Addressing Cyber Warfare:
Bolstering Deterrence through developing norms

by

Ashley Dawson

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES
(Political Science)

THE UNIVERSITY OF BRITISH COLUMBIA
(Vancouver)

August 2013

Abstract:

This paper is interested in two things: one, exploring the ways in which states can deploy cyber-attacks that aim at disrupting, paralyzing and possibly destroying another state's assets, with direct bearing on national security; and two, the potential strategies for limiting the scope and number of these attacks in the absence of viable deterrence. There is an ongoing debate about the nature and possibility of a 'cyber war' in the international system. By revisiting traditions conceptions of war, this paper argues a large-scale cyber war can be deterred using a strategy of *deterrence by punishment*, but deterrence fails to prevent ongoing limited-aims cyber attacks due to the issue of plausible deniability. Moreover, international legal frameworks fall short because states cannot credibly commit, even states could credible commitment the issue of adequately balancing humanitarian concerns and military necessity poses a challenge. As controlling behavior through traditional deterrence or purely rationalist legal frameworks fail with respect to limited-aims cyber attacks, this paper considers the possibility of changing states' preferences as a means of addressing the problem. By allowing an agency/structure dichotomy to enter into the analysis, this paper explores the potential for norms in bolstering cyber deterrence. Although the development of new norms of behaviour is still in its early stages, there is evidence of states asserting their role in the process, acting as norms entrepreneurs in an attempt to shape state preferences in cyberspace.

Table of Contents:

Acknowledgments:

I offer my enduring gratitude to the faculty, staff and my fellow students at the UBC, who have supported me through this process. I owe particular thanks to Dr. Katharina Coleman, whose attention to detail and continuous encouragement showed me clarity and patience is the key to successful writing.

I thank Dr. Brian Job for acting as my second reader, as well as pushing me to be more outspoken in an academic setting, by far one of my greatest challenges over the past year.

Special thanks are owed to my parents, who have supported me throughout my years of education, both morally and financially. Also to Katie Meredith, your editing skills made the past few months much easier.

1. Introduction

In recent years the term *cyber war* has come to dominate the international security landscape, but questions still surround the possibility and nature of such a war. As one analyst aptly described, "cyber warfare has assumed the shape of an elephant, assessed by a group of blind people, with everyone drawing different meanings based upon their perceptions".[1] The domain of cyberspace remains a field of great debate among policy makers and security analysts alike. Moreover, many analysts dismiss the relevance of cyber arms control discussions on the basis that "information – the central ingredient of cyberwarfare – is thought to be impossible to control in today's digitally networked and highly distributed environment".[2] Such arguments center on the assertion that traditional strategic approaches to arms control, such as deterrence, may not be suitable mechanisms for limiting cyber attacks in the international system.[3]

Yet to completely dismiss the potential of strategic deterrence in cyber warfare would be incorrect. This paper contends that states may, in fact, be moving towards strategic deterrence, enabling the prevention of a major cyber war campaign. This trend is evidenced by the initial development of offense-dominant cyber strategies.[4] What remains a real concern in the international system, however, is the prevalence of limited aims cyber attacks. Due to issues of plausible deniability surrounding cyber technology, limited aims cyber attacks remain tactically viable despite strategic deterrence, inflicting relatively high costs with little fear of retribution. In other words, a strategic/tactical paradox exists in cyberspace whereby states are able to deter a potential cyber war but are

[1] Sharma 2010, 62.
[2] Diebert 2012, 31.
[3] Geers 2012.
[4] E.g. McCullough 2008.

not able to protect against a potentially costly cyber attack.

Rational Deterrence Theory (RDT), a theory that gained prominence during the post World War II era, postulates that states oftentimes adopt offense-dominant postures to prevent rather than start a conflict, driven by the logic of *deterrence by punishment* or Mutually Assured Destruction (MAD), a strategy contingent on the credible threat of offensive retaliation. However due to issues of plausible deniability and similarities between cyber and nuclear technology, RDT fails to provide a strategy for deterring tactical limited aims cyber attacks. It is important to note this paper is not concerned with cyber espionage, cyber terrorism, and cyber crime, which fall outside its scope of inquiry. Rather, this paper is interested in exploring two things: one, the ways in which states can deploy cyber attacks that aim at disrupting, paralyzing and possibly destroying another state's assets, with direct bearing on national security;[5] and two, the potential strategies for limiting the scope and number of these attacks in the absence of viable deterrence.

Divided into three main parts, this paper first utilizes Clausewitz's *Trinitarian Theory of Warfare* to conceptualize the strategic concerns currently facing states in cyberspace. Using this formulation, a nuclear comparison is introduced and conclusions are drawn about the inability of traditional deterrence strategies to discourage limited-aims cyber attacks. Second, this paper examines the potential use of existing legal frameworks for conventional arms control in cyberspace. The issue here is twofold: first, the problem of credible commitment, and second, the challenge of balancing humanitarian concerns and military necessity, a central principle in existing legal

[5] For similar definitions see-Billo and Welton 2004.

frameworks.[6] In response to the failure of both the deterrence and the legal approach to address the problem of limited aims cyber attacks, the third section suggests an alternative answer—the adoption of new norms in deterrence, acknowledging that state preferences may differ from traditional notions of national interest.[7] Moving away from the assumption of national interests as endogenously given, this section argues that states, in fact, are affected by logics of appropriateness in matters of strategic deterrence, therefore the development of norms can shape international behaviour in cyberspace. In the case of strategic cyber security, normative behaviours are emerging. Moreover, at a time where we expect to see civil society asserting itself in the process, it appears that policy leaders, United States (U.S), Russia, and China, are acting as both norms entrepreneurs and norms leaders in the development of strategic cyber norms.

[6] Engram 2010, 87.

[7] Traditional definitions of national interest include some combination of power, security, and wealth -see Morgenthau 1948.

2. Conceptualizing the Issues: Deterrence and its limits in cyber warfare

Different from the force multiplying impact of information-enhanced warfare, cyber war is a new paradigm of state warfare "used in principle to achieve strategic ends".[8] While technology has made an irrefutable impact on conventional warfare over the past few decades, cyber war is something separate. Strategic cyber war is a new type of state warfare, "capable of achieving the desired strategic ends by inducing a strategic paralytic effect onto an enemy nation, pushing it into chaos and mayhem"[9]. This strategic effect relies on the framework defined across the whole spectrum of affairs, right from the grand strategic to the tactical level.

The significance of cyber warfare is apparent when returning to classic formulations of the nature of war. In *On War* Clausewitz explains, "war is won when one side is able to compel its enemy to do its will",[10] while the great strategist Sun Tzu asserts, "the best type of warfare is the kind where you do not need to use physical force".[11] Ideally, cyber war embodies both strategic elements: belligerents are able to compel (by inducing strategic paralysis) but are able to achieve their desired ends almost completely without the use of physical force.[12] According Clausewitz, the key to achieving success in war is through the pursuit of the elusive Trinitarian warfare—a three-pronged strategic approach that recognizes that war has three key components: "blind force composed of primordial violence, hatred, and enmity; the play of uncertainty and chance in which the creative spirit roams; and the reason for violence or the political

[8] Sharma 2010, 64.
[9] Sharma 2010, 72.
[10] Clausewitz 1976, 583.
[11] Sun Tzu 1963, 77.
[12] Sharma, 2010, 65.

instrument".[13] Abstracted, these three components can be understood as "the people or the will to fight wars including finances, manpower, and support; the military or the means; and the leadership and direction essential for the functioning of the nation". [14] Victory in war, according to the Trinitarian theory, is accomplished by paralyzing these three key components of one's opponent simultaneously, or in contemporary strategic terms, through parallel warfare.[15] An attack against all three components at once causes a '*cascade effect'* resulting in a strategic paralytic hold on the nation.[16]

However, even Clausewitz doubted the possibility of a Trinitarian campaign. Intensely skeptical of any positive doctrine that was not highly context-specific,[17] Clausewitz asserted, "Our task . . . is to develop a theory that maintains a balance between these three tendencies".[18] Victory can only be achieved by controlling all three components simultaneously; a considerable task at the time, and an overwhelming task today given the unstable and shifting relationships between public, government and military. This unpredictable relationship ultimately limits the possibility of achieving such a strategic paralytic hold, and over the past century this type of attack was only thought achievable in the case of a nuclear attack.

The development of cyber attack capabilities challenges this assertion. A key similarity between nuclear technology (hereafter referred to simply as nuclear) and cyber technology (hereafter just 'cyber') is that they approximate Trinitarian warfare. Both technologies are capable of producing strategic paralysis: nuclear because of it

[13] Clausewitz 1976, 89.
[14] Sharma 2010, 64.
[15] Clausewitz 1976, 583.
[16] Ibid.
[17] Clausewitz 1976. The author spends much of the second half of this book dealing with these concerns.
[18] Ibid, 89.

overwhelming lethality, and cyber because of the overlapping and interpenetrating character of private and public information systems.

The new domain of cyberspace has transformed the modern security landscape in a way similar to the dynamics of the Cold War, making a Trinitarian cyber-campaign a real possibility. Broader than the Internet, cyberspace includes an "entire spectrum of networked information and communications systems worldwide". [19] These new digital systems, now commonly recognized by governments as critical infrastructure, permeate all levels of civil society, military and government. The modern world's reliance on technology is not a luxury, but a necessity; [20] all three components of Clausewitz's Trinity are dependent on cyberspace one way or another.

> "People rely extensively on computers and cyber assets for almost all of their daily chores (utilities such as gas and electricity, health, transportation, and banking facilities rely on cyber or network assets), modern militaries depend considerably on information assets and cyberspace, and governments rely on criminal records and other coordination networks, such as emergency response and recovery networks."[21]

A Trinitarian cyber campaign could cause the systematic shutdown of networks that allow for the normal functioning of society.[22] A parallel cyber campaign—an attack against all three components—would cause mass confusion rather than mass destruction. Despite little bloodshed, the outcomes on infrastructure, national security, and, in a time of conflict, military strategy, could be devastating.

By conceptualizing cyber war, not simply as a force multiplier, but a new paradigm in strategic warfare, the question becomes 'what strategies are available for states to protect themselves against this this new security concern?' In order to answer this question we first need to clarify what types of attacks constitute cyber war. This paper

[19] Deibert 2012ii, 1.
[20] Sharma 2010, 67.
[21] Sharma 2010, 65-67.
[22] Lewis 2010.

divides the cyber attacks used in cyber war into two categories: 1) an unlimited aims attack (ULAA), and 2) a limited-aims attack (LAA). A ULAA is the type of attack we would expect to see in used in Clausewitz's Trinitarian approach, it is not merely a single attack against one component of critical infrastructure, rather it is a series of simultaneous attacks aim government, military and civilian technologies with the goal of inducing a strategic paralytic effect of the entire state. A LAA attack can be best described as an attack against only a single component of Clausewitz's trinity. In the case of the LAA, the goal of the attack is primarily tactical, aiming to disrupt the partial functioning of state infrastructure in order to achieve some limited goal. An LAA is used by states attempting to power maximize through attritional attacks or as a barging tool.[23] In other words, the difference between the two categories of attacks is not the method of attack because both deploy malicious technologies (e.g. botnets, service-of-denial attacks, etc.), rather it is the goal if the attack itself.

It is important to note that a ULAA can only be undertaken by the more powerful states in the system. As it currently exist, there are few states with a monopoly of power in cyberspace.[24] Despite the ease by which new malicious cyber technologies can be acquired, an attack of this scale would need level of state resources only available to those strong states. Moreover, it is likely a ULAA would need to be followed by some military action in order to hold the newly acquired territory. The following sections (2.1 and 2.2) assess the potential for deterring both ULAAs and LAAs in the international system.

[23] See Mearsheimer 1999.
[24] Adam Liff 2012.

2.1. The Possibility of Cyber Deterrence – Offensive capabilities development and deterrence of unlimited aims cyber attacks

In addition to the Trinitarian approximation, in managing the threat of ULAAs, we can draw lessons from nuclear because of six critical similarities between the two technologies: 1) the superiority of offensive over defensive;[25] 2) the possibility of first and second strike scenarios; 3) the potential creation of automated responses when time is short; [26] 4) the likelihood of unintended consequences and cascading effects when a technology is new and poorly understood;[27] 5) the belief that new weapons are "equalizers"; and 6) the constant development of new technologies. These similarities lead to adopting one strategy of deterrence over the other. Like nuclear, strategic *deterrence by punishment*, not *deterrence by denial*, works for cyber, but only in the case of large-scale attacks cyber war, leaving the issue of limited aims unresolved.

RDT is centered around two central strategies with the goal of dissuading an adversary from undertaking an action that it has not already started through fear of the consequences: *deterrence by punishment* or MAD, a strategy that centres on a credible threat of offensive retaliation, and *deterrence by denial*, a defensive strategy in which a potential aggressor is convinced that the offensive and defensive balance is such that an offensive attack cannot succeed and therefore should be avoided. Moreover, according to Achen and Snidal, two key components are crucial for the success of RDT: the

[25] Despite the superiority of offensive over defensive cyber technologies, many technologies are both (retaliatory, as well as, defensive). Evidence of cyber technology use for defensive purposes is NATO's 2010 declaration that cyber-security is to be a defensive collective obligation, if member states should face a catastrophic cyber-attack all states would respond. This is further substantiated by counties such as the United Kingdom; South Korea; India; China; and Russia, who have since 2007 reinforced their cyber defenses,"[by] including anything from recruiting future cyber-warriors to establishing full blown cyber commands—Hughes 2010, 530.
[26] Nye 2011, 23.
[27] Ibid.

credibility of the deterrence capabilities, and the rational actor assumption of decisions rely on a cost-benefit analysis.[28] In other words, cyber deterrence is pursued by rational actors undertaking a cost benefit analysis before making logical decisions,[29] where states only engage in conflicts when they expect to win or from which they expect to at least yield a net gain. Therefore the proliferation of any cyber-technology that lowers a weaker state's estimation of the power/capabilities gap between it and a stronger adversary can thus be expected to make war more likely.

Keeping these assumptions in mind, returning to the similarities between nuclear and cyber, we can assess the potential of both deterrence strategies—*deterrence by punishment* and *deterrence by denial. Deterrence by denial* would fail in the case of cyber war as its success is contingent the superiority defensive of offensive, which is reversed in the cyber (similarity # 1). Moreover, the equalizing character of the technology (similarity # 5) and constant development of new technologies (similarity # 6) changes the potential damage a weaker state is capable of inflicting, no longer giving the stronger state a clear defensive advantage. In the case of cyber the stronger state cannot depend on the credibility if its capabilities and can no longer credibly signal to the weaker adversary a defensive advantage. In turn, this increases the weaker state's estimation of the power/capabilities gap, increasing the potential for cyber war.

By contrast, *deterrence by punishment* is more likely to be successful today. Firstly, the transformative nature of the technologies due to constant development of new technologies (similarity # 6) engenders an acute lack of understanding of cyberspace. We face a scenario where states have a limited understanding of the current security

[28] Achen and Snidel 1998, 139-169.
[29] Sharma 2010, 71.

landscape; the constant development of new technologies has created a learning experience for both government and private industry as they try to adopt new strategies to handle the technology.[30] While U.S. cyber technologies trace back as far as 1991, with the latest being released in 2013,[31] observers argue it remains far from comprehensively capable of dealing with the current cyber security dilemma.[32] This is not so different from the nuclear era, where Earnest May once described the U.S. nuclear defense policy following the end of World War II as 'chaotic.'[33] This chaotic environment has become the background against which actors must make their decisions. In a scenario where technology is new, an actor can be only somewhat more sure of their own defensive capabilities than their adversaries, and with deterrence by denial not an option, actors undertaking any kind of cost benefit analysis are left with the only of option of second strike capabilities (similarity # 2), dependent on automated responses (similarity #3) capable of producing a cascading effect (similarity # 4).

For this logic to hold, it is necessary to recognize that while the goal of a ULAA is to induce a state wide strategic paralytic effect the reality is something separate. Due the continuous evolution of cyber technology, the ability to create such an effect is fleeting. Unlike the early post-World War II era, where states perceived no retaliatory capacity—an actual condition for the Russians, a perceived one for the West—this is not the case with cyberspace. With growing evidence of states developing offense-dominant cyber strategies, the continuous development of cyber of offensive and defensive, and the clandestine nature of the technology itself, it appears there is no way to ensure a

[30] Ibid, 23.
[31] Ibid.
[32] Ibid.
[33] May quoted in Nye 2011, 23.

Trinitarian attack would be achieve such lofty goals. This leads to uncertainty regarding potential second-strike attack capabilities, it would be unwise for a state to presume an adversary is unable able to achieve some sort of retaliatory attack outside the targeted infrastructure. Essentially, the same reasons why the strategy of 'deterrence by denial' fails—offensive over defensive, the equalizing character of the technology, and the constant development of new technologies—is the same reason why 'deterrence by punishment' is likely to be an effective strategy in cyberspace.

However, evidence of this scenario unfolding in cyberspace today remains limited. While media reports suggest countries such as the U.S., the United Kingdom, China and Russia have been pursuing offense-dominant strategies, details including broad outlines and total spending levels remain classified information.[34] One alternative explanation for the pursuit of offense-dominant strategy development is it allows certain states to challenge the status quo. While this may be true for weaker states who aim at acquiring a cyber arsenal capable of limited aims cyber attacks (this issue is dealt with in the following section), it is unlikely powerful states have this goal in mind as costs inflicted would likely exceed any net gains. Logically, the adoption of offense-dominant strategies is more likely an attempt by states to maintain, not change, the status quo.

Although evidence is limited, some preliminary evidence for the deterrence argument can be found in the United States' 2006 National Military Strategy for Cyberspace Operations. The document notes:

> "Offensive capabilities in cyberspace offer the United States and our adversaries an opportunity to gain and maintain the initiative. DOD cyber operations are strongest when offensive and defensive capabilities are mutually supporting. This requires a long-range

[34] Menn 2013.

focus and dedicated resources to achieve this goal.[35]

Although this document lacks sufficient evidence to suggest a broad international shift towards offense-dominant cyber strategies, it does suggest that the U.S, the country with the "most robust, sophisticated, and technically and institutionally up-to date cyber posture",[36] recognizes the need for development of offensive cyber capabilities. What is lacking in this statement is to what ends the development of offensive capabilities will be used.

However, U.S intentions are becoming clearer. In March of 2013 the U.S. admitted to the development of offense cyber war units, with thirteen teams in total. During a meeting of the Senate Committee on Armed Services, General Keith Alexander, head of the National Security Agency (NSA) and commander of the US Cyber Command, highlighted the offensive directive of the new military units, stating, "This is an offensive team that the Defense Department [will] use to defend the nation if it were attacked in cyberspace".[37] This statement clearly highlights the pursuit of offense for the purpose of defense, and therefore work to support the above theory that states, or at least the U.S., is attempting to secure itself against large-scale cyber war using strategic deterrence by punishment.

Despite the lack of details provided describing the exact directive of these new war units, we can hypothesize what an offensive second-strike response would encompass. A crucial component for the success of a strategy, which uses offense as defense, is the development of countervailing capabilities. As described by Sharma, a successful second-strike response might look as follows:

[35] Department of Defense 2006, 1-10.
[36] Saltzman 2013, 45.
[37] Keith Alexander, 2013.

> "Cyber triad capability can consist of regular defence/military assets and networks as forming the first section of the triad, the second section being an isolated conglomerate of air-gapped networks situated across friendly nations as part of cooperative defence, which can be initiated as a credible second-strike option, and the third section consisting of a loosely connected network of cyber militia, involving patriotic hackers, commercial white hats and private contractors, which can be initiated after the initial strike or in case of early warning of a potential strike".[38]

Reminiscent to a nuclear triad, [39] the aim is to achieve retaliation through the creation of automated responses in a short span of time achieving paralleled warfare resulting in the complete paralysis of government, military and society. [40] If this is in fact the formulation of U.S offensive capabilities, or that of other states, remains to be seen and is beyond the scope of this paper. What is apparent is that deterrence through the development of an offensive cyber arsenal is an effective means of limiting a large-scale cyber war and likely the way of going forward. Moreover, despite the its Trinitarian approximation, an unlimited aims cyber attack may be unlimited it its goals but likely limited to achieve it due to the potential of counter strike capabilities.

2.2. The Failure of Cyber-Deterrence: Limited aims cyber attacks and issues of plausible deniability

With nearly two billion citizens connected in cyberspace and over a hundred countries developing cyber arsenals with comparable capabilities that will intensify in the future,[41] the occurrence of LAA, such as Titian Rain (2003 through 2005), Stuxnet (2010), and those experienced in Estonia (2007) and Georgia (2008), remain an acute threat in the

[38] Sharma 2010, 69.

[39] A nuclear triad refers to a nuclear arsenal made up of three elements, intercontinental ballistic missiles (ICBMS), strategic bombers, and submarine launched ballistic missiles (SLBM). Its purpose is to ensure a credible second strike.

[40] Liff 2013, 222.

[41] Hughes 2010.

international system. Unlike the ULAA, attacks of this nature have specific tactical aims striking primarily at a single component of Clausewitz's trinity.[42] For example, the attacks on Estonia and Georgia were targeted to cripple civil infrastructure, while Titian Rain was a series of hacker attacks against American government systems aimed at gaining access to military data. Although attacks such as these are not intended to induce the same paralytic effect as a ULAA, LAA are capable of inflicting relatively high costs with little fear of retribution, creating a major security concern in the international system.

Conceptualized differently, a limited aims cyber attack is similar to proxy warfare—a method of warfare where opposing powers use third parties as substitutes for fighting each other directly. The goal of proxy war is to inflict costs on an opponent without direct contact, in the hope that further escalation leading to war will not occur. A limited-aims cyber attack serves a similar purpose. The origins of cyber technology are often times undetectable and attacks are seldom possible to trace, able to evade detection by exploiting poorly secured computers and using those hijacked systems as proxies through which they can launch and route attacks worldwide. The resources spent on a cyber attack are inconsequential relative to the amount of man-hours and financial investment it would take to track actors down and identify them as instruments of a particular state. This anonymity allows belligerent states to inflict relatively high cost with little fear that the attack will prompt retaliation escalating into a larger conflict.

The perfect example of a limited-aims cyber weapon capable of achieving such ends is the Stuxnet virus. This virus, a piece of malware discovered by security company VirusBlok Ada in 2010, appeared to be designed to target Iranian nuclear facilities in the

[42] Sharma 2010, 67.

hope of shutting down Iran's nuclear program. Its origin is the subject of much speculation. Experts studying Stuxnet consider that the complexity of the code indicates only a nation state would have the capabilities to produce it.[43] This claim is further supported by reports coming from the Russian digital security company Kaspersky Labs, which concluded that the attacks could only have been conducted "with nation-state support".[44] Thus, while it is difficult to attribute the exact source of the attack, it is clearly a state sponsored attack. Stuxnet was able successfully inflict cost by attacking Iran's nuclear program, and avoid escalation by remaining untraceable upon discovery.

However, like proxy war, a limited-aims cyber attack is not without risk: Military strategists are becoming increasingly concerned that such an attack may, in fact, escalate into a larger conflict between states. Due to the "newness of technology . . . and the potential to misidentify an [attack] as the opening phase of a military action, cyber conflict entails a greater risk of miscalculation and inadvertent escalation of conflict".[45] Therefore, states that possess advanced cyber capabilities must tread cautiously. As states continue to arm themselves, there is a growing international consensus that an attack against critical infrastructures could be deemed an act of war triggering a potential military response: "If you shut down a power grid, maybe we will put a missile down one of your smoke stacks".[46]

In addition, this is not the only way in which a limited-aims cyber attack can escalate into larger military conflict. An alternate instance where this type of attack leads to conflict is in a bargaining scenario. In this case the addition of cyberwarfare

[43] Kaspersky Labs 2010.
[44] Markoff 2010.
[45] Lewis 2013, 5.
[46] Gorman and Barnes 2011.

capabilities may affect perceptions, bargaining dynamics, and the probability of conflict between actors. A state, strong or weak, can develop a cyber arsenal in an attempt to strengthen its bargaining position. With the addition of a cyber arsenal, the expected outcome of this strategic interaction would not be war but a negotiated resolution with a better bargain for the weaker state than it would have otherwise. However, disparate perceptions – *asymmetric information* – about relative power and resolve may render a mutually-acceptable bargain unattainable, thereby increasing the probability of war.[47] In this scenario the probability of escalation is particularly high.[48] In a strong state and superpower dyad, a strong state with limited objectives risks underestimating the superpower's resolve and willingness to escalate to a higher level of conflict.[49] In this scenario conflict is likely to occur when "misperceptions about relative resolve may weaken the superpower's conventional deterrent".[50] Again, this outcome is analogous to cases in a weak state vs. strong state/super power dyad because weak state underestimates resolve and willingness to fight. The only difference being a weak state would not have the brute force needed for any type of second-strike retaliation.[51]

Due to the potential for escalation of conflict, limited-aims cyber attacks remain a major security concern for states. Unfortunately, neither *proactive denial* nor *reactive punishment* suitably deter potential attacks. The unique characteristics of cyber technology prevent successful deterrence and work together to create a level plausible deniability among states. This plausible deniability is the primary reason limited-aims cyber attacks remain a threat in the international system.

[47] Fearon 1995.
[48] Liff 2013, 224.
[49] Ibid.
[50] Ibid.
[51] Ibid, 225.

For deterrence to work, states must be able to dissuade an adversary from undertaking an action through fear of consequences. If a state is unable to identify an attacker, the adversary no longer needs to fear such consequences. For smaller scale attacks, the key problem impeding deterrence is the relatively simple means of acquiring, deploying, and hiding cyber technology and cyber weapons, making cyber threats almost impossible to identify, define, and monitor. [52] Cyber technology is readily available due the commercial predominance and the affordability, and therefore barriers for weaker states are relatively low – certainly much lower than in the nuclear realm.[53] Acquiring a 'botnet' to carry out a digital attack in cyberspace is easy and affordable. For example, in 2001 a teenage boy was able to inflict $1 billion in corporate losses after the successful denial of service attack—a digital attack aimed at disrupting the service of a host or provider—making the network resource unavailable to its intended audience. [54] In addition, cyber intrusions (such as a logic bomb—a piece of code intentionally inserted into a software system setting off a malicious function when specified conditions are met) can go unnoticed for long periods before being used, and even then are often difficult to trace.[55] Furthermore, it has become increasingly common for states to outsource the illegal business of hacking to commercial organizations or third party criminals.[56]

These characteristics work simultaneously to provide a level of plausible deniability for states making deterrence virtually impossible. Due to the potential for outsourcing, the affordability, and the clandestine nature of a cyber technology it becomes almost impossible to discourage a state from acquiring a cyber arsenal. Once a

[52] Ibid.
[53] Ibid.
[54] Verton 2002.
[55] Owens, Dam, and Lin 2009, 294.
[56] Geers 2010, 299.

cyber weapon is obtained, the plausible deniability attached to a limited-aims cyber attack provides few incentives for states to refrain from attacking an adversary.

3. The Limits of Legal Mechanisms for Addressing Limited Aims Attacks

With deterrence ill-equipped to handle limited-aims cyber attacks and a real potential for escalation, the core issue remains the prevention of limited-aims cyber attacks in the international system. One alternative approach to limiting such attacks is by utilizing existing legal frameworks, drawing comparisons between cyber attacks and other conventional forms of warfare.[57] However, using existing legal frameworks for conventional arms control in cyberspace is not without its challenges. The issues here are twofold: first, there a problem of credible commitment, and second, even if states could credibly commit, there is the remaining challenge of balancing humanitarian concerns and military necessity, a central principle in existing legal frameworks.[58]

Although international discussions around effective cyber arms policy and law have begun, current international cooperation places emphasis on the need to deter criminal efforts and apprehend cyber terrorists rather than restricting state sponsored attacks. Various institutions within the United Nations (U.N.) have created policies addressing international cyber terrorism and combatting the criminal misuse of information technology.[59] For example, 2000 the U.N. General Assembly adopted Resolution 55/63 addressing the various ways states can work to combat the criminal misuse of information technologies; in 2002 it adopted Resolution 57/239 on the creation of a global culture of cyber-security; and in 2003 it adopted Resolution 58/199 on the creation of a global culture of cyber-security and the protection of critical information

---

[58] Engram 2010, 87.
[59] Scholberg 2010, 11-12.

infrastructure, to collectively aid in confronting non-state actors who engage in unlawful attacks against global information systems.

There is less evidence of international cooperation prohibiting offensive cyber tactics due to legal and technical actions. One U.N. working group, with the support of the U.S. and China, has been exploring the possible end of anonymity online through infrastructure alterations to cyberspace through the development Internet Protocol Trace-Backing—a process which attempts to reliably determine origins of cyber intrusions.[60] However, in the Fall 2012 over 20 countries, including the U.S., boycotted of any discussion of an international agreement addressing international Internet control, contradicting the previous initiative.

One explanation for the absence progress for this policy area is the continuous evolution of cyber technologies and undisclosed capabilities of governments. Due to the strategic advantage provided by these characteristics, states are unable commit to possible international restrictions placed upon them despite risk to civilians and civilian infrastructures. As Fearon[61] and Powell[62] have shown, an enforceable deal often requires states to make a credible commitment not to exploit a first-strike advantage, a large exogenous shift in power, or a shift in power that derives from possession of the disputed good. Due to the tactical offensive advantage of a limited-aims cyber attack, the equalizing potential of cyber weapon, and ease of access to technology, it is unlikely states could credibly commit to an enforceable deal restricting limited-aim cyber attacks in the near future.

---

[60] McCullough 2008.
[61] Fearon 1995.
[62] Powell 1999, 2004, 2006.

As long as cyber arms remain relatively cheap and readily available, limited-aim cyber attack remains an attractive means of circumventing the Law of Armed Conflict (LOAC) that govern other conventional arms. However, if states were able to solve their commitment problem, the application of existing legal frameworks remains problematic because of the inability to define the legal norm of 'necessary force' for a cyber-attack. Necessary force, a concept that balances humanitarian concerns and military necessity, is a defining concept of the LOAC. [63] It is this balance between military necessity, which authorizes the use of force required to accomplish a mission, and the principle of humanity, which demands military force must minimize unnecessary suffering, that proves challenging in cyberspace.

The concept of necessary force is becoming increasing difficult to define in cyberspace as critical infrastructure continues to integrate private and military systems, decreasing the ability to differentiate between the two. Take the case of the 2007 attacks against Estonia, a country often know as "eStonia", as it has "instituted an e-government in which ninety percent of all bank services, and even parliamentary elections were carried out via the Internet". [64] The attacks targeted Estonian organizations, including Estonian Parliament, banks, ministries, newspapers and broadcasters. The challenge is differentiating between civil and military targets and deciding what are legitimate justifications to attack a military target wherein dual-use infrastructure such as water, energy and transport networks are involved.[65] For an international agreement to be reached, states would need to come to some agreement of what is necessary force for a cyber attack. With states focused primarily the role of non-states actors, the inability of

[63] Engram 2010, 87.
[64] Shackleford 2009.
[65] Hughes 2010, 538.

states to credibly commit and the unlikelihood of states to agree on legal limits in cyberspace, there is limited potential for existing legal frameworks to address the issue of ongoing limited-aims cyber attacks.

4. The (Potential) Answer: Norms for cyber deterrence

Ways of controlling behavior through traditional deterrence or purely rationalist legal frameworks fail with respect to limited-aims cyber attacks; consequently, we must consider the possibility of changing states' preferences as a means of addressing the problem. By allowing an agency/structure dichotomy to enter into the analysis, we recognize that states are not merely unitary actors exhibiting behaviours arising from exogenously given interests; rather, the behaviour of states is a product various actors' decisions based on expectations developed through intersubjective beliefs about the material and social world. In reality, decision makers can be reflective goal-directed individuals, their decisions affected by various social, economic, and historic forces.[66] Examining the actor's choices and the structures which affect them can provide an alternative mechanism by which to address limited-aims cyber attacks.

The follow section argues that the challenge is to change and introduce new norms, logics of appropriateness based on a moral standard of behaviour, to nascent cyber strategies may allow states to achieve a form of cyber deterrence above and beyond norms of rational 'self-interested' militarily action and existing legal frameworks. To understand how and why this is the case, first, we address norms and their ability to change states' preferences; second, we revisit the relationship between norms and deterrence; and third we examine how "norms and deterrence are related in the current efforts of the U.S. to promote certain norms norms through global policy and strategy".[67] It appears the U.S. is attempting to counter balance other actors, such as Russia and China, who are also acting as norm entrepreneurs but have conflicting interests and

[66] Finnemore 1996.
[67] Stevens 2012, 149.

ideology.

4.1. Norms and Preferences: Intersubjective beliefs between material and social worlds

Finnemore defines norms as "shared expectations about appropriate behaviour held by a community of actors".[68] Expectations emerge "from intersubjective beliefs about the social and material worlds, and therefore these expectations do not exist in the private subjective beliefs of individuals but in public social relationships between individuals and in shared practices".[69] Norms are commonly differentiated as constitutive norms and regulatory norms. Constitutive norms, "define the set of practices that make up a particular class of consciously organized social activity – that is to say, they specify what counts as that activity". [70] Meanwhile regulatory norms "define the basic 'rules of the game' in which actors find themselves in their interaction".[71] Regulatory norms differ from instrumentally-driven rational behaviour because actors attempt to 'do the right thing' rather than purely maximize or optimize their non-normative preferences.[72]

4.2. Revisiting the Role of Norms in Deterrence

Norms do not require the exercise of material power to persist or proliferate, however, "they are more likely to do so if they either serve material interests or are supported by them".[73] According to Finnemore and Sikkink, actors can engage in 'strategic social construction' whereby "actors are making detailed means-ends calculations to maximize

[68] Finnemore 1996, 22.
[69] Wendt 1999, 73-74.
[70] Ruggie 1998, 871.
[71] Risse 2000, 4
[72]. Raymond 1996, 214.
[73] Stevens 2012, 156.

their utilities, but the utilities they want to maximize involve changing the other player's utility function in a way that reflects the normative commitments of the norms entrepreneurs."[74] Therefore norms may be adopted either "because an actor is interested in 'doing the right thing' and also because it is seeking to maximize personal utility in doing so".[75] The study of norms does not dismiss actor can exhibit rational choice behaviour but "seeks to augment and deepen the understanding of actors' strategic decision-making"[76]. The addition of norms to the study of deterrence, allows for the addition of the structure/agent dichotomy to enter into analysis where it is ignored by purely rationalist approaches to deterrence.[77]

Argued by Lawrence Freedman, a normative approach is more appropriate for understanding how deterrence actually works in practice.[78] Freedman asserts a 'norms-based approach' to deterrence – rather than a strictly 'interests-based approach'-- reinforces "certain values to the point where it is well understood that they must not be violated".[79] Contrary to the use or threatened use of military force alone, the norms-based approach to deterrence requires the exercise of many elements of foreign policy.[80] By attaching political cost to the use of a particular class of weapon, even on the small scale can aid in deterrence.[81] Although these norms may not be prohibitive, the addition of political costs may result in a government's compliance.[82]

Additionally, deterrence strategies demand that rational actors "hold normative

[74] Finnemore and Sikkink 1998, 910.
[75] Steven, 2012, 156.
[76] Ibid.
[77] Freedman 2004, 5.
[78] Ibid, 4.
[79] Ibid.
[80] Ibid.
[81] Ibid, 71.
[82] Ibid.

assumptions about the appropriateness and proportionality of military actions",[83] while being aware of the "rules and logic of the [strategic] game', which is communicated between actors in a two player game and serving to inform their actions and identities.[84] Overtime norms become mutual, internalized assumptions that are broadly recognized as constitutive of international order[85] and, therefore, norms define a behavior that will no longer be tolerated and do this in a way that allows for deterrence to become instinctive to the community members.

The attachment of norms to cyber deterrence is crucial for the future of limited aims cyber attacks. The norms needed in cyberspace are whole or partial prohibition of limited-aims cyber attacks, which aims at protecting civilian populations. In the past normative assumptions have attached themselves to particular weapons regimes (i.e. nuclear, chemical/biological, and land mines) no longer making them a viable use of force among the international community creating a taboo, or norm of non-use. Such normative assumption can lead to regulatory norms: "The patterns of non-use cannot be fully understood without taking into account the development of prohibitory [or regulatory] norms that shaped these weapons as unacceptable 'weapons of mass destruction'.[86] As the dependence of society on cyberspace continues to grow, the attachment of social norms and cultural meanings to cyber weapons would allow new normative understandings to shape the interests and the identities of the actors involved and, therefore, shape practices.

[83] Adler 2009, 88.
[84] Ibid.
[85] Bull 1977.
[86] Price et al, 1996, 114.

4.3. Norms in Cyberspace: The potential for norms and cyber deterrence

It is the establishment of such logics of appropriateness that remains a major contention in cyber deterrence today. Despite the acute need, the international community has yet to establish an international regime of cyber norms. Norms are, however, beginning to emerge in cyberspace with the assistance of states as norms entrepreneurs. [87] In the case of cyber governance, states are working alongside civil society actors asserting their interests in issues of global governance, shaping cyberspace itself. [88] While in the case of cyber deterrence, states are acting as primary norms entrepreneurs with this policy area receiving little attention from civil society actors.

Over the past decade global governance in cyberspace has been pushed to the forefront of international discussions,[89] with governments becoming increasingly influential across a number of governance forums. This has included deliberations on how to exercise power in and through cyberspace, with deep divisions between democratic and authoritarian regimes. Western liberal democracies are "moving away from laissez-faire and market-oriented approaches to more state-directed controls and regulations focusing on issues of authentication and proper functioning of the networks that support global trade, finance, and communications. [90] Nondemocratic states such as Russia and China have begun to forcefully assert their interests, "focused on regime control in various cyberspace governance regimes, including some, like the International Telecommunications Union, which were previously marginalized in the Internet space". [91]

Norms for cyber deterrence, however, are less palpable but there are some signs

[87] Finnemore and Sikkink 1998, 895.
[88] Deibert and Crete-Nishihata, 2012.
[89] Deibert 2012ii.
[90] Deibert and Crete-Nishihata, 2012
[91] I.bid

of their emergence. In particular, the work done by Tim Stevens provides growing evidence in the contemporary discourse and practice of the US cyber strategy, which clearly recognizes the need for regulative norms in an effort to signal to states that a responsible member of the international community should refrain from conducting limited aims cyber attacks.[92] Steven provides a series of examples of from recent policy documents, which exhibit the addition of new norms, put forward by the U.S. Since 2008, the United States, aware of the potential damage inflicted by limited aims cyber attacks and the inability to deter or defend against them, has recognized the importance of norms for preventing limited-aims cyber attacks. The Center for Strategic and International Studies (CSIS), a think tank commissioned by President George Bush, first raised this concern in their position on cybersecurity set out by the nongovernmental Commission on Cybersecurity for the 44th Presidency, providing strategic insights and practical policy solutions to decision makers on matters of cyber deterrence, stating:

> The U.S. willingness to cooperate with other governments on cybersecurity will be an important component of U.S. advocacy. That cooperation should focus on establishing norms, which are expectations or models for behavior . . . A normative approach to international cybersecurity focuses on how countries should behave.[93]

According to Stevens, norms along with deterrence were proposed together as part of an "international engagement" strategy, involving "advocacy, cooperation, norms, and deterrence".[94] The Commission envisaged that norms would be promoted and propagated using a combination of inducement and coercion. Compliance would be capable through 'embarrassment or stigmatization' as a result of violation.[95]

Two years later, under President Obama, many of the ideas contained in the

[92] Stevens, 2012, 157.
[93] CSIS Commission on Cybersecurity 2008 quoted in Stevens 2012, 158.
[94] Ibid.
[95] Ibid.

commission's report were then incorporated in to the *2010 Cyber policy Review*, which assess US policies and structures for cybersecurity.[96] The Review stated:

> The Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force. International norms are critical to establishing a secure and thriving digital infrastructure. . . Only by working with international partners can the United States best address these challenges, enhance cybersecurity, and reap the full benefits of the digital age.[97]

As a consequence, in 2011, a policy document named the *International Strategy for Cyberspace* was formulated answering Obama's plea. The first sentences of the document stated government's aims to introduce "an approach that unifies our engagement with international partners on the full range of cyber issues".[98] Addressing norms promotion by "applying the broad expectations of peaceful and just interstate conduct to cyberspace . . . to effect stability", obtained in "other spheres of international relations".[99] Stevens notes that while the normative program is still in its early stages in the U.S., and no global U.S.-supported framework has emerged, "we are beginning to see the emergence of national cyber strategy in which cyber deterrence may be pursued not only through national security capabilities, but also through diplomatic, information, economic and political means". [100]

Conversely, some states, including Russia and China, have resisted these norms initiatives; citing cyberspace is a matter of national, their primary concern is regime control. Steven notes that in 2009 working through the Shanghai Cooperation Organization (SCO), alongside states such as Kazakhstan, Kyrgyzstan, Tajikistan and

[96] U.S White House 2009 quoted in Stevens 2012.
[97] Ibid
[98] Ibid
[99] Clinton 2011, 9 quoted in Stevens 2012.
[100] Stevens, 2012, 159.

Uzbekistan, Russia and China adopted an accord that defined "information war'" as the "dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other States".[101] And in 2009, China, Russia, Tajikistan and Uzbekistan presented the UN general assembly with a new code of conduct for cyberspace, calling for international security. Framed in terms of "information security", they proposed a variety reasonable measure of limiting the proliferation of cyber arsenals and prevention of cyber attack, but, notably, also proposed "information security' included the need to protect against information dissemination that may endanger a states' "political, economic and social stability, as well as their spiritual and cultural environment".[102]

This incongruence between U.S. lead initiatives calling for norms of cooperation and non-liberal/non-democratic states, such as Russia and China, primarily focused on regime protection has created a major obstacle for broad adoption of norms in cyberspace. At a time where states are acting as the primary norm entrepreneurs, the inability to convince one another of divergent logics of appropriateness may prevent any broad recognition of common standards of behaviour in cyberspace. However, despite acute differences over governance issues, states do appear to recognize the need to prevent future limited-aims cyber attacks. It is possible, over time, states may settle on some agreed-upon norm able to address this going security concern. When, exactly what they will be, and how they will be enforced is the subject for further research.

[101] Ibid.
[102] Letter to UN Secretary-General 2011 quoted in Stevens 2012.

5. Conclusion

Over the past few decades technology and warfare have undergone a major transformation. For the first time since the development of nuclear technology, states are faced with an international security threat that could disrupt the entire functioning of societies. Cyber warfare or Information warfare is strategic warfare, which derives the spirit of both Sun Tzu and Clausewitz, as it is a type of warfare that is capable of compelling the enemy to do one's will by inducing strategic paralysis to achieve the desired ends. However, by exploring the similarities between nuclear and cyber technologies—offensive advantage, their ability equalize power inequalities and continuous development technologies— it becomes clears states may, in fact, be able to deterring against cyber war by establishing countervailing capabilities able to induce a retaliatory paralytic effect. What remains the major challenge for policy makers and military strategists is the issue of limited-aims cyber attacks. Due to the unique characteristics of cyber technologies, which contribute to relatively simple means of acquiring, deploying, and hiding cyber technology, a limited aims cyber attack provides states' the cover of plausible deniability leading to problems of deterrence.

Recognizing controlling state behavior through traditional deterrence or purely rationalist legal frameworks fails to adequately address limited-aims cyber attacks, this paper suggests an alternate solution focusing on norms due to their ability to shape states' preferences. Norms and deterrence can work simultaneously; logics of appropriateness along with the potential use of coercion may be the answer. Despite evidence of norms developing in cyber deterrence, specifically in the case of the U.S. and its current cyber strategy, norms development in this area faces challenges due to conflicting interests and

ideology of states such as Russia and China.

Whether the effort to adopt norms regarding states' actions in cyberspace will be successful remains to be seen. In recent months, in response to an onslaught of cyber attacks against U.S. computer network, the U.S. has publicly accused China of launching a sophisticated range of cyber attacks on it which posed a risk "to international trade, to the reputation of Chinese industry and to our overall relations".[103] However, China has not admitted to the attacks nor is there any real proof such attacks will not happen again in future.

Going forward, an additional area of research may be to follow the development of potential norms and to analyse the extent to which they shape preferences and behaviours in cyberspace. Cyber deterrence discourse may never reach the level of nuclear and other weapons deemed illegitimate by the international community.[104] However, the similarities with between the two may, over time, serve to form and perpetuate the notion of a cyber taboo. The linkages between cyber and nuclear technologies may allow for the use of cyber as a deterrent, but not as a legitimate use of force. [105] Until a time where an international cyber-norms regime has been established and states reach a level of normative understanding making intrusive cyber technologies unacceptable, it appears they - and limited aims attacks in particular – will remain a real threat in the international system.

[103] Office of the Press Secretary, 2013.
[104] Price 1997, 101.
[105] See Price 1997, 101-102 for similar analogy between nuclear and chemical weapons.

References:

Achen, Christopher H., and Duncan Snidal. 1989. "Rational deterrence theory and comparative case studies." *World Politics* 41, no. 2: 143-169.

Adler, Emanuel. 2009. "Complex Deterrence in the Asymmetric-Warfare Era." *Complex Deterrence: Strategy in the Global Age*:85-108.

Billo, Charles, and Welton Chang. 2004. *Cyber warfare: An analysis of the means and motivations of selected nation states*. Dartmouth College, Institute for Security Technology Studies.

Bull, H. 2002. *The anarchical society: a study of order in world politics*. Columbia University Press.

Carr, J. 2011. *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly.

"Charter of the United Nations." 2010. *Welcome to the United Nations: It's Your World*.

Clausewitz, Carl von. 1976. *On War*, translated and edited by Michael Howard and Peter Paret." Princeton University Press

Clinton, Hilary. 'Internet Rights and Wrongs: Choices and Challenges in a Networked World', Washington, DC, 15 February 2011

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington, DC: White House, 2009)

Deibert, Ronald. 2012. Cyber Security. In T. H. Christian Leuprecht, Kim Richard Nossal (Ed.), *Evolving Transnational Threats and Border Security* (pp. 29-38). Kingston, ON: Centre for International and Defense Policy, Queen's University.

Deibert, Ron. 2012 "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace." *Journal of Military and Strategic Studies* 14, no. 2.

Deibert, Ronald. 2012. "The Growing Dark Side of Cyberspace (... and What To Do About It)." *Penn. St. JL & Int'l Aff.* 1:260-390.

Deibert, Ronald J., and Masashi Crete-Nishihata. (2012) "Global Governance and the Spread of Cyberspace Controls." *Global Governance: A Review of Multilateralism and International Organizations* 18, 3: 339-361.

Farrell, Theo. 2005. *The norms of war: cultural beliefs and modern conflict*. Lynne Rienner Publishers.

Freedman, Lawrence. 2004 *Deterrence*. Cambridge: Polity.

Finnemore, Martha 1996 "National Interests in International Society." *Cornell: Cornell*

Finnemore, Martha, and Kathryn Sikkink. 1998 "International norm dynamics and political change." *International organization* 52.4: 887-917.

Geers, Kenneth. 2010"The challenge of cyber attack deterrence." *Computer Law & Security Review* 26, 3: 298-303.

Geers, Kenneth. 2012 "Strategic Cyber Defense: Which Way Forward?." *Journal of Homeland Security and Emergency Management* 9, 1: 1-10.

Hughes, Rex. 2012 "A treaty for cyberspace." *International Affairs* 86, no. 2: 523-541.

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, DC: White House, 2011).

Lewis, James. 2007 "Cyber Attacks Explained." *CSIS Commentar*y.

Letter to UN Secretary-General, 12 September 2011, http://blog.internetgovernance.org /pdf/UN- infosec-code.pdf

Libicki, Martin C. 2011. "Cyberwar as a Confidence Game." *Strategic Studies Quarterly* 5 (2011)*:132-146*

Liff, Adam P. 2012 "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, 3: 401-428.

McGraw, Gary. "Cyber War is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies* 36, no. 1 (2013): 109-119.

Markoff, John. 2010 "A Silent Attack, but Not a Subtle One." *New York Times*, 26 Sept. 2010.

Nackashima, Ellen. "Control of Intelligence Budget Will Shift." *Washington Post*. Nov. 2010.

Nye, Joseph S. 2011. Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly*. Winter:20-38.

Owens, William., Dam, Kenneth., and Lin, Herbert., eds. 2009. *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington: National Academies Press.

U.S. Office of the Press Secretary, 2013. Donilon, Remarks By Tom Donilon, National Security Advisor to the President: "The United States and the Asia-Pacific in 2013".

U.S White House, 2009. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure

Center for Strategic and International Studies, 2008. *Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*. Washington, DC:, pp. 20–21.

Price, Richard. 1995."A genealogy of the chemical weapons taboo." *International Organization* 49: 73-73.

Price, Richard, Nina Tannenwald, and Peter Joachim Katzenstein. 1996 *Norms and deterrence: The nuclear and chemical weapons taboos*. Columbia University Press.

Ray, Charles A. 1997. 'Cyber War and Information Warfare: A Revolution in Military Affairs or Much Ado about Not Too Much?', *National War College Report*.

Raymond, Gregory A. 1997. "Problems and Prospects in the Study of International Norms." *Mershon International Studies Review* 41, 2: 205-245.

Risse, Thomas. 2000 '"Let's Argue!": Communicative Action in World Politics', International Organization, 54:1.

Ruggie, John Gerard. 1998. "What makes the world hang together? Neo-utilitarianism and the social constructivist challenge." *International organization* 52, no. 4 (1998): 855- 885.

Saltzman, Ilai. 2013."Cyber Posturing and the Offense-Defense Balance." *Contemporary Security Policy* 34, no. 1: 40-63.

Schjolberg, Stein. 2006. "Terrorism in Cyberspace–Myth or reality?." *Terrorism* 1:1.

Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency (Washington, DC: Center for Strategic and International Studies, 2008), pp. 20–21.

Sharma, Amit. 2010. "Cyber Wars: A Paradigm Shift from Means to Ends." *Strategic Analysis* 34, no. 1: 62-73.

Stevens, Tim. 2012. "A cyberwar of ideas? Deterrence and norms in cyberspace." *Contemporary Security Policy* 33, no. 1 (2012): 148-170.

Tzu, S. (1963). The Art of War. Translated by Samuel B. Griffith. *New York: Oxford University*.

Verton, Dan. 2003. *Black ice*. McGraw-Hill/Osborne.

War in the Fifth Domain. *The Economist* 3 July 2010: 25-28.

Wendt, Alexander. 1999. *Social theory of international politics*. Cambridge University Press.