] Ibid.

[22] Laozi, and William Scott Wilson. Tao Te Ching: an All-New Translation. Boulder, CO: Shambhala, 2013.

[23] Ostrom, V., & Ostrom, E. (2003). Rethinking institutional analysis: Interviews with Vincent and Elinor Ostrom. Mercatus Center: George Mason University.

[24] I am aware of the strong negative associations with use of the phrase, “collateral damage.” Here, it is not attempting any euphemistic avoidance of dealing with the very real people and places who fall victim to the violent overtures of politics. Rather, it remains a term of art and as this is an academic paper, it is still appropriate nomenclature. Rest assured, this research and continuing work will never shy away from the fact that the matter of warfare means that the lives of real people are at risk.

[25] Smith, Adam, and Andrew S. Skinner. “Bk. IV, Ch. II.” Essay. In The Wealth of Nations. London: Penguin, 1999.

[26] Hardin, Garrett. 1968. “The Tragedy of the Commons.” Science 162 (3859): 1243–48. doi:10.1126/science.162.3859.1243. 1248.

[27] Wiesner and York characterize the arms race as a, “steady open spiral downward to oblivion” (Wiesner and York 1964, 35).

[28] Hardin, Garrett. 1968. “The Tragedy of the Commons.” Science 162 (3859): 1243–48. doi:10.1126/science.162.3859.1243.

[29] Perhaps the first signs of artificial intelligence becoming truly sentient will be the discovery of a binary exhibition of some form of ego in which a chess-playing program ranks itself above its human competitors.

[30] *All art is concerned with the realm of coming-to-be, i.e., with contriving and studying how something which is capable both of being and of not being may come into existence, a thing whose starting point or source is in the producer and not in the thing produced.* Aristotle. 1962. Nicomachean Ethics. P.152. Englewood Cliffs, NJ: Prentice Hall.

[31] Rhodes, Richard. Arsenals of Folly: Nuclear Weapons in the Cold War. New York: Alfred A. Knopf, 2007. 74.

[32] Ostrom, Elinor, Roger B. Parks, Gordon P. Whitaker, and Stephen L. Percy. 1978. Formation of Police and Law Enforcement Policy: The public service production process: A framework for analyzing police services. Policy Studies Journal 7. 381-9.

[33] These three categories are best elucidated in chapter one of Ostrom's 1990 work Governing the Commons. She refers to "Three Influential Models," including the Tragedy of the Commons, the Prisoner's Dilemma Game, and the Logic of Collective Action (Ostrom 1990, 2-7).

[34] Ostrom, E. and Vincent Ostrom. 1985. Studies in Institutional Analysis and Development. Unknown. 3. This thing is insanely difficult to find in full. If I am unable to locate it by the time I'm done writing this paper, I'll leave this comment alone and ask someone to send it my way. I already asked Scott Shackelford but he hasn't yet responded.

[35] This is about as meta as it gets. Ostrom researches issues that arise out of common pool resource sharing and comes to the conclusion that the very independent disciplines seeking to understand how individuals ought to share resources are, in fact, not adequately self-coordinating to produce meaningful research. Oh yeah, by the way, she doesn't know it when she's writing this, but she will go on to win a Nobel Prize, in part, for demonstrating that top-down governance is not mandatory for efficient resource allocation. But whereas she may see her research as contributory, it could also be seen as a sort of top-down governance in its own right. Whoa.

[36] Ostrom, Elinor. 1990. Governing the Commons: The Evolutions of Institutions for Collective Action. Cambridge: Cambridge University Press. 45.

[37] Ibid.

[38] Research into international governance regimes and especially those attempting to influence hyperconnected cyberspace necessarily deals with the subject of polycentricity, but this is a rabbit hole too easy to go down and one that would distract from the paper's main thesis. Please do read Aligica and Tarko's Polycentricity: From Polanyi to Ostrom and Beyond in Governance: An International Journal of Policy, Administration, and Institutions, Vol. 25, No. 2, April 2012 (pp. 237–262).

[39] Ostrom, E. .2005. Understanding Institutional Diversity, Princeton, NJ: Princeton University Press. 15.

[40] I also want to acknowledge that there exists a newer iteration of the Institutional Analysis and Development framework called the Social Ecological Systems framework. However, as far as I can tell, the SES is more distinction than difference.

[41] Davidow, Bill. "The Tragedy of the Internet Commons." The Atlantic. Atlantic Media Company, May 18, 2012. https://www.theatlantic.com/technology/archive/2012/05/the-tragedy-of-the-internet-commons/257290/.

[42] Ibid.

[43] Raymond, Mark. 2013. "Puncturing the Myth of the Internet as a Commons." Georgetown Journal of International Affairs

[44] Ibid. 6.

[45] Ibid. 8.

[46] Hardin, Garrett. 1968. “The Tragedy of the Commons.” *Science* 162 (3859): 1243–48. doi:10.1126/science.162.3859.1243.

[47] Polski, M.M. and Ostrom, E., 1999. An institutional framework for policy analysis and design. 1999.

[48] Ibid.

[49] Schmitt, Michael N. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, United Kingdom: Cambridge University Press. 415.

[50] McGinnis, M.D., 2011. An introduction to IAD and the language of the Ostrom workshop: a simple guide to a complex framework. *Policy Studies Journal*, *39*(1), pp.169-183.

[51] Ibid.

[52] Ibid.

[53] Ibid.

[54] Ostrom, Elinor. 1993. *Governing the Commons: The Evolutions of Institutions for Collective Action*. Cambridge: Cambridge University Press.

[55] McGinnis, M.D., 2011. An introduction to IAD and the language of the Ostrom workshop: a simple guide to a complex framework. *Policy Studies Journal*, *39*(1), pp.169-183.

[56] Directorate, O. (n.d.). OECD Glossary. Retrieved July 07, 2020, from https://stats.oecd.org/glossary/detail.asp?ID=890

[57] McGinnis, M.D., 2011. An introduction to IAD and the language of the Ostrom workshop: a simple guide to a complex framework. *Policy Studies Journal*, *39*(1), pp.169-183.

[58] It is with every fiber of my all too frail being that I tried to avoid any reference to Clausewitz, or certainly, and god forbid, the Clausewitzian Trinity. But here’s something I’ve learned. While survival isn’t a guarantor of validity, it is a really good heuristic. The more I thought about the question of how to define attributes of the community, the more it genuinely made sense to fall back to the relationships so well codified by Clausewitz. So it is with apologies to those who think that this is just another military guy writing about Clausewitz. On War is a good book. Yeah, even the part about the impassability of swamps.

[59] McGinnis, M.D., 2011. An introduction to IAD and the language of the Ostrom workshop: a simple guide to a complex framework. *Policy Studies Journal*, *39*(1), pp.169-183.

[60] Ibid.

[61] Ibid.

[62] Ibid.

[63] Ibid.

[64] Rid, Thomas. 2017. *Cyber War Will Not Take Place*. London: Hurst et Company.

[65] Gartzke, E., 2013. The myth of cyberwar: bringing war in cyberspace back down to earth. *International Security*, *38*(2), pp.41-73.

[66] Najam et al. 2006; Club of Rome n.d.
[67] Slaughter, Anne-Marie. 2005. *A New World Order*. Princeton, NJ: Princeton University Press.

[68] Avant, Deborah D., Martha Finnemore, and Susan K. Sell, et al. 2014. *Who Governs the Globe?* Cambridge: Cambridge University Press. 1.

[69] Slaughter, Anne-Marie. 2005. *A New World Order*. Princeton, NJ: Princeton University Press.

[70] Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: the next Threat to National Security and What to Do about It*. New York: HarperCollins Publishers.

[71] Kaplan, Fred. 2017. *Dark Territory*. Place of publication not identified: Simon & Schuster.

[72] Ibid.

[73] US Attorney's Office District of Massachusetts. July 19, 2011. "Alleged Hacker Charged With Stealing Over Four Million Documents from MIT Network" (Press release). Archived from the original on May 26, 2012. Retrieved July 8, 2020.

[74] Halbert, D., 2016. Intellectual property theft and national security: Agendas and assumptions. *The Information Society*, *32*(4), pp.256-268.

[75] Borghard, Erica, and Shawn Lonergan. "Chinese Hackers Are Stealing U.S. Defense Secrets: Here Is How to Stop Them." Council on Foreign Relations. Council on Foreign Relations. Accessed July 7, 2020. https://www.cfr.org/blog/chinese-hackers-are-stealing-us-defense-secrets-here-how-stop-them.

[76] Ibid.

[77] "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information." The United States Department of Justice, June 7, 2019. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[78] Halbert, D., 2016. Intellectual property theft and national security: Agendas and assumptions. *The Information Society*, *32*(4), pp.256-268.

[79] Dropping the other alleged attack here as there is such little evidence that anything actually happened at the unnamed German steel mill in 2014 that it is impossible to independently analyze what happened, who may have been involved, or what methods may have been used. The German BSI dedicated only 139 words to the incident in their only report on the matter, offering very little to go on. Further A year after the alleged event, Dragos CEO Robert Lee let loose a firm warning about drawing conclusions about anything related to the alleged incident, affirming that making assumptions and basing them on unnamed sources is a chronic problem in information security. As recently as 2019, German media still could not identify the steel mill in question. It's not worth discussing unless more details emerge.

[80] Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the Worlds First Digital Weapon*. New York: Crown Publishers.

[81] Kaspersky, E. November 2, 2011. The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight. Retrieved July 07, 2020, from https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/

[82] How a Secret Cyberwar Program Worked. (2012, June 01). Retrieved July 08, 2020, from https://archive.nytimes.com/www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html?_r=0

[83] Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the Worlds First Digital Weapon*. New York: Crown Publishers.

[84] Simpson, C. (2013, November 20). Stuxnet Used an Old Movie Trick to Fool Iran's Nuclear Program. Retrieved July 08, 2020, from https://www.theatlantic.com/international/archive/2013/11/stuxnet-used-old-movie-trick-fool-irans-nuclear-program/355340/

[85] Glaser, John. 2017. Cyberwar on Iran Won't Work. Here's Why. (2017, August 21). Retrieved July 08, 2020, from https://www.cato.org/publications/commentary/cyberwar-iran-wont-work-heres-why

[86] International Atomic Energy Agency. November, 8, 2011. Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran. Retrieved July 8, 2020. https://isis-online.org/uploads/isis-reports/documents/IAEA_Iran_8Nov2011.pdf

[87] Raytheon Presentation on Future Missile Defense. (2017, March 04). Retrieved July 08, 2020, from https://www.nytimes.com/interactive/2017/03/04/world/asia/document-Raytheon-Missile-Defense.html

[88] Broad, W., & Sanger, D. (2017, March 04). U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight. Retrieved July 08, 2020, from https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html

[89] UCLA. Hiroshima and Nagasaki Death Toll, 2007. http://www.aasc.ucla.edu/cab/200708230009.html.

[90] Medetsky, A. (2004). KGB Veteran Denies CIA Caused '82 Blast: News. Retrieved July 08, 2020, from http://oldtmt.vedomosti.ru/sitemap/free/2004/3/article/kgb-veteran-denies-cia-caused-82-blast/232261.html

[91] Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the Worlds First Digital Weapon*. New York: Crown Publishers.

[92] Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: the next Threat to National Security and What to Do about It*. New York: HarperCollins Publishers. 93.

[93] Aquinas, St. Thomas. 1270. Commentary, *I Metaphysics, lect. 3.*

[94] RSA Conference. March 2, 2016. Remarks by Admiral Michael S. Rogers. Retireved July 8, 2020. https://youtu.be/3DdkRK0hn8Q?t=1741 (quote at 29:00 mark)

[95] Ottis, R. (2008). Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008. Reading: Academic Publishing Limited, pp 163-168.

[96] Ibid.

[97] Ibid.

[98] Cambridge University Press – Academic. April 29, 2013. Retrieved July 8, 2020. https://www.youtube.com/watch?v=Jxvm815Z96w

[99] Ibid.

[100] Schmitt later asserted that it took about four minutes to determine *if* international law applied to cyberspace. The answer was a resounding yes.

[101] Schmitt, Michael N. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, United Kingdom: Cambridge University Press.

[102] Asser Institute. 2016. The Tallinn Manual 2/0 and The Hague Process: From Cyber Warfare to Peacetime Regime. Retrieved July 8, 2020. https://www.asser.nl/media/2878/report-on-the-tallinn-manual-20-and-the-hague-process-3-feb-2016.pdf

[103] Cambridge University Press – Academic. April 29, 2013. Retrieved July 8, 2020. https://www.youtube.com/watch?v=Jxvm815Z96w

[104] Charney, Scott. 2009. Rethinking the Cyber Threat. Microsoft Corporation. Retrieved July 8, 2020. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroB

[105] Ibid.

[106] Charney, Scott. 2014. Governments and APTs: The Need for Norms. Retrieved July 8, 2020. https://www.microsoft.com/en-us/download/details.aspx?id=45011

[107] McKay, Angela, et al. 2014. International Cybersecurity Norms: Reducing conflict in and Internet-dependent world. Retrieved July 8, 2020. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA

[108] Ibid.

[109] Ibid.

[110] Charney, Scott, et al. June 2016. From Articulation to Implementation: Enabling progress on cybersecurity norms. Retrieved July 8, 2020. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8

[111] Microsoft. March 1, 2017. Brad Smith at RSA 2017: The Need for a Digital Geneva Convention. Retrieved July 8, 2020. https://www.youtube.com/watch?v=C-YvpuJO6pQ

[112] Avant, Deborah D., Martha Finnemore, and Susan K. Sell, et al. 2014. *Who Governs the Globe?* Cambridge: Cambridge University Press.

[113] Rudnick, J. (2017, August 02). What the Digital Geneva Convention means for the future of humanitarian action. Retrieved July 09, 2020, from https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/

[114] Tworek, H. (2017, June 03). Microsoft Is Right: We Need a Digital Geneva Convention. Retrieved July 09, 2020, from https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/

[115] Franceschi-Bicchierai, L. (2020, June 10). Facebook Helped the FBI Hack a Child Predator. Retrieved July 09, 2020, from https://www.vice.com/en_us/article/v7gd9b/facebook-helped-fbi-hack-child-predator-buster-hernandez

[116] Burt, T. (2019, October 04). CyberPeace Institute fills a critical need for cyberattack victims. Retrieved July 09, 2020, from https://blogs.microsoft.com/on-the-issues/2019/09/26/cyberpeace-institute-fills-a-critical-need-for-cyberattack-victims/

[117] Wallace, D. and Visger, M., 2018. Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community. *Journal of Law & Cyber Warfare*, *6*(2), pp.3-55.

[118] Simonite, T. (n.d.). US Companies Help Censor the Internet in China, Too. Retrieved July 09, 2020, from https://www.wired.com/story/us-companies-help-censor-internet-china/

[119] Drezner, Daniel W. 2007. *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton, NJ: Princeton University Press.

[120] Charney, Scott. 2014. Governments and APTs: The Need for Norms. Retrieved July 8, 2020. https://www.microsoft.com/en-us/download/details.aspx?id=45011

[121] Ibid.

[122] Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: the next Threat to National Security and What to Do about It*. New York: HarperCollins Publishers.

BIBLIOGRAPHY

Aquinas, St. Thomas. 1270. Commentary, *I Metaphysics, lect. 3.*

Aristotle. Translated by Martin Ostwald. 1962. Nicomachean Ethics. Englewood Cliffs, NJ: Prentice Hall.

Asser Institute. 2016. The Tallinn Manual 2/0 and The Hague Process: From Cyber Warfare to Peacetime Regime. Retrieved July 8, 2020. https://www.asser.nl/media/2878/report-on-the-tallinn-manual-20-and-the-hague-process-3-feb-2016.pdf

Avant, Deborah D., Martha Finnemore, and Susan K. Sell, et al. 2014. Who Governs the Globe? Cambridge: Cambridge University Press.

Borghard, Erica, and Shawn Lonergan. March 11, 2019. "Chinese Hackers Are Stealing U.S. Defense Secrets: Here Is How to Stop Them." Council on Foreign Relations. Council on Foreign Relations. Retrieved July 7, 2020. https://www.cfr.org/blog/chinese-hackers-are-stealing-us-defense-secrets-here-how-stop-them.

Broad, W., & Sanger, D. March 4, 2017. U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight. Retrieved July 08, 2020, from https://www.nytimes.com/2017/03/04/world/asia/left-of-launch-missile-defense.html

Bumiller, Elisabeth, and Thom Shanker. October 11, 2012. "Panetta Warns of Dire Threat of Cyberattack on U.S." The New York Times.

Bundesamt für Sicherheit in der Informationstechnik. 2014. Die Lage der IT-Sicherheit in Deutschland 2014. Retrieved July 3, 2020. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf;jsessionid=DE5A404BE5A89777D3C819B5552BE5B0.2_cid369?__blob=publicationFile&v=2

Burt, T. October 4, 2019. CyberPeace Institute fills a critical need for cyberattack victims. Retrieved July 09, 2020, from https://blogs.microsoft.com/on-the-issues/2019/09/26/cyberpeace-institute-fills-a-critical-need-for-cyberattack-victims/

Charles, Deborah. January 24, 2013. "U.S. Homeland Chief: Cyber 9/11 Could Happen 'Imminently.'" Reuters. Thomson Reuters. https://www.reuters.com/article/us-usa-cyber-

threat/u-s-homeland-chief-cyber-9-11-could-happen-imminently-idUSBRE90N1A320130124.

Charney, Scott. 2009. Rethinking the Cyber Threat. Microsoft Corporation. Retrieved July 8, 2020. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroB

Charney, Scott. 2014. Governments and APTs: The Need for Norms. Retrieved July 8, 2020. https://www.microsoft.com/en-us/download/details.aspx?id=45011

Charney, Scott, et al. June 2016. From Articulation to Implementation: Enabling progress on cybersecurity norms. Retrieved July 8, 2020. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmc8

Clarke, Richard A., and Robert K. Knake. 2010. *Cyber War: the next Threat to National Security and What to Do about It*. New York: HarperCollins Publishers.

Davidow, Bill. May 18, 2012. "The Tragedy of the Internet Commons." The Atlantic. Atlantic Media Company. Retrieved July 8, 2020. https://www.theatlantic.com/technology/archive/2012/05/the-tragedy-of-the-internet-commons/257290/.

Directorate, O. (n.d.). OECD Glossary. Retrieved July 07, 2020, from https://stats.oecd.org/glossary/detail.asp?ID=890

Drezner, Daniel W. 2007. *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton, NJ: Princeton University Press.

Franceschi-Bicchierai, L. June 10, 2020. Facebook Helped the FBI Hack a Child Predator. Retrieved July 09, 2020, from https://www.vice.com/en_us/article/v7gd9b/facebook-helped-fbi-hack-child-predator-buster-hernandez

Gartzke, E. 2013. The myth of cyberwar: bringing war in cyberspace back down to earth. *International Security*, *38*(2).

Glaser, John. Cyberwar on Iran Won't Work. Here's Why. August 21, 2017. Retrieved July 08, 2020, from https://www.cato.org/publications/commentary/cyberwar-iran-wont-work-heres-why

Halbert, D. 2016. Intellectual property theft and national security: Agendas and assumptions. *The Information Society*, *32*(4).

Hardin, Garrett. 1968. "The Tragedy of the Commons." Science 162 (3859): 1243–48. doi:10.1126/science.162.3859.1243.

International Atomic Energy Agency. November 8, 2011. Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran. Retrieved July 8, 2020. https://isis-online.org/uploads/isis-reports/documents/IAEA_Iran_8Nov2011.pdf

The International Committee of the Red Cross. "Declaration (IV,2) Concerning Asphyxiating Gases. The Hague, 29 July 1899." Treaties, States parties, and Commentaries - Geneva Conventions of 1949 and Additional Protocols, and their Commentaries. Retrieved July 25, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument.

Kaplan, Fred. 2017. *Dark Territory*. Place of publication not identified: Simon & Schuster.

Kaspersky, E. November 2, 2011. The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight. Retrieved July 07, 2020, from https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/

Laozi, and William Scott Wilson. 2013. Tao Te Ching: An All-New Translation. Boulder, CO: Shambhala.

Lawson, Sean, and Michael K. Middleton. 2019. "Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016. First Monday. Retrieved online July 3, 2020. https://firstmonday.org/ojs/index.php/fm/article/view/9623/7736.

Lyngaas, Sean. February 23, 2015. "NSA's Rogers Makes the Case for Cyber Norms." FCW. https://fcw.com/articles/2015/02/23/nsa-rogers-cyber-norms.aspx.

McGinnis, M.D. 2011. An introduction to IAD and the language of the Ostrom workshop: a simple guide to a complex framework. *Policy Studies Journal*, *39*(1).

McKay, Angela, et al. 2014. International Cybersecurity Norms: Reducing conflict in and Internet-dependent world. Retrieved July 8, 2020. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA

Medetsky, A. 2004. KGB Veteran Denies CIA Caused '82 Blast: News. Retrieved July 08, 2020, from http://oldtmt.vedomosti.ru/sitemap/free/2004/3/article/kgb-veteran-denies-cia-caused-82-blast/232261.html

Minárik, Tomáš, and LTC Kris van der Meij. "Geneva Conventions Apply to Cyberspace: No Need for a 'Digital Geneva Convention'." CCD COE, 2017. https://ccdcoe.org/news/2017/geneva-conventions-apply-to-cyberspace-no-need-for-a-digital-geneva-convention/.

The New York Times. How a Secret Cyberwar Program Worked. June 1, 2012. Retrieved July 08, 2020, from https://archive.nytimes.com/www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html?_r=0

Ostrom, Elinor. 1990. Governing the Commons: The Evolutions of Institutions for Collective Action. Cambridge: Cambridge University Press.

Ostrom, Elinor. 1993. *Governing the Commons: The Evolutions of Institutions for Collective Action*. Cambridge: Cambridge University Press.

Ostrom, Elinor. 2005. Understanding Institutional Diversity, Princeton, NJ: Princeton University Press.

Ostrom, E. and Vincent Ostrom. 1985. Studies in Institutional Analysis and Development. Unknown.

Ostrom, V., & Ostrom, E. 2003. Rethinking institutional analysis: Interviews with Vincent and Elinor Ostrom. Mercatus Center: George Mason University.

Ostrom, Elinor, Roger B. Parks, Gordon P. Whitaker, and Stephen L. Percy. 1978. Formation of Police and Law Enforcement Policy: The public service production process: A framework for analyzing police services. Policy Studies Journal 7. 381-9.

Ottis, R. 2008. Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective. Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008. Reading: Academic Publishing Limited.

Pollard, A. O. 1932. Fire-Eater; the Memoirs of a V.C. London: Hutchinson.

Polski, M.M. and Ostrom, E. 1999. An institutional framework for policy analysis and design.

Raymond, Mark. 2013. "Puncturing the Myth of the Internet as a Commons." Georgetown Journal of International Affairs.

Rhodes, Richard. 2007. Arsenals of Folly: Nuclear Weapons in the Cold War. New York: Alfred A. Knopf.

Rid, Thomas. 2017. *Cyber War Will Not Take Place*. London: Hurst et Company.

Rudnick, J. August 2, 2017. What the Digital Geneva Convention means for the future of humanitarian action. Retrieved July 09, 2020, from https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/

Schmitt, Michael N., et al. 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, United Kingdom: Cambridge University Press.
Simonite, T. (n.d.). US Companies Help Censor the Internet in China, Too. Retrieved July 09, 2020, from https://www.wired.com/story/us-companies-help-censor-internet-china/

Simpson, C. November 20, 2013. Stuxnet Used an Old Movie Trick to Fool Iran's Nuclear Program. Retrieved July 8, 2020, from https://www.theatlantic.com/international/archive/2013/11/stuxnet-used-old-movie-trick-fool-irans-nuclear-program/355340/

Slaughter, Anne-Marie. 2005. *A New World Order*. Princeton, NJ: Princeton University Press.

Smith, Adam, and Andrew S. Skinner. 1999. "Bk. IV, Ch. II." Essay. In the Wealth of Nations. London: Penguin.

Smith, Brad. May 15, 2018. "The Need for a Digital Geneva Convention." Microsoft on the Issues. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Tworek, H. June 3, 2017. Microsoft Is Right: We Need a Digital Geneva Convention. Retrieved July 09, 2020, from https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/

The University of California, Los Angeles. Hiroshima and Nagasaki Death Toll, 2007. Retrieved July 8, 2020. http://www.aasc.ucla.edu/cab/200708230009.html.

US Attorney's Office District of Massachusetts. July 19, 2011. "Alleged Hacker Charged With Stealing Over Four Million Documents from MIT Network" (Press release). Archived from the original on May 26, 2012. Retrieved July 8, 2020.

Wallace, D. and Visger, M. 2018. Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community. *Journal of Law & Cyber Warfare*, *6*(2).

World Economic Forum. December 29, 2017. "Why We Urgently Need a Digital Geneva Convention." World Economic Forum. Retrieved July 8, 2020. https://www.weforum.org/agenda/2017/12/why-we-urgently-need-a-digital-geneva-convention/.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the Worlds First Digital Weapon*. New York: Crown Publishers.