MILITARY ESCALATION IN CYBERSPACE: MYTH OR REALITY?

AN ANALYSIS OF THE NECESSARY CONDITIONS TO REDUCE THE LIKELIHOOD OF MILITARY ESCALATION IN CYBERSPACE

Master of Arts in Law and Diplomacy Capstone Project

Submitted by NIKOLAS OTT

Under the advisement of Professor Michele Malvesti

May 2016

http://fletcher.tufts.edu

THE FLETCHER SCHOOL

TUFTS UNIVERSITY

Executive Summary

In July 2010, Stuxnet was discovered, a sophisticated malware that had infected Iranian nuclear facilitates causing physical damage. Such offensive military operations in cyberspace are in fact becoming more common. However, the likelihood of military escalation through such operations is contested and an exact threshold of military escalation in cyberspace remains unclear. This paper contributes to the discussion by reviewing recent case studies of military operations in cyberspace and identifying conditions that help reduce the likelihood of military escalation in cyberspace.

None of the case studies analyzed had a very high chance of military escalation in cyberspace. Victims of offensive operations generally responded in a proportionate manner that gave little reason for escalation. States seem to consistently operate below a certain threshold of military escalation, though the exact threshold remains unclear. The case studies also indicate that the most severe causes of military escalation in cyberspace originate outside of cyberspace, namely in geopolitical disputes and large-scale military confrontation between adversaries.

Therefore, it is evident that military cyber operations do not occur in a vacuum; they are affected by larger geopolitical trends, regional developments, internal political developments, and individual threat perceptions. For this reason, while a narrow and technical discussion about military operations in cyberspace is important, the debate about military escalation in cyberspace needs to become part of the larger field of international relations research and policy analysis in order to be truly effective at identifying means to properly address this challenge.

The key conditions identified in this paper to reduce the likelihood of military escalation in cyberspace are divided into several levels. On the state level, key conditions include: governmental transparency about military operations in cyberspace and extensive confidence-building measures on states' military operations in cyberspace. On the global level, key conditions

include: the existence of effective conflict prevention mechanisms, a precise understanding of how public international law applies to military operations in cyberspace, and the extent to which law limits military operations in cyberspace. On the cross-cutting level, key conditions include: an increase in globalization and economic interdependence among nations and a higher threshold for success for attackers in cyberspace. The threshold for success could be raised by more sophisticated and widespread cyber 'hygiene practices', an overall change in the imbalance between offensive and defensive operations in cyberspace, the absence of 'low-hanging fruit' or a reduction in software vulnerabilities, and an international environment that encourages states to focus on improving national resilience instead of concentrating exclusively on deterrence strategies. If none or only very few of these conditions are met, then the current increase in military and intelligence activities within cyberspace provides reason to worry about military escalation in cyberspace.

These conditions cannot be met without a proper and sustainable implementation process. While most of them need to be implemented by governments and international organizations, Internet businesses, and non-state actors also play key roles in facilitating the implementation process. Key suggestions of this paper include: providing international organizations with stronger mandates to facilitate the implementation process of the aforementioned global solutions; encouraging states to develop more sophisticated frameworks for collaboration with private businesses, increase national capacity building among diplomats and policy-makers, and put stronger emphasis on shifting the current imbalance between offensive and defensive military operations in cyberspace; urging academics and NGOs to call upon governments to improve transparency measures and promote improved 'cyber hygiene'; and motivating representatives of the media to roll back the 'military' discourse about cyberspace.

Table of Contents

Glossary

Term	Definition
Advanced Persistent Threats (APTs)	Generally referred to as APTs, this term refers to sophisticated attacks that normally require significant amounts of intelligence, technological knowledge and resources to create and deploy them.
Air Gap	An air gap is a network security measure employed on one or more computers to ensure that a computer network is physically isolated from other networks, such as the public Internet or other local area networks.
Computer Network Attacks (CNA)	CNA "…includes actions designed to destroy or otherwise incapacitate enemy networks."[1] Such activities include acts of sabotage.
Computer Network Exploitation (CNE)	CNE describes activities that take advance of computer and network vulnerability without creating damage. Such activities are commonly referred to as espionage or surveillance.
Cyber Conflict	This paper defines cyber conflict as "…the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities."[2]
Cyber Security	Security in cyberspace (i.e., cybersecurity) "…is about technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate

[1] Schneier, "Computer Network Exploitation vs. Computer Network Attack."
[2] Valeriano and Maness, *Cyber War versus Cyber Realities*, 5.

	actions against information technology by a hostile or malevolent actor."[3]
Cyber War	This paper follows Thomas Rid's framework of cyber war.[4] Acts such as sabotage, espionage, and subversion are offensive and violent political acts, but do not constitute acts of cyber war. Instead, a long-lasting, sustainable and damaging offensive military operation that only takes place in cyberspace should be understood as cyber war.
Cyberspace	This paper defines cyberspace as: "…the artifacts based on or dependent on computing and communications technology; the information that these artifacts use, store, handle, or process; and how these various elements are connected."[5]
Distributed Denial of Service Attack (DDoS)	A DDoS attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.
Escalation	"Escalation, in broad military terms, is an increase in the intensity or scope of conflict. It is a fundamental dynamic in which adversaries engaged in a contest for limited objectives increase the force or breadth of their attacks to gain advantage or avoid defeat."[6]

[3] Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, als eBook:2.
[4] Rid, *Cyber War Will Not Take Place*.
[5] Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, als eBook:2.
[6] Morgan, Project Air Force (U.S.), and United States, *Dangerous Thresholds*, 1.

GhostNet	An allegedly Chinese cyber spying operation that infiltrated high-value political, economic and media locations in 103 countries.
Information Security	"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."[7]
Malware	"A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim."[8]
Phishing Attack	Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in an email or other communication channels.
Stuxnet	"Stuxnet is computer malware first discovered in July 2010 that mainly targeted Windows PCs and other industrial software and equipment. The worm exploited a zero-day vulnerability in Windows. It is believed that Stuxnet spread through infected USB flash drives."[9]
TURLA	An allegedly Russian malware program that targeted governments and militaries infrastructure to extract information.
Virus	"A computer program that can copy itself and infect a computer

[7] Kissel, "Glossary of Key Information Security Terms," 94.
[8] Ibid., 118.
[9] Techopedia, "What Is Stuxnet?"

	without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk."[10] Viruses rely on a host, typically a piece of software, to be operational.
Worm	"A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself."[11]
Zero-Day Exploit	A zero-day vulnerability refers to a weakness in software that is unknown to the creator. It can be exploited by hackers without the knowledge of the software owner or user; such an activity is called a zero day attack.

[10] Kissel, "Glossary of Key Information Security Terms," 212.
[11] Ibid., 215.

Introduction

Cyberspace has become a crucial environment for economic development, communication, innovation, political participation, and beyond. However, the news coverage about cyberspace, especially in the United States (U.S.),[12] places emphasis largely on the dangers, fears, and threats that originate from this domain. Cyber war, cyber-espionage, 'cyber Pearl Harbor', cyber-attack, cyber weapons, and many other terms are used to describe the latest hacks, viruses, and malware. Yet it remains unclear what military activities in cyberspace actually look like and whether Internet users and nations should be concerned about military escalation in this domain.[13]

This paper contributes to the ongoing discussion about the likelihood of military escalation, the potential escalation threshold, and possible solutions that may help prevent military escalation in cyberspace. Therefore, the leading research question is: *which conditions help reduce the likelihood of military escalation in cyberspace*? Additionally, significant attention will be placed on clarifying whether it is realistic to expect that increased military and intelligence activities within cyberspace provide reason to worry about military escalation in cyberspace.

Chapter One clarifies conditions under which increased military and intelligence activities[14] within cyberspace occur and how these conditions contribute to instability within cyberspace. Key sources of instability include: fear-based decision-making, lack of understanding of cyberspace, dramatization of the threat originating out of cyberspace through media and

[12] Special attention is given to the United States because it is considered to be one of the main trend-setters for military activities in cyberspace.

[13] This paper follows Forrest Morgan et al. definition on escalation and applies this to cyberspace. They define escalation as "…an increase in the intensity or scope of conflict. It is a fundamental dynamic in which adversaries engaged in a contest for limited objectives increase the force or breadth of their attacks to gain advantage or avoid defeat." See: Morgan, Project Air Force (U.S.), and United States, *Dangerous Thresholds*, 1.

[14] Military and intelligence operations in cyberspace are oftentimes difficult to distinguish or keep separated. As Chapter One describes in more detail, victims of offensive cyber operations might not know immediately whether they are being attacked or just surveilled. For this reason, this paper includes intelligence and surveillance operations into its analytic framework of military operations in cyberspace and therefore does not consider nation states internal distinction between intelligence and military cyberspace operations.

politicians, lack of governmental transparency on the scope of military operation in cyberspace, imprecise understanding of the asymmetric distribution of power in cyberspace, uncertainty about the scope and effectiveness of deterrence strategies in cyberspace, uncertainty about the applicability of public international law and legal terms in cyberspace, imperfect attribution in cyberspace, and ambiguity between computer network exploitation and computer network attacks.

Chapter Two presents a risk analysis framework for military operations in cyberspace, which is then applied to several case studies in Chapter Three. The methodology is qualitative in nature and, given the scope of this paper, is not based on extensive statistical evidence. The case studies offer an analytical review of the field based on their respective features. Additionally, secondary literature and technical reports from third parties are used to assure that the nuances of each case are sufficiently scrutinized through risk analysis.

The case studies confirm that conflict in cyberspace does in fact exist.[15] However, the outcome of these case studies indicate that none had a very high chance of military escalation in cyberspace. Instead, states seem to consistently operate below a certain threshold of military escalation, though the exact threshold still remains unclear. However, cyber restraint seems to be the guiding *modus operandi* for states' activities in cyberspace.

The case studies also highlight the importance of a holistic analysis of military and intelligence cyber operations. None of these activities occur in a vacuum; they are affected by larger geopolitical trends, regional developments, internal political developments, and individual threat perceptions. For this reason, it is important to integrate discussions about military activity in cyberspace into the larger field of international relations research and policy analysis. In fact,

[15] This paper applies Valeriano and Maness definition of conflict in cyberspace. They define it as "the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities" See: Valeriano and Maness, *Cyber War versus Cyber Realities*, 5.

the case studies indicate that the most severe causes of military escalation in cyberspace originate outside of cyberspace, namely in geopolitical disputes and large-scale military confrontation.

Chapter Four explores a variety of conditions that help reduce the likelihood of military escalation in cyberspace. The key conditions identified in this paper are divided up in several levels. On the state level, key conditions include: governmental transparency about military operations in cyberspace and regular confidence-building measures between states focused on their military operations in cyberspace. On the global level, key conditions include: the existence of effective conflict prevention mechanisms and a precise understanding of how public international law applies to military operations in cyberspace and to what extent law limits military operations in cyberspace. On the cross-cutting level, key conditions include: an increase in globalization and economic interdependence among nations and a higher threshold for success for attackers in cyberspace. The threshold for success could be raised by more sophisticated and widespread 'cyber hygiene' practices, an overall change in the imbalance between offensive and defensive operations in cyberspace, the absence of 'low-hanging fruit' or a reduction in software vulnerabilities, and an international environment that encourages states to focus on improving national resilience instead of concentrating exclusively on deterrence strategies. If none or only very few conditions are met, then the current increase in military and intelligence activities within cyberspace provide reason to worry about military escalation in cyberspace.

Chapter Five identifies key responsibilities in implementing the proposals made in Chapter Four. While most proposals need to be implemented by governments and international organizations, Internet businesses and non-state actors also play key roles in facilitating the implementation process. The key suggestions of this paper include: providing international organizations with stronger mandates to facilitate the implementation process of the

aforementioned global solutions; encouraging states to develop more sophisticated frameworks for collaboration with private businesses, increase their national capacity building among diplomats and policy-makers, and put stronger emphasis on shifting the current imbalance between offensive and defensive military operations in cyberspace; applying pressure through academics and NGOs to improve governmental transparency measures and promote improved 'cyber hygiene'; and encouraging representatives of the media and academia to roll back the 'military' discourse about cyberspace. Overall, all entities should help maintain a global, stable, and secure cyberspace, which is a key condition for preventing military escalation in cyberspace.

The paper concludes by suggesting that there is reason to worry about military escalation in cyberspace, though its likelihood can be reduced significantly if the appropriate measures, outlined in Chapters Four and Five are taken. While this paper concludes that all case studies analyzed in this paper fall under the threshold of military escalation, identifying a more precise escalation threshold for military operations in cyberspace requires further research.

Since this paper is limited to state-based or state-encouraged cyber operations, military cyber operations against terrorist organizations such as Daesh or al-Qaida exceed the scope of this paper. Similarly, use of offensive cyber operations by terrorists is not covered, and thus many of the proposals presented in this paper are not applicable in helping prevent non-state actors from destabilizing cyberspace. Non-state actors with little or no ties to a state deserve further analytical attention, since the threshold for acquiring sophisticated offensive capabilities in cyberspace is slowly declining. Compared to nation states, these actors tend to be less constrained by inter-state dependencies, more difficult to deter, and more likely to exploit existing sources of instability within cyberspace, which might lead to unintended military escalation in cyberspace among states.

Chapter 1 – Sources of Instability in Cyberspace

This Chapter explores the sources of instability for inter-state relations within cyberspace. This paper defines instability among states as a situation that is dominated by lack of trust, disagreement over (geo-)political issues, competing interests and the competition for power between states. A multitude of factors contribute to the real and perceived instability in cyberspace. Tackling these factors requires a comprehensive understanding of their root causes. Some factors are unique in cyberspace, while others are not. Whereas some scholars argue that existing frameworks for analyzing the use of force and armed attacks can be applied to cyberspace[16], this paper argues that military action in cyberspace has several unique features that are important to understand when aiming to establish more trust and confidence among states, leading toward a more stable cyberspace environment.

1.1 The Cognitive Level

On the cognitive level, misunderstanding between actors and confusion about the issues at hand, for example through bad analogical reasoning, can contribute to instability. U.S. Senator Ted Stevens comparison of the Internet with a *series of tubes* in 2006 was one of the few bad analogies that was rebuked by the public.[17] Most analogies are rarely questioned and lead to false impressions about the features of cyberspace. These factors often lead to fear, which affect decision-making. Currently, cyberspace is the main arena of inter-state relations in which "fear-based process of threat construction [is] becoming dominant."[18] While fear is not a unique cause

[16] Shackelford, Scott Russell, and Kuehn, "Unpacking the International Law on Cybersecurity Due Diligence"; Stahl, "Uncharted Waters of Cyberspace."
[17] Belson, "Senator's Slip of the Tongue Keeps on Truckin' Over the Web."
[18] Valeriano and Maness, *Cyber War versus Cyber Realities*, 2.

of instability for cyberspace, two important additional factors highlight the relevance of this level. Additionally, the regular dramatization of cyber incidents through media outlets further contributes to this sense of alarm. This is especially true in the United States, where continuous public warnings by representatives of the military, intelligence and politics about a *Cyber Pearl Harbor* or a *Cyber 9/11* get picked up by mainstream media and further exaggerated.[19] The latest data suggests that these tendencies reflect a hype that cannot be supported by real evidence.[20]

Moreover, cyberspace tends to be branded as a completely new domain with unique technological characteristics. While this may be true to a certain extent, the simplification and generalization, both among the general public and political decision-makers, contributes to raising concerns about perceived risks originating from cyberspace. The same holds true for information technology experts who lack a legal or policy background. Additionally, the diversity in framing the threats in cyberspace also exist across ideological regions. Subchapter Three elaborates on the ongoing dispute over the scope and definitions of *cyber security* and *information security,* which is just one of many ideological debates in this field.[21]

To summarize, reducing the likelihood of military escalation in cyberspace requires addressing cognitive sources of instability through the following conditions: decreasing fear, increasing trust, improving the understanding of cyberspace, addressing the significant dramatization of cyber security issues by the media and politicians, and addressing cyber war with facts instead of sensationalized coverage.

[19] Ibid., 7.
[20] Valeriano and Maness, *Cyber War versus Cyber Realities*- Chapter 5.
[21] von Solms and van Niekerk, "From Information Security to Cyber Security."

1.2 The State-Actor Level

On the state-actor level, vagueness within the decision-making process on cyber related issues occurs regularly. Existing procedures, legislation or separation of tasks further complicates how governmental bodies deal with challenging cyber incidents. While many nations have established new government entities to develop cyber security policy, the adjustment of governmental processes is still ongoing. Even one of the most advanced nations with regard to cyber security, namely the United States, is still debating which government institution would be in charge when the nation is attacked through cyberspace.[22]

The low-cost to entry toward cyberspace led scholars such as Joseph Nye to believe that diffusion of power will occur in cyberspace.[23] This would lead unconventional players, namely non-state actors, to enter the stage and further complicate inter-state discussions and negotiations to introduce mechanisms that could reduce conflict in cyberspace. While cyberspace is indeed a low-cost entry domain and initiating unsophisticated offensive operations is easy, the presumption that conflict in cyberspace is inherently asymmetric has not proven to be correct so far. Terrorists organizations that are known for using asymmetric tactics, have not yet acquired the capability to develop or take advantage of advanced persistent threats (APTs) in cyberspace.[24] Weaker actors will face steeper challenges to build up capabilities in cyberspace.[25]

Given the asymmetric distribution of military power and capability in cyberspace, traditional concepts of deterrence are difficult to apply or at least require significant adjustment.

[22] Sternstein, "The Pentagon Still Hasn't Decided Who's In Charge If America Comes Under Cyberattack."
[23] Nye, *The Future of Power*- Chapter 5 - Diffusion of Cyberpower.
[24] Operations that require significant human intelligence, resources and information to deploy them are generally referred to as APTs.
[25] Rid, *Cyber War Will Not Take Place*.

A recent effort to adjust deterrence in cyberspace was done by Christopher Haley, who split up deterrence in cyberspace in three distinct categories: defense, attribution and retaliation:[26]

1. "Defense – A powerful cyber defense is the first step in protecting against the vast majority of aggressors and dissuading some from attacking at all.
2. Attribution – The ability to attribute an attack to a specific source is important for maintaining credibility and ensuring legitimacy at home and abroad.
3. Retaliation – The willingness and capability to retaliate against any (but not necessarily every) attack from any source under any circumstances must be assured."[27]

However, politicians and experts in the United States still fear that they lack an effective deterrence strategy for cyberspace. This is an alarming development since the United States is considered to be a trend-setter for military activities in cyberspace. Valeriano and Maness warn that "[i]f states fall into the trap of buying into the fear-based cyber hype by developing offensive weapons under the mistaken belief that these actions will deter future incidents, cyberspace is doomed."[28] While this might sound plausible at first, there are many reasons to argue that deterrence does work in cyberspace, especially on a state-actor level.[29] However, the discussion over the applicability of deterrence strategies in cyberspace is far from over in the United States. While this process continues, this paper argues that the uncertainty of an effective deterrent contributes to the overall sense of instability.

[26] Haley, "A Theory of Cyber Deterrence."
[27] Ibid.
[28] Valeriano and Maness, *Cyber War versus Cyber Realities*, 4.
[29] Healey, "Cyber Deterrence Is Working."

Cyberspace should not be analyzed in a vacuum. Real world events are by no means a less important source of instability for cyberspace. Be it geopolitical disputes, ongoing international negotiations, conflict resolution efforts, emerging partnerships or changing alliances, all of these factors contribute to state-actor behavior in cyberspace. The challenging factor is that it remains largely unclear which role cyberspace plays within such events. Is it a separate military domain or an overarching layer for various types of military operations? Given the difficulty in fast and reliable attribution, state-actors almost always face a certain amount of uncertainty when cyber incidents occur, which generally leads to a sense of instability.

Moreover, the number of potential actors is significantly higher compared to other domains since the technical threshold for entering cyberspace for offensive purposes is relatively low.[30] The confusion surrounding the origin of the Sony hack[31] reflects this trend. Even weeks after the incidents, security experts were not absolutely sure who was behind the attack.[32] The reason for this was the simplicity and lack of sophistication of the hack. In fact, the attack could have been created easily by many non-state actors as well. Ultimately, a deep review of the *intent* of the attackers, combined with additional intelligence and geo-political and foreign policy knowledge was necessary to be able to determine with reasonable confidence that North Korea was behind the attack.[33]

If a few individuals with experience in hacking are able to conduct the same operations that a highly sophisticated military of an industrialized country can,[34] then this leads to an erosion

[30] Nye Jr, "Nuclear Lessons for Cyber Security."
[31] In November 2014, a hacker group leaked a significant amount of confidential data, including personal informational about employees, internal e-mails, salaries of executive, copies of then-unreleased films, and other information about Sony Pictures Entertainment. More information about the incident can be found in Chapter Three.
[32] Schneier, "We Still Don't Know Who Hacked Sony."
[33] Sanger and Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say."
[34] Schneier, "Attack Attribution and Cyber Conflict - Schneier on Security.pdf."

of (hard) power that we have not seen in recent decades. However, experts believe that ordinary hackers are not able to create computer worms like Stuxnet.[35] Such sophisticated attacks are generally labelled as APTs, given the significant amount of human intelligence, resources and information that is required to deploy them.[36] These attacks involve not only the creation of a malicious virus that hacks into a network, but also an extensive knowledge of unknown software bugs, network vulnerabilities, human intelligence, and on-the-ground operations.[37] While these facts might be acknowledged by decision-makers, the overall perception of the security environment in cyberspace should not be underestimated. The likelihood of developing a cyber arms race increases significantly if governments are driven by fear and operate under the assumption outpacing their adversaries in cyberspace is the only way to ensure their own safety in the digital world.[38]

To summarize, reducing the likelihood of military escalation in cyberspace requires addressing state sources of instability through the following conditions: ameliorating vagueness within the policy process, helping governments respond properly against threats in cyberspace originating from non-state actors, defining the extent of the level of asymmetric power within cyberspace, adjusting the concept of state power in cyberspace, clarifying the applicability and usefulness of deterrence strategy in cyberspace, fostering a holistic view among policy-makers when responding to threats originating out of cyberspace, and helping lower the level of uncertainty within the governmental decision-making process.

[35] Geers et al., "World War C."
[36] Falliere, Murchu, and Chien, "W32.Stuxnet Dossier."
[37] Ibid.
[38] Valeriano and Maness, *Cyber War versus Cyber Realities*, 15.

1.3 The Global Environment Level

Given the borderless design of cyberspace,[39] conflict in cyberspace is inherently global. International and regional organizations are actively involved in addressing the sources of instability, which are largely driven by ideology and diverging concepts of international law and states obligations. Especially offensive military operations in cyberspace pose a new challenge for the applicability and enforcement of public international law. Since 2013 the United Nations (UN) has acknowledged that conflict in cyberspace is a serious concern for the international community.[40] States[41] agree that cooperation is essential to reduce the risk of military escalation and enhance security within cyberspace.[42] Given this commitment, it is fair to say that state representatives suppose that further escalation in cyberspace can be prevented through the implementation of international regimes[43], treaties[44], or agreements[45]. However, when it comes to military activities, few states are currently willing or able to engage in comprehensive negotiations on treaties governing military use of cyberspace.[46] Below the threshold of international treaties,

[39] Architecturally, cyberspace was not designed based on national boundaries. As data travels through networks divided up in many small packets of information, the backbone infrastructure of cyberspace only cares about delivering the data to the recipient as fast as possible. This may mean that the different packets may travel through different routes, crossing different countries, maybe even different continents. Physical distance does not play a role in determining which route data will take to get to its recipient.
[40] United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015.
[41] It is important to note that the discussions about conflict in cyberspace include many non-state actors such as Internet Service Providers (ISPs) and other relevant private businesses. The same holds true for several civil society representatives. Given the scope of this paper, the analysis will focus on inter-state developments. A future version of will seek to include non-state voices and opinions given their increasingly important role in cyberspace.
[42] United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015; United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013.
[43] Nye, "The Regime Complex for Managing Global Cyber Activities."
[44] Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, "Proposal for an International Code of Conduct for Information Security."
[45] Hirschfeld Davis and Sanger E., "Obama and Xi Jinping of China Agree to Steps on Cybertheft"; Roth, "Russia and China Sign Cooperation Pacts."
[46] Sputnik International, "UN Cybersecurity Report Compromises on Self-Defense Issue - Russian Official."

there are norms, which have the potential to be codified or implemented through use. The same applies to confidence-building measures (CBMs) as means to further promote this dialogue. Many international institutions are facilitating such talks at this stage.[47] However, most of these talks are focused on law enforcement cooperation against organized cyber-crime rather than military activities in cyberspace.[48]

During the latest round of consultations of the United Nations Group of Governmental Experts on Cybersecurity (UN GGE), the group hardly addressed military activities as relevant to their discussion of norms and principles in cyber space. Instead, in their July 2015 report to the UN General Assembly, the relevant section focused on critical infrastructure and information and communications technology (ICTs).[49]

While the UN GGE reports from 2013 and 2015 demonstrate that there is a general agreement that existing international laws—such as the law of armed conflict—do indeed apply to cyberspace, the actual scope of their application remains contested.[50] Some analysts argue that the latest UN GGE report made some important steps in clarifying the applicability of the law of armed conflict in cyberspace.[51] Even so, the discussion of a definition of 'armed attack' and the 'use of force' in cyberspace is hardly over.[52] Chapter Four will provide further details on the importance

[47] United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015; Organization for Security and Co-operation in Europe Permanent Council, "Decision No. 1106 Initial Set Of OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies," 1; ASEAN, "ARF Work Plan on Security of and in the Use of Information and Communications Technologies."
[48] Rõigas and Minárik, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law."
[49] United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015; Rõigas and Minárik, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law."
[50] Sputnik International, "UN Cybersecurity Report Compromises on Self-Defense Issue - Russian Official"; Chernenko, "Global Cybersecurity: 6 Questions on the Key Issues as Seen from Moscow."
[51] Marks, "U.N. Body Agrees to U.S. Norms in Cyberspace."
[52] Giles and Hagestad, "Divided by a Common Language."

of a dialogue on legal norms, which aims at harmonizing different interpretations among countries. There are several key developments that try to clarify the scope and extent to which existing international law applies to cyberspace.[53] However, the current discourse on norms, at least at the UN level, seems to be stagnant.[54]

To summarize, reducing the likelihood of military escalation in cyberspace requires addressing global sources of instability through the following conditions: clarifying the scope of applicability of public international law and legal terms in cyberspace, expanding CBM efforts focused on military operations in cyberspace, and fostering stronger inter-state cooperation on non-military issues within cyberspace.

1.4 The Cyber Infrastructure Level

Attribution in cyberspace remains a core challenge. Given the wide variety of options for acting anonymously in cyberspace, guaranteed attribution down to the human level of every single attack remains technically difficult.[55] The most sophisticated intelligence agencies might be able to identify the computer that was used to create a certain code or to carry out an attack, but this does not mean that they know who was actually using the computer or whether the computer was a means to carry out the attack, while the attack was actually planned somewhere else. In many situations hijacked computers around the world are used to further complicate tracing an attack back to its originator. While some experts argue that attribution in cyberspace is no longer a

[53] Selin, "Governing Cyberspace"; Maurer, "Cyber Norm Emergence at the United Nations"; Nye, "The Regime Complex for Managing Global Cyber Activities"; Meyer, "Seizing the Diplomatic Initiative to Control Cyber Conflict"; Watts, "Cyber Norm Development and the United States Law of War Manual."
[54] Meyer, "Another Year, Another GGE? The Slow Process of Norm Building for Cyberspace."
[55] Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem"; Schneier, "Attack Attribution and Cyber Conflict - Schneier on Security.pdf."

challenge, it remains unclear what kind of attribution they are referring to.[56] Most security experts remain rather reluctant to say that attribution, especially for international legal purposes, has been solved. Given the ongoing evolution of technological capabilities, experts in most cases are able to track a connection to a machine. However, as noted above, connecting this computer to the user is extremely difficult. This problem is often referred to as the 'endpoint security issue'[57], effectively tying the device to the person is currently almost impossible. Putting aside the legal and technical challenges for attribution, all case studies in Chapter Three indicate, geopolitical considerations proved to be essential in the recent years to place cyber incidents into context. Chapter Four puts these different considerations toward attribution into context and provides some future recommendations how to minimize the challenges of attribution.

Given the borderless design of cyberspace, the geographical location of an attacker and its target no longer play a major role in determining the origin of an operation. In other military domains, physical distance is used to be an impediment for confrontation. Moreover, one could build walls, fences or use natural borders such as mountains or water to create distance. In cyberspace, such borders do not exist by design, and it is difficult to artificially create them at this point in time. In fact, the entire concept of distance becomes obsolete in cyberspace. Once an attacker has access to the victim's network or computer, data extraction, surveillance or even destruction may occur almost instantaneously. However, this does not mean that anybody connected to cyberspace is immediately and constantly under attack. As the case of Stuxnet, which is described in detail in Chapter Three of this paper, shows, sophisticated offensive cyber operations are costly and require long-term planning. Once developed, its execution is in fact

[56] Libicki, "Would Deterrence in Cyberspace Work Even with Attribution."
[57] Tatam, "Cracking the Problem of Endpoint Security."

instantaneous in most cases but they are by no means operational whenever an actor wants to conduct a certain operation. It is yet to be seen how this trend will shape future geopolitical strategic thinking.

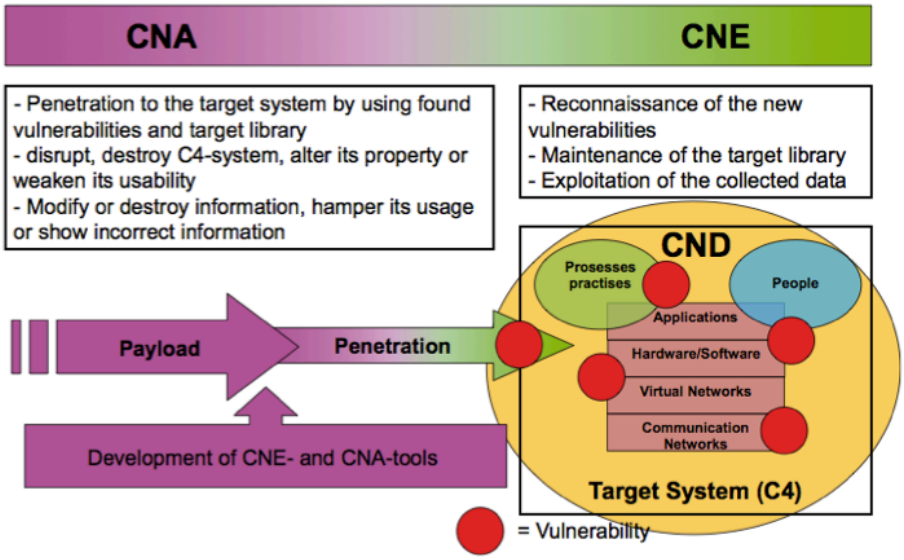
Besides the difficulty of attribution in cyberspace, it is often very challenging to put cyber network operations (CNO) into context without a clear understanding of the intent of the perpetrator. For example, computer network exploitation (CNE) and a computer network attack (CNA) can look fairly similar for network and defense operators.[58] As Figure One below shows, CNE operations are necessary for the conduct of CNA operations. Actors who identify CNE operations within their networks, therefore, have reason to worry about a CNA and require a good understanding of the perpetrators' intent before taking a decision. In the case of the United States, legal definitions also have an effect on the cyber-attack threshold analysis. While CNE and CNA are technically the same[59], they are treated differently from a legal perspective.[60] A perceived CNA might cause a significantly different response from a perceived CNE, though the technical symptoms of both activities might look identical. Moreover, incorrect identification of the origin of an attack, commonly referred to as false flag events, are more likely to occur in cyberspace than in traditional military domains. From a technological perspective there is no such thing as 'passive hacking' since a hack is an inherently active action.[61] To make such a determination, knowing the intent of the actor is required. Without a clear understanding of the intent behind the activity, states might overreact because they think they are being attacked, even though they are not. Without

[58] Schneier, "Computer Network Exploitation vs. Computer Network Attack."
[59] Ibid.
[60] Joint Chiefs of Staff, "Cyberspace Operations"; Joint Chiefs of Staff, "Information Operations."
[61] Schneier, "Computer Network Exploitation vs. Computer Network Attack."

clear communication lines and a sufficient level of trust between the nations, this technical characteristic of cyberspace constitutes a concerning source of instability for interstate relations.[62]

For these reasons, almost every activity related to cybersecurity could be identified as a potential 'dual use' good, depending on the intention of the actor. Moreover, national cyber defense experts might not be able to distinguish immediately whether a network intrusion is done to spy on, steal, or destroy data and/or infrastructure. Any legal norm that aims at reducing conflict in cyberspace will have to acknowledge this reality. The latest legal effort to introduce international regulations on this issue failed due to the ambiguity in the proposed legal language.[63]

Figure One: Differences between CAN and CNE[64]



Source: Jari Rantapelkonen et al., "The Fog of Cyber Defence," Julkaisusarja 2, p.150.

[62] Brake, "Strategic Risks of Ambiguity in Cyberspace."
[63] Cardozo and Galperin, "What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?"; Peterson, "The Government Is Headed back to the Drawing Board over Controversial Cybersecurity Export Rules."
[64] Rantapelkonen, Salminen, and others, "The Fog of Cyber Defence," 150.

When one observes Internet traffic, it is difficult to know immediately what a certain package of data may contain. The design of the package itself is neutral. Recent technological advancements such as deep package inspection make it easier to detect known malign internet traffic, but they cannot stop new kinds of attacks. Ultimately, intent is what distinguishes Google's testing of its own networks for vulnerabilities from outside hackers who are stealing data from that same network. While Google's employees most likely have good intentions when improving their network defense capabilities, the hacker's intentions could be characterized as malign. Thus, the intent of an action is crucial to determining whether the action is offensive or defensive.

To summarize, reducing the likelihood of military escalation in cyberspace requires addressing infrastructural sources of instability through the following conditions: tackling the existence of imperfect attribution, creating mechanisms to distinguish between CNE and CNA operations, and adjusting domestic and international policy-making on the borderless design of cyberspace.

Overall, given the variety of sources of instability, one has reason to worry about military escalation in cyberspace. The following Chapter puts these theoretical sources of instability into context by analyzing several case studies of military and intelligence operations in cyberspace.

Chapter 2 – A Risk Analysis Framework for Military Operations in Cyberspace

This chapter focuses on establishing a risk analysis framework for offensive military activities in cyberspace, which is then applied to several case studies in Chapter Three. Frederic Lemieux, an expert in security studies, identified four different kinds of cyber operations, varying in intensity.[65] While intensity is an important benchmark, it should only be considered in combination with additional benchmarks: the amount of actors that possess the capability and intent to carry out an operation (threat); the level of vulnerability that a certain target possesses (vulnerability); and the consequences, such as the magnitude or intensity of a cyber operation (consequences). This results in the following, commonly used equation for risk:[66]

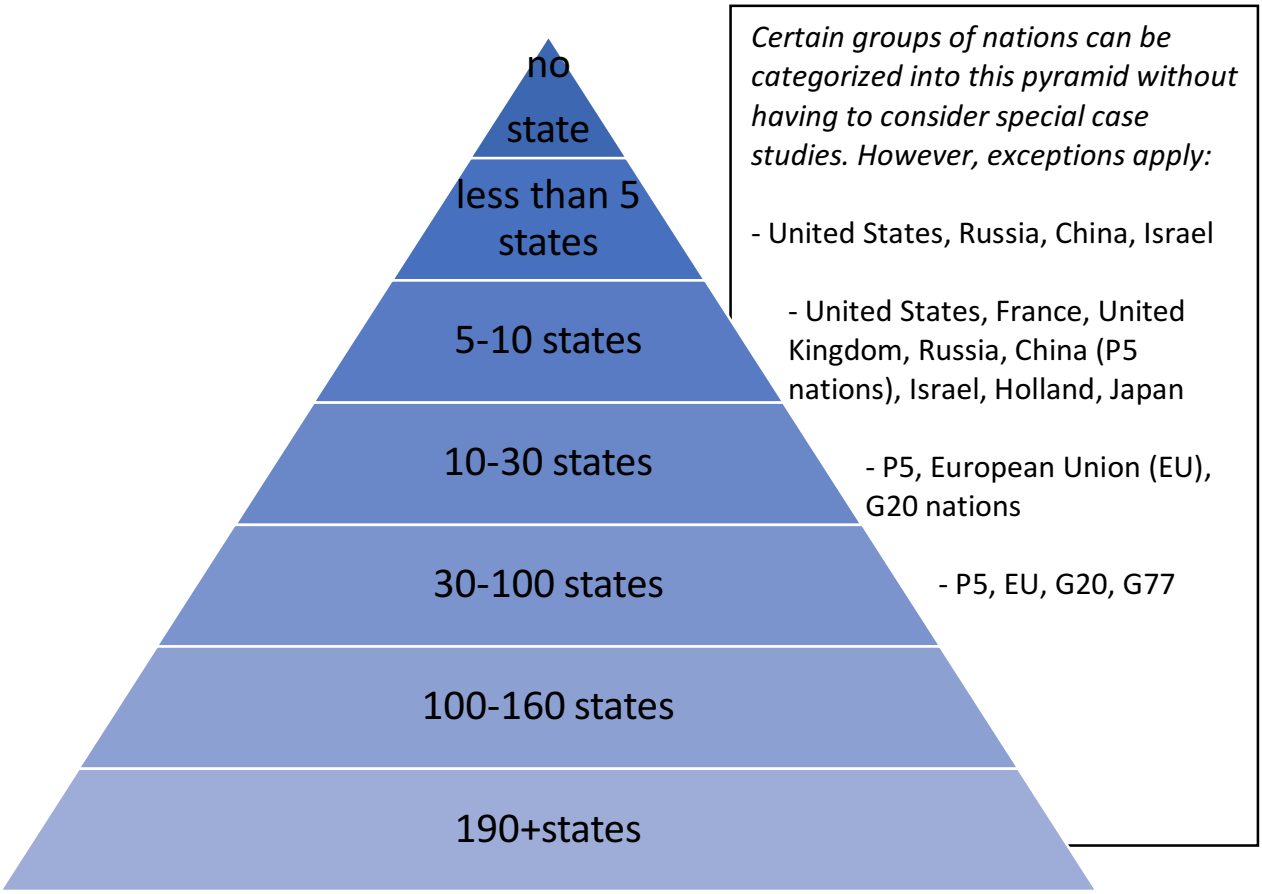
Risk = Threat (Capability x Intent) x Vulnerability (different level of damage probability) x Consequences (expected magnitude/ intensity of the incident)

The threat level is defined by the amount of actors that possess the capability to carry out military operations in cyberspace and their intent to use the capability. Whether intent exists or not must be discussed on an individual case analyses.[67] Capabilities of certain operations can be assessed numerically and then categorized into groups. For example, while very few nations are capable of creating APTs such as Stuxnet, most nations engage in some form of cyber-enabled espionage. Moreover, distributive denial of service attacks (DDoS) can be purchased on the black market by

[65] Lemieux, *Current and Emerging Trends in Cyber Operations*, 5–7.
[66] This paper does not argue that this equation should be used as mathematical formula but rather as a general guiding framework when assessing risk.
[67] Several case studies will be presented and analyzed in Chapter three.

any actor who wishes to use them. Recent research suggests that approximately 29 countries have "formal military or intelligence units dedicated to offensive operations" and 49 have acquired off-the-shelf malware. Both numbers are expected to increase over the next years.[68] Figure Two outlines the seven numerical categories for states with capabilities to conduct a certain military operation in cyberspace.

Figure Two: Broad categorization of nations ranked by sophistication military cyber operations

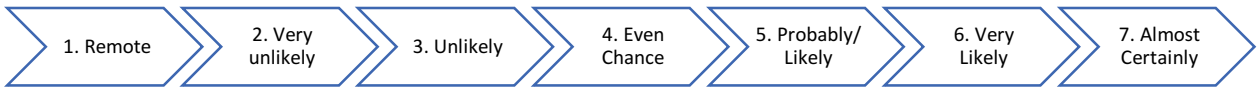


The level of vulnerability and the respective probability of damage depends on the respective target. While the U.S. military network has sophisticated protections in place and therefore is more

[68] Segal, *The Hacked World Order*, 11.

difficult to attack or penetrate, the Estonian governmental networks were much more vulnerable when they suffered large DDoS attacks in 2007. The probability of creating damage was therefore higher in the Estonia's case, while the magnitude, discussed below, is lower than a successful attack would be on the U.S. military network. Figure Three illustrates the following categories commonly used among the risk analysis and intelligence reports[69] to determine the likelihood of success.

Figure Three: likelihood of success of a certain military operation in cyberspace[70]



Source: National Intelligence Council, "Iran: Nuclear Intentions and Capabilities," National Intelligence Estimate (Office of the Director of National Intelligence, November 2007), p. 5.

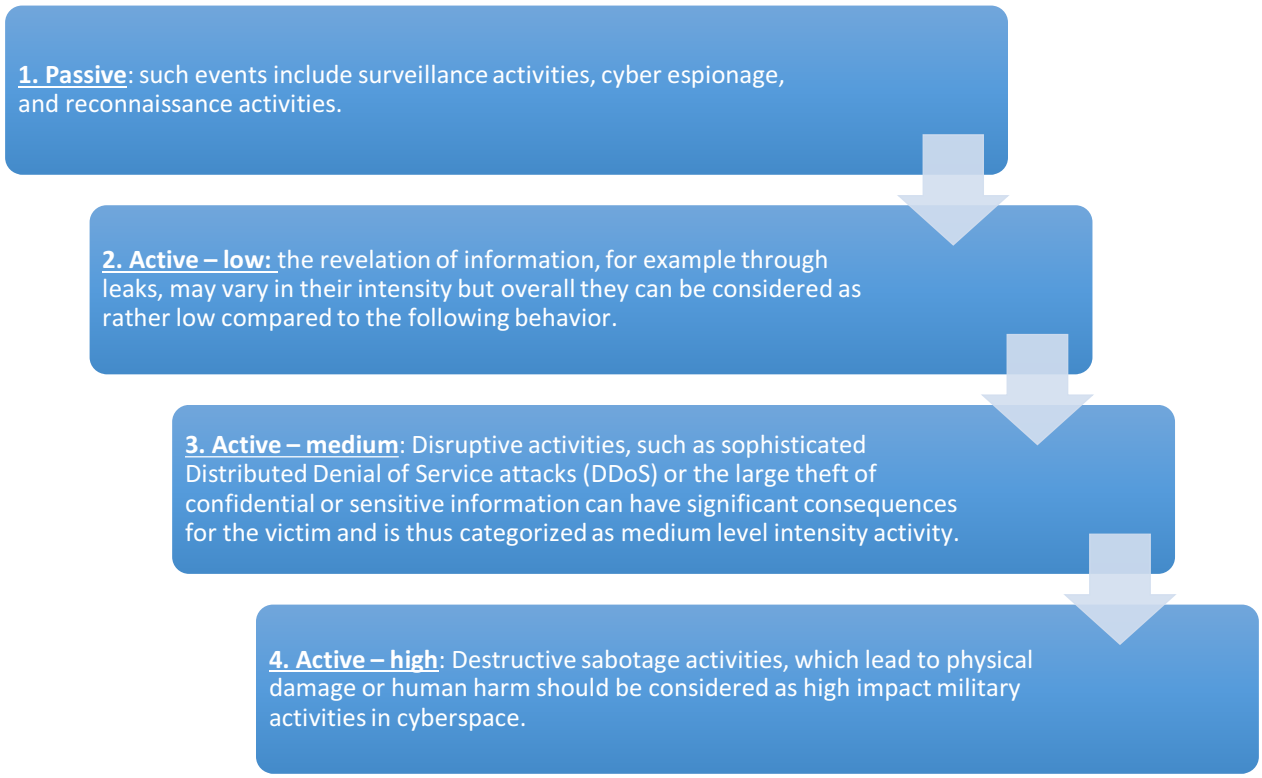
A remote chance of success often correlates with a high impact and vice versa. Any nation could create a DDoS attack on any other nation with almost complete certainty, though the impact would remain rather low given that most networks have improved their resilience against such attacks in recent years. More complicated military operations that involve several steps that build up on each other, such as Stuxnet, have a lower likelihood of success given the large amount of variables that may affect the operability of the operation.

Lastly, the intensity and specific consequences for the reliance on the attacked system depends on the attacker, the victim, the broader environment in which the operation takes place and other

[69] National Intelligence Council, "Iran: Nuclear Intentions and Capabilities," 5.
[70] Ibid.

additional factors. However, certain types of operations can be categorized in the following four broad categories: *passive*, active-*low*, active-*medium*, and active-*high*.[71] Figure Four outlines the different levels of magnitude and intensity, with passive operations having the lowest and active (high) operations having the highest level of magnitude and intensity in most cases.

Figure Four: Consequences measured by the level of magnitude and intensity[72]



Source: Lemieux, Current and Emerging Trends in Cyber Operations, p. 5–7.

[71] The term 'passive' within this ranking can be slightly misleading and deserves further clarification. As described in the previous Chapter, 'passive hacking' does not exist from a technological perspective. The term passive here refers to the impact and consequences of the respective operation rather than the technical characteristics of the operation itself. For example, a surveillance operation with no additional features has no immediate impact on the victim and is therefore categorized as passive, rather than active.
[72] Lemieux, *Current and Emerging Trends in Cyber Operations*, 5–7.

Chapter 3 – Scenarios of Potential Military Escalation in Cyberspace

Based on the risk analysis framework in Chapter Two, this Chapter analyzes past offensive military activities and scenarios for potential future activities. All case studies are ranked by the level of risk of military escalation. The primary goal of this Chapter is to demonstrate the gap between the publicly perceived hype surrounding cyber-attacks and cyber war compared to reality. As the following case studies demonstrate, traditional state rivalries have extended to cyberspace, but they do not constitute a completely independent domain of operation. In fact, conflict in cyberspace has barely changed how states interact with each other and there is reason to believe that the fears associated with military operations in cyberspace are exaggerated.[73]

3.1 High Risk of Military Escalation

Hypothetically, the highest danger of escalation are severe cyber disputes that aim at "changing the foreign policy behavior of a state, infiltrate critical infrastructure or compromise networks of states' military apparatuses."[74] According to Valeriano and Maness, "… none of these rare incidents has actually led to significant escalation."[75] APTs, such as Stuxnet, are oftentimes designed to achieve these exact goals. They, therefore, tend to have the highest risk of military escalation in cyberspace. To date, no publicly known cyber operation constitutes an event of *high* threat, *significant* vulnerability, and *large* consequences. All real world examples contain at least one weakness within their risk analysis. The publicly perceived threshold of an escalatory cyber

[73] Valeriano and Maness, *Cyber War versus Cyber Realities*, 209.
[74] Ibid., 214.
[75] Ibid.

incident is therefore higher than the actual threshold. The key facts of each case study's risk assessment are summarized in the boxes displayed before each section.

Hypothetical high risk scenario:
capable nations: less than five |likelihood of success: very likely |consequences: high

If two nations with sophisticated military cyber capabilities are at a kinetic war with each other, the risk for military escalation within cyberspace through destructive cyber-attacks would be *fairly high*. Given the direct military confrontation, it is reasonable to expect that an offensive cyber-attack would not constitute the only military operation that would lead to further escalation of the conflict. Moreover, reasons to restrain their offensive cyber operations would be reduced given that both nations are already at war with each other. Given that this incident would occur during a war situation, this risk assessment should not come as a surprise.

Currently, no nations with sophisticated military cyber capabilities are at war with each other. The ongoing conflicts in Ukraine and Syria, and the land disputes in the South China Sea can be identified as potential sources for the manifestation of this hypothetical scenario. However, the current global political environment makes such a scenario still *unlikely*. Erik Gartzke argues that even though some nations possess sophisticated offensive cyber capabilities, malicious cyber incidents on infrastructure, which would be a core component of a larger military operation, have been and will continue to be rare to nonexistent because states are restrained due to the high probability of civilian harm, the nature of the weapons (single use), and the weak payoff.[76] This finding goes hand in hand with Thomas Rid's frustration about how loosely the term '*cyber war'*

[76] Gartzke, "The Myth of Cyberwar," 16.

is used by commentators.[77] If every single DDoS attack constituted an act of cyber war, multiple nations would go to war every single day, including significant amounts of non-state actors.

Russo-Georgian war (2008) | victim: Georgia | alleged perpetrator: Russia
capable nations: 10 – 30 states |likelihood of success: probably |consequences: medium

In 2008, during the brief Russo-Georgian war over South Ossetia and Abkhazia, Georgia experienced cyber-attacks similar to, but more targeted than, those suffered by Estonia the previous year. This is the first known use of an offensive cyber operation during a conventional armed conflict. Russia's decision to use offensive cyber capabilities to paralyze Georgia's governmental servers, military command and control structure, and its air defense systems seemed to be a real time assessment of their CNO deployment capabilities.[78] Disabling an adversary's information systems is a fairly common component in military strategy and thus this operation does not constitute a new method for military operations, though it shows that cyber operations can have the same effect as kinetic means, if successful. Additionally, this incident appears to be the first case of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains, in this case land and air. This again demonstrates that for cyber aggression to have lasting effects, a virtual attack must be combined with physical intervention.

Since Georgia did not possess similar military capabilities in cyberspace, this conflict did not lead to military escalation in cyberspace, but rather to an escalation through kinetic means. Moreover, Georgia's national information and communication infrastructure is relatively small

[77] Rid, *Cyber War Will Not Take Place*.
[78] Berlich, *Schlachtfeld Internet? Eine Analyse Moderner Kriegsführung Am Beispiel Des Russisch-Georgischen Krieges 2008*, 60,62.

compared to Russia's. For these reasons, Russia's cyber operation can be categorized as an event of *medium-high* risk of military escalation given its significant likelihood for military escalation.[79]

This cyber operation was the first of its kind, though it is likely that future military confrontations among nations will include attacks on command and control systems through cyber operations. While Georgia might have been an easy target for offensive cyber operations in general, given its small military and its unpreparedness for such an attack, other nations military command and control structures could be connected to non-military networks. An attack on dual-use cyberspace infrastructure could quickly escalate and drag other nations into a military conflict.

3.2 Medium Risk of Military Escalation

Medium risk events have two or more *weak* components, be it either that *very few* nations possess the capabilities, or because the likelihood of success is *lower* or the consequences are *not high*. All of the following case studies have at least one *weak* or *low* component within the risk analysis.

Stuxnet (2009-2010) | victim: Iran | alleged perpetrator: United States and Israel capable nations: less than 5 |likelihood of success: unlikely |consequences: medium

Operation Olympic Games[80], and especially its core component Stuxnet[81] was categorized by many experts such as Bruce Schneier[82], Jason Healey[83] and others as the most severe CNA

[79] For a more detailed overview of the incident see: Healey and Grindal, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 194–204.
[80] Stuxnet was not the only covert cyber sabotage campaigns aimed at Iranian nuclear facilities. As it was later discovered, a worm labelled as Duqu and a malware called Flame were also part of a larger cyber operation against Iran's nuclear facilities. The umbrella term for this operation is Olympic games, which is the alleged code name within the United States government for this operation.
[81] Stuxnet is computer malware that mainly targeted Windows PCs and other industrial software and equipment. The worm exploited a zero-day vulnerability in Windows. It is believed that Stuxnet spread through infected USB flash drives. For an extensive coverage about Stuxnet see: Zetter, *Countdown to Zero Day*.
[82] Messmer, "Stuxnet Cyberattack by US a 'Destabilizing and Dangerous' Course of Action, Security Expert Bruce Schneier Says."
[83] Healey, "Stuxnet and the Dawn of Algorithmic Warfare."

operation in cyberspace thus far, given the physical destruction of nuclear centrifuges in Iran as a result. Kim Zetter, cybersecurity journalist for WIRED magazine, even labelled it to be the first cyber weapon.[84] While most experts agree that Stuxnet can be categorized as use of force, fewer would go as far as defining it as an armed attack.[85] The main reason why this paper categorizes Stuxnet as a *medium risk* example is the magnitude of the incident and masking effect the worm had on the infrastructure of the centrifuges it was physically impacting. However, it is important to note that no human harm was caused by the operation and the physical damage, while impressive for a non-kinetic operation, did not stop nor significantly derail the Iranian nuclear enrichment process.[86]

Even if the level of vulnerability of the deployed hardware and software could be categorized as *high*, Iran took many precautionary steps to assure that their centrifuges were not vulnerable to an attack before Stuxnet was deployed. The facilities were constructed underground, the computer networks were air-gapped[87], and access to the area was very limited and tightly controlled. For this reason, the perceived level of damage probability from the Iranian perspective was *unlikely*, while it was *likely* from the perpetrator's perspective after having developed and tested Stuxnet.

Looking beyond the initial target of Stuxnet, computer experts such as Ralph Langer were able to reverse engineer Stuxnet and provide technical details to the public.[88] Initial concerns about

[84] Zetter, *Countdown to Zero Day*.
[85] The distinction between the use of force and an armed attack remains contested among international lawyers. For more information see: Hollis, "Is a Use of Force the Same as an Armed Attack in Cyberspace?"
[86] Zetter, *Countdown to Zero Day*- Chapter 4: Stuxnet Deconstructed.
[87] A network is air-gapped when it is physically disconnected from the Internet. All data traffic therefore remains within the system and there is no means of connecting to outside networks. This procedure is used to protect important networks from intrusions. A physical device, such as a USB drive, a hard-drive or a DVD are the only means of transferring data into or out of air-gapped networks.
[88] Langner, "To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve."

the revelation of Stuxnet's technical details as means of providing the public at large a weapon to deploy its capabilities against other critical infrastructure objects around the world proved to be wrong. So far, no known re-deployment of Stuxnet against other facilities has occurred. Although the coding mechanism has been made public, an adjusted Stuxnet version is fairly unlikely because of the design of the malware itself. Every single step of the malware was carefully designed to prevent it from damaging anything but the narrowly defined target. Although the malware was found on more than 300,000 computers around the world, it would activate itself only if it was able to locate a specific configuration of Siemens logic controllers. In theory, it was supposed to delete itself if the infected computer did not meet the specific criteria.[89] However, the exploitation of software vulnerabilities will remain a key component of future cyber enabled sabotage operations. Lastly, the threat of such an attack is *fairly remote*. Only *few* actors have the capability and even *fewer* have the intent for such an operation. While the consequences were *significant*, the vulnerability and threat level remain *fairly low* overall given the highly sophisticated design of Stuxnet, its long development phase, the use of several unknown software vulnerabilities, the *low probability* for reoccurrence and the small amount of actors with the capability and intent for such an operation.[90] Moreover, no military escalation occurred in the aftermath of Stuxnet. While news reports stated that the Shamoon malware that affected 30,000 Saudi Aramco computers and deleted significant amounts of data was a direct retaliatory response by Iran, this incident could be categorized as a proportionate response and not an escalation of the situation.[91]

[89] Falliere, Murchu, and Chien, "W32.Stuxnet Dossier."
[90] Ibid.
[91] Perlroth, "Cyberattack on Saudi Oil Firm Disquiets U.S."

3.3 Low Risk of Military Escalation

Most offensive military operations in cyberspace can be categorized as *low* risk events. While many of these operations can be conducted by a significant number of states, most of the incidents lack significant consequences or remain *low* in overall magnitude. Many of these operations are aimed at information collection or political coercion from a powerful state toward a significantly weaker state (such as Russia and Estonia).

DDoS attacks on Estonia (2007) | victim: Estonia | alleged perpetrator: Russian hackers capable nations: 30-100 |likelihood of success: probably |consequences: medium

The three-week long DDoS attacks against Estonian government, communication and banking networks in 2007 can be categorized as a *low risk* event for military escalation in cyberspace because the Estonian government responded to this situation with a call for technical, not military help.[92] While the attacks were politically motivated and aimed at changing the Estonian government's position on a Soviet World War II monument, the attacks also reflect the limits of offensive cyber operations for coercive purposes. Despite the initial intensity of the DDoS attacks, the Estonian government found a technological solution to neutralize the attacks and did not change its opinion toward the controversial monument. Many state actors could have ordered a DDoS attack of this magnitude and the chances of success were *fairly high* given Estonia's limited cyber resilience at that time. However, the consequences were more annoying than actual damage or fear among the population. The political motivation and the intent behind the operation to have an impact on Estonian domestic politics is clear,[93] however, evidence of Russian government's involvement in these attacks remains inconclusive, though the operation has been widely attributed

[92] Healey and Grindal, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 191.
[93] Ibid., 273.

to "Russian patriotic hackers".[94] After the Estonian government dealt with the attack, its response was calculated and non-militaristic. It called upon the Russian government to halt the attack and asked representatives of Western governments to compel Russia to stop the attack.[95] For this reason, and because no physical damage was caused through the attack, the overall consequences of the incident are *low*. However, the incident resulted in political decisions such as NATO's move to enhance its cyber war capabilities and to establish the alliance's cyber defense research center in Tallinn in 2008. They also motivated Estonia to call on the EU to make cyber-attacks a criminal offense.

OPM hack (2015) | victim: United States | alleged perpetrator: China
capable nations: 5-10|likelihood of success: very likely |consequences: passive

In the summer of 2015, a massive data breach at the U.S. Office of Personnel Management (OPM) was revealed that had initially started in March 2014. It is estimated that up 21.5 million records of U.S. government employees, including personally identifiable information, were stolen during this breach.[96] Technical details about the hack remain largely undisclosed and an investigation about the incident is still ongoing. The stolen data has not appeared on the black market for sale yet, which suggests that a state actor was behind the hack. It is fair to say that few nations would risk penetrating U.S. government networks, let alone stealing massive amounts of data. Brian Krebs and other cyber security analysts believe that Chinese hackers carried out this operation.[97] It was later disclosed that the stolen information was not encrypted[98] and the network was ill-

[94] Nye, *The Future of Power*, 127.
[95] Healey and Grindal, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, 188.
[96] Krebs, "Catching Up on the OPM Breach — Krebs on Security."
[97] Ibid.
[98] Gallagher, "Encryption 'would Not Have Helped' at OPM, Says DHS Official."

prepared[99] to deal with sophisticated intrusions. For this reason, the likelihood of success was *very likely*. While the media described the incident as a massive cyber-attack, the risk of military escalation through this hack remained *fairly low* because the United States does not consider espionage as a reason to go to war. In the private sector in the United States, many consider cyber-enabled espionage as part of the cost of doing business in the 21st century. Similar interpretations apply to the U.S. government, given the increasing likelihood of massive data breaches in the digital age.[100]

Sony hack (2014) | victim: Sony Entertainment | alleged perpetrator: North Korea capable nations: 30-100|likelihood of success: very likely |consequences: low

In November 2014, a hacker group which identified itself as the *Guardians of Peace* leaked a significant amount of confidential data, including personal informational about employees, internal e-mails, salaries of executive, copies of then-unreleased films, and other information about Sony Pictures Entertainment.[101] The hack originated with a phishing attack, a fairly common but rather unsophisticated way to gain access into an internal network. *Many* actors have the capability to conduct such an operation, though *very few* have the motivation to do so. One key component of the hack was a demand not to release *The Interview,* a comedy about a plot to assassinate North Korean leader Kim Jong-un, to the public. Early reports remained inconclusive about the origin of the operation[102], though it was later disclosed that the U.S. government was convinced that the

[99] Gallagher, "Why the 'biggest Government Hack Ever' Got Past the Feds."
[100] Swire, "The Declining Half-Life of Secrets."
[101] For an extensive and detailed overview of the incident see: RiskBasedSecurity, "A Breakdown and Analysis of the December, 2014 Sony Hack."
[102] Schneier, "We Still Don't Know Who Hacked Sony."

North Korean government was behind the hack.[103] Given the unpreparedness of Sony Entertainment for such an attack, the likelihood of success was *very high*. While the reputational and financial consequences for Sony were devastating, the likelihood of military escalation between states remained *fairly low*. President Obama announced North Korea will have to face a proportionate response such as tightened economic sanctions.[104] Shortly after the U.S. government announced that North Korea was behind the attack, North Korea lost its connection to the Internet for a few hours.[105] It remains unclear whether this was an act of retaliation by the United States or simply a coincidence. Regardless, it proves that the likelihood of military escalation between the United States and North Korea as a response to the Sony hack was *very low*.

EPIC TURLA (?-2014) | victims: Western governments | alleged perpetrator: Russia capable nations: 5-10|likelihood of success: likely |consequences: low

In 2014 Reuters reported that a spyware called EPIC TURLA had quietly infected hundreds of government, military and diplomatic computers across Europe, the United States and the Middle East[106]. EPIC TURLA is considered to be one of the most complex cyber espionage programs uncovered to date given its sophisticated design and the use of two zero day exploits.[107] It was also linked to a previously known, massive global cyber spying operation dubbed Red October, targeting diplomatic, military, and nuclear research networks.[108] *Very few nations* are able to

[103] Sanger and Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say."
[104] Ibid.
[105] Perlroth and Sanger, "North Korea Loses Its Link to the Internet."
[106] Apps and Finkle, "Suspected Russian Spyware Turla Targets Europe, United States."
[107] Kaspersky, "The Epic Turla (snake/Uroburos) Attacks | Virus Definition"; Kaspersky Lab Global Research and Analysis Team, "The Epic Turla Operation: Solving Some of the Mysteries of Snake/Uroboros."
[108] Kaspersky, "Kaspersky Lab Identifies Operation 'Red October,' an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide"; Apps and Finkle, "Suspected Russian Spyware Turla Targets Europe, United States."

develop such a sophisticated espionage and surveillance software and even fewer would target the European Union (EU) and the United States at the same time. Security experts believe that Russia was behind EPIC TURLA, though the evidence remains inconclusive.[109] Given its sophistication and use of unknown vulnerabilities, the likelihood of success was *fairly high*. It remains unclear how significant the impact of this operation was, though one can presume that this operation is a continuation of traditional state espionage and surveillance through new means. The consequences for military escalation can therefore be categorized as *low*.

GhostNet (?-2009) | victims: Asian governments | alleged perpetrator: China capable nations: 5-10|likelihood of success: likely |consequences: low

In March 2009, a large-scale cyber-espionage operation called GhostNet was discovered. Computer systems in foreign ministries, embassies and other government offices in Asia were the main target.[110] The Dalai Lama's Tibetan exile centers in India, London, and New York were also compromised by GhostNet. Given the target selection, experts presume that China's military Unit 61398 designed GhostNet, though technical evidence remains inconclusive.[111] The main task of GhostNet was to collect information and intercept communication. Given the sophistication of operation, the success of the operation can be considered as *likely*. Similar to operation EPIC TURLA, it remains unclear how large the impact of this operation was. However, the consequences for military escalation can be categorized as *low* given its narrow focus on surveillance and espionage.

[109] GReAT, "The Epic Turla Operation Solving Some of the Mysteries of Snake/Uroburos."
[110] Markoff, "Vast Spy System Loots Computers in 103 Countries."
[111] Tiezzi, "Report: 'Highly Sophisticated Cyber Espionage' Group Linked to Chinese Intelligence."

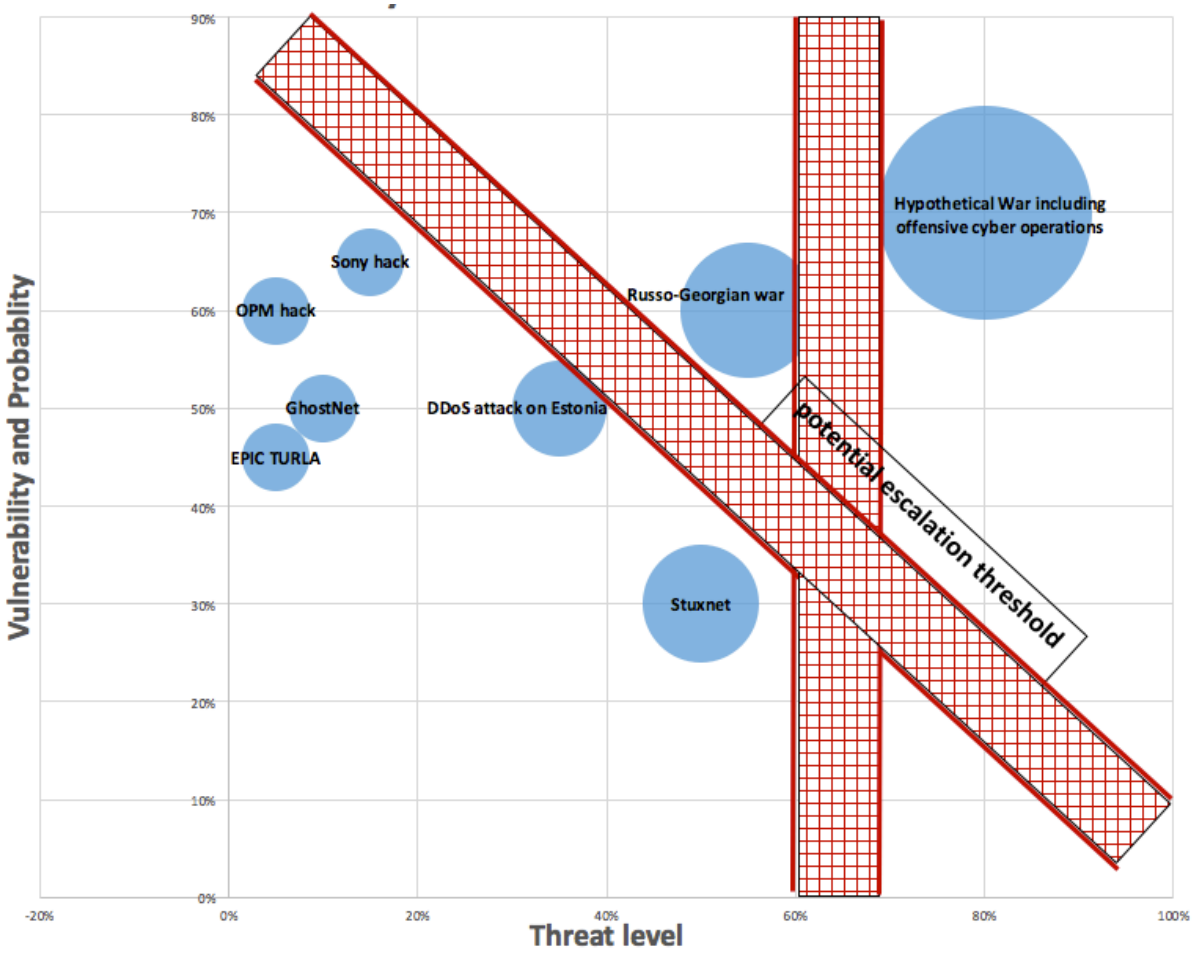
3.4 Overall Risk Evaluation

The findings of the case studies confirm that "[c]yberspace is […] a perfect forum for low-level, widespread, and sometimes psychological threats to an enemy population"[112], state espionage, and surveillance operations. In fact, the 2015 Worldwide Threat Assessment of the U.S. Intelligence Community came to a similar conclusion. It stated that "…the likelihood of a catastrophic [cyber] attack from any particular actor is remote at this time. […] We foresee an ongoing series of low-to-moderate level cyber-attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security."[113]

Cyberspace offers significant potential for advanced surveillance and espionage activities – a core component of national security and security policy of most nations. Few cases exist that go above the threshold of surveillance – Stuxnet being one of them. Overall, states seem to operate under a notion of cyber restraint and thus actively avoid military escalation in cyberspace.[114] However, the exact threshold for military escalation in cyberspace remains unclear and is difficult to assess in a broader setting. While all cases are context dependent and are difficult to compare, Figure Five below combines all discussed case studies and visualizes the different levels of thread (x axis) vulnerability (y axis) and magnitude (size of the respective bubble). Based on the case study assessment, the red areas reflect a potential threshold for military escalation in cyberspace. All cases in the upper right corner have a high risk of military escalation.

[112] Valeriano and Maness, *Cyber War versus Cyber Realities*, 9.
[113] Clapper, "Worldwide Threat Assessment of the US Intelligence Community," 1.
[114] Valeriano and Maness, *Cyber War versus Cyber Realities*, 4.

Figure Five: Overview of the potential level of risk of military escalation in cyberspace based on the case studies' level of threat, vulnerability, and magnitude.



Source: Author's own research

Another finding of the case studies is the geopolitical component of the events. This finding confirms Valeriano's and Maness' discoveries on regionalism in cyberspace.[115] They concluded that "despite the vastness and transboundary capacity of the Internet, most operations

[115] Ibid., 17.

are limited to local targets and connected to traditional causes of conflict, such as territorial disputes and leadership disagreements. Issues are important in world politics and in cyber politics."[116] Geopolitical analysis therefore deserves a great deal of attention when clarifying the intention or origin of past and future cyber operations.

To summarize, the case studies with *high* and *medium* risk of military escalation indicate that the main conditions causing military escalation in cyberspace originate outside of cyberspace, namely in geopolitical disputes and large-scale military confrontation between adversaries. This finding has consequences for the potential options that aim at preventing military escalation in cyberspace, which are discussed in the following Chapter.

[116] Ibid.

Chapter 4 – Proposals for Preventing Military Escalation in Cyberspace

Despite the low likelihood of an event with high risk of military escalation, we have reason to worry about military escalation in cyberspace because the stakes are extremely high. Cyberspace, and the Internet in particular, have had a tremendous impact on modern life in the past two decades with the social, economic, political, and cultural benefits of cyberspace continuously to expanding. If cyberspace became a risky and insecure domain for commerce or other activities, many of these benefits would be diminished, if not completely lost. Fortunately, many opportunities exist on the cognitive, state, global and infrastructural level to reduce the likelihood of military escalation in cyberspace. Interestingly, sources of instability described in Chapter One are not necessarily solved within the same level they originate from. For example, many issues that arise within the state level, such as uncertainty within the decision-making process, miscommunication, confusion and non-cyber related conflicts, can be better addressed on the global level. The following subsections are intended to facilitate a roadmap toward reducing the likelihood of military escalation in cyberspace on different levels, though many of the proposed solutions could be placed within a different level through certain adjustments. This flexibility important when considering the best approach toward the implementation of the following proposed solutions.[117]

4.1 Solutions on the Cognitive Level

Drawing upon historical examples helps human beings to deal with new situations, items or phenomena. Unfortunately, analogies are accepted too quickly and differences are ignored too quickly. Cyberspace has suffered significantly from bad analogical reasoning in the past years. *Cyber Pearl Harbor*, cyber warfare, cyber power, cyber deterrence, and *cyber Wild West* are just

[117] The implementation of the respective proposed solutions is discussed separately in Chapter Five of this paper.

a few of many cyber analogies with regard to security aspects and military operations.[118] Many of them are flawed – few of them are rebuked.

Bad analogies are one of many reasons why more emphasis should be put on the de-mystification of cyberspace. Younger generations have the benefit of growing up with the Internet and receiving computer (science) courses in high school or college. However, current policy-makers rarely have a sophisticated understanding of cyberspace. Not everybody needs to know the technical details on the infrastructure of cyberspace, though a general understanding of key features, including similarities and differences to other domains, is crucial to prevent wrong analogies and false assumptions. Of special importance for this paper are efforts by scholars such as Erik Gartzke, who help reduce the misconceptions about military operations in cyberspace.[119]

To summarize, the key conditions on the cognitive level that would help reduce the likelihood of military escalation in cyberspace are increased efforts toward improving the understanding of cyberspace among policy-makers and similar efforts to help computer scientists better understand the implications of their work for political decision-making, both domestic and international.

4.2 Solutions on the State Level

This subchapter focuses on transparency measures, cross-domain deterrence, and CBMs in cyberspace. Almost all nations keep the details of their military capabilities in cyberspace secret. This behavior is not unique to cyberspace, similar trends of secrecy can be observed with past military developments in other domains such as nuclear weapons programs. Many scholars have

[118] For an extensive evaluation of cyber analogies see: Goldman and Arquilla, "Cyber Analogies."
[119] Gartzke, "The Myth of Cyberwar."

written about how secrecy around military cyber operations can lead to an arms race.[120] Many sophisticated cyber capabilities are based on zero day exploits, which can get patched once revealed. This volatility in development and effectiveness of offensive cyber capabilities makes it extremely difficult to create a more transparent environment. Besides the technological developments, tactics, and strategy matter as much. Unfortunately, only a handful of states, such as the United States, declassify military documents outlining their military cyber strategy.[121]

A recommendation for more transparency, though important, is trivial. While technical details might be more difficult to share, a stronger exchange about military cyber doctrines is quite possible. This recommendation also includes greater transparency efforts from victims of cyber incidents. The Peoples Liberation Army's indictment in May 2014 was the first of its kind for several reasons, though the one relevant here is that it included a detailed list of companies that had suffered from cyber intrusions.[122] This included details about the theft of intellectual property and other proprietary material. While the indictment was not meant as a transparency measure per se, it helped many private actors understand the scope and magnitude of cyber espionage and theft.

Applying the concept of deterrence in cyberspace remains contested. Depending on the definition and scope of deterrence, scholars such as Joseph Nye or Jason Healey argue that deterrence does indeed work in cyberspace, though only above a certain threshold.[123] Deterring cyber actions conducted by non-affiliated non-state actors will be difficult. However, this does not mean that the concept of deterrence has no relevance in cyberspace altogether. Especially among state actors, the concept of deterrence deserves more attention. Jason Healey argues that the world has not experienced a 'cyber war' until this date because deterrence in cyberspace does in fact

[120] Nye Jr, "Nuclear Lessons for Cyber Security"; Goldsmith, "Can We Stop the Global Cyber Arms Race?"
[121] The Department of Defense, "The DoD Cyber Strategy."
[122] United States District Court - Western District of Pennsylvania, "Peoples Liberation Army Indictment."
[123] Nye Jr, "Nuclear Lessons for Cyber Security"; Healey, "Cyber Deterrence Is Working."

work.[124] Especially, if cross-domain deterrence is taken into consideration, this paper argues that there should be even more efforts to adjust the concept of deterrence to cyberspace because it reduces the likelihood of the hypothetical high-risk scenario described in Chapter Three.

Improving deterrence in cyberspace could also be achieved by maintaining and expanding the intertwinement of military and civil cyberspace infrastructure. This suggestion might sound counterintuitive first because it increases the vulnerability and potential collateral damage in case of an attack. However, it also means that discriminating between civil and military targets becomes much more difficult for an attacker. Any cyber operation that causes significant collateral damage will be proscribed publicly and violates the concept of discrimination in international humanitarian law. This has a deterring effect on all states that generally comply with international humanitarian law. For nations and non-state actors who do not feel compelled to abide by these international legal norms, this solution was little to no effect. However, paired with strong cyber resilience, the intertwinement could still be used advantageously. In the case of the United States, over 90 percent of military and intelligence communication is delivered through privately owned backbone telecommunication networks.[125] Anyone who would want to interfere with U.S. command and control structures would therefore probably be forced to accept significant collateral damage.

Given the highly political circumstances under which military operations in cyberspace are discussed between states, Confidence Building Measures (CBMs) are considered to be a good method to identify areas of cooperation and reduce mistrust among nation states. In fact, CBMs between states are generally considered to be "one of the key mechanisms in the international

[124] Healey, "Cyber Deterrence Is Working."
[125] Segal, *The Hacked World Order*, 17.

community' toolbox aimed at preventing or reducing the risk of a conflict by eliminating the causes of mistrust and miscalculation between states."[126]

While international legal norms reflect *values*, which are ideas that exist among actors and therefore aim at a certain end state or a goal, CBMs are considered to be *means* because they provide the process of getting to the end state that norms envision.[127] Establishing CBMs in cyberspace share some of the challenges that face the effort to develop norms, including state sovereignty, the non-physical nature of cyberspace, and the significant number of non-state actors.[128] The lack of reasonable attribution in cyberspace makes it difficult to implement CBMs that are based on verification, a common feature among traditional CBMs. These challenges need to be acknowledged by all involved actors before innovative CBMs for cyberspace can be developed.

Once acknowledged, CBMs have several features that cannot be accessed through pure discussions around norms. CBMs help prevent miscalculation, misunderstanding, and escalation between states. They do not require reaching consensus on everything. It is possible to work around the edges of contested issues and gradually move to a more comprehensive agreement.[129] Generally, there are four types of CBMs that are relevant in cyberspace:

First, CBMs on collaboration are designed to share information, provide transparency, and build trust. They provide a platform for dealing with the unique challenges of cyberspace outlined in Chapter One. They foster trust by creating channels for communication. Collaborative CBMs also contribute to transparency, accountability, and stability. One of the first international

[126] Pawlak, "Cyber Diplomacy," 3.
[127] For more general information and latest proposals on CBMs in cyberspace, see: Healey et al., "Confidence-Building Measures in Cyberspace - A Multistakeholder Approach for Stability and Security."
[128] See Chapter One for more information on characteristics on cyberspace.
[129] Healey et al., "Confidence-Building Measures in Cyberspace - A Multistakeholder Approach for Stability and Security."

organizations that implemented a first round of collaborative CBMs is the Organization for Security Cooperation in Europe (OSCE), which are aimed at information sharing and regular meetings. Proposals for additional CBMs on collaboration include the establishment of a framework for joint investigations, the application of environmental law in cyberspace, and increased compliance policing through best current practices.[130]

Second, CBMs on crisis management are intended to manage tense moments to avoid outbreak of major wars between nation-states. In cyberspace, such efforts would require the inclusion of non-state actors as observers or policing forces. Current practical proposals on crisis management CBMs include the functional alignment of crisis emergency response teams (CERTs) to increase transparency.[131] Actors that share the CERTs with other governments before a crisis hits know immediately whom to reach out to in a tense situation. Another way to facilitate easy and fast communication during an emergency situation was put forward by the United States and Russia, who were among the first to implement a cyber 'hotline'. To further promote stability, one could expand this concept into a multilateral setting and also include private sector actors, such as Internet Service Providers (ISPs) to keep them informed about emergency situations. Lastly, scholars recommend fostering accountability in cyberspace through the establishment of a cyber adjudication and attribution council. Such an international body should be able to investigate and assign responsibility for cyber crises that could spiral into conflict. It could also serve as local arbitration court to avoid conflict. However, even the authors of this idea acknowledge how difficult the implementation of such a council would be.[132]

[130] Ibid.
[131] Ibid.
[132] Ibid.

Third, CBMs aimed at increasing engagement with non-state actors are also crucial in cyberspace. Stronger engagement across both sides would create leverage for international technical regimes and help develop norms. This could be done by facilitating existing regimes, such as the Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), or the World Wide Web Consortium (W3C) to work with governments to set norms. Moreover, neutral activists' entanglement and support could be fostered. This would encourage and support security researchers to collaborate across borders and thus increase the discussion and engagement of technical, scientific, and legal experts across the world.

Fourth, CBMs aimed at restraining activities could help on three levels: They could increase stability of the internet backbones and infrastructure by creating target restrictions and neutrality; improve accountability by asking states to declare responsibility for behavior within their territory; and enhance transparency by joint research on the applicability of international human rights law in cyberspace.

CBMs are not designed to substitute discussions around international legal norms. In fact, the feasibility of CBMs depends on the *parallel* development of international legal norms. Instead of looking at CBMs as a replacement of legal norms, both should rather be considered as reinforcing methods that help reduce conflict in cyberspace. Eventually, both paths may lead to the codification of best practices, behavior, and norms within cyberspace.

Ultimately, the main challenge that all of these proposals face is identifying clear and precise language that reflects the complexity of the technical circumstances, while still being understandable by policy-makers. The OSCE successfully bridged this gap in its first set of CBMs,

but it remains the only international body which has made this effort.[133] Closing this bridge between technology experts, policy-makers, and lawyers should be at the core of any future CMB process. In countries with less clear civilian leadership over military operations, the additional challenge would be reaching an agreement by state actors vis-à-vis their military.

To summarize, the key conditions on the state level that would help reduce the likelihood of military escalation in cyberspace are increased transparency measures about military operations in cyberspace, a precise understanding of the applicability of cross-domain deterrence strategies in cyberspace, and the further development of CBM efforts focused on military operations in cyberspace.

4.3 Solutions on the Global Level

While cyberspace might indeed be a separate domain for military operations, conflict in cyberspace does not occur in a vacuum. Addressing the root causes of international disputes is at the core of preventing military escalation in cyberspace. This requires a broader approach toward cybersecurity than most scholars currently take. Narrowing down on the complexities of cybersecurity issues is tempting and helpful to create more clarity on certain details, but it also leads to a loss of a more holistic view on military conflict in general. Ultimately, the "normal political domain" is the source of conflicts.[134] Such an approach will also help overcome technical and legal challenges of attribution. As the case studies of this paper show, geopolitical analysis is crucial in clarifying who has the capability to conduct certain cyber operations and also

[133] Organization for Security and Co-operation in Europe Permanent Council, "Decision No. 1106 Initial Set Of OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies."
[134] Valeriano and Maness, *Cyber War versus Cyber Realities*, 15.

understanding the motivation and intend behind their actions. Non-technical attribution is crucial with regard to sophisticated cyber operations and to a lesser extend also toward low-scale operations.[135]

Clarifying the scope of applicability of existing international law is another important component of integrating cyber conflict into existing operational frameworks. However, this effort has to go beyond legal debates and be addressed in political, cultural, and economic fora. China, the United States and the European Union (EU) have begun to create these non-legal environments to discuss conflict in cyberspace. More nations should initiate these efforts and help integrate conflict in cyberspace into a larger discussion about mediation and conflict resolution among states and non-state entities.

This process should be accompanied by the establishment of a database with relevant legal and technical terms. A prominent example of this idea is the New America Foundation Global Cyber Definitions Database[136], which was supported by the OSCE. Such efforts will increase understanding of different points of views across sectorial and jurisdictional borders. Databases should also help reduce complexity from both the legal and technical sides.

The ongoing debate on the applicability of the laws of war in cyberspace gained momentum in the last years through the introduction of the Tallinn Manual on the International Law Applicable to Cyber Warfare, which was funded by NATO, created by an international group of approximately twenty experts, and officially facilitated by NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) However, the CCDCOE's Tallinn Manual largely reflects ideas and perceptions of academics from NATO membership countries.[137] Moreover, the Tallinn

[135] Sheldon, "Geopolitics and Cyber Power."
[136] New America Foundation, "Global Cyber Definitions Database."
[137] Deeks, "Tallinn 2.0 and a Chinese View on the Tallinn Process."

Manual's definition and scope is also contested and not accepted by many non-NATO member countries such as Russia or China[138]. For this reason, moving this discussion forward and making it more inclusive continues to be essential for the reduction of military escalation in cyberspace. Having a clear and precise understanding on thresholds and the scope of military action helps prevent misunderstandings, unnecessary provocations and also reduces the likelihood of a cyber arms race.

Scholars and experts continue to discuss what kinds of actions are necessary to constitute a conflict in cyberspace. In fact, there is no universally accepted definition of cyber warfare. Authors such as John Arquilla, Thomas Rid, Peter Singer, and many others have contributed to the search for a definition, but so far none has been widely endorsed among states.[139] The lowest common denominator seems to be that definition simply depends on the circumstances, the involved actors, the target, the intent, and the scale of the event. So far, we have not yet seen broad offensive cyber activities like the hypothetical case study presented in Chapter Three, but we have experienced several events in which offensive cyber operations supplemented kinetic attacks, such as in the Russo-Georgian war in 2008.[140]

Agreeing on a definition for cyber warfare is important because it helps reduce ambiguity and complexities; this evolution can facilitate the reduction of conflict in cyberspace. This paper follows Thomas Rid's narrow interpretation[141] of cyber war. He argues that cyber war, which is exclusively fought in cyberspace, has to include an active force to compel the enemy to your will

[138] An updated version of the Tallinn Manual, labelled Tallinn 2.0, is expected to be released in late 2016.
[139] Arquilla, "Cyberwar Is Already Upon Us"; Rid, *Cyber War Will Not Take Place*; Singer, *Cybersecurity and Cyberwar*.
[140] Tikk et al., *Cyber Attacks Against Georgia: Legal Lessons Identified*; Kenneth Geers, *Cyber War in Perspective*.
[141] Rid argues that: "… all acts of war are violent or potentially violent […], an act of war is always instrumental: physical violence or the threat of force is a means to compel the enemy to accept the attacker's will [….] to qualify as an act of war, an attack must have some kind of political goal or intention."

plus a political goal or intention.[142] Based on his definition, states are not yet operating in an environment of cyber war.

Although, even before theorizing on the existence of cyber war, one needs to define what an 'armed attack' and 'the use of force' in cyberspace actually mean. Several states, international organizations, researchers, and other actors have come up with potential definitions.[143] While few states acknowledge this argument, most of them actually follow a crude logic: "an armed attack in cyberspace is when we say it was an armed attack."[144] Thus, depending on the actors' perspective, they will either observe or not observe 'cyber war'. Similar discussions take place around the definition of 'the use of force' in cyberspace.[145]

Generally, the UN Charter, the Law of Armed Conflict, and subsequent legal interpretations of these documents are considered as foundational legal documents for legal analysis of an 'armed attack' and 'the use of force' in cyberspace. Additionally, customary international law is considered a secondary source for the legal interpretation of state practice. Article 2(4) in the UN Charter prohibits the use of force except in situations of self-defense (Article 49) or through UN Security Council approval under a Chapter VII resolution. Lastly, Article 51 refers to the "…inherent right of individual or collective self-defence if an armed attack occurs."[146] As mentioned above, the legal discussion about the correct application of these terms for

[142] Rid, *Cyber War Will Not Take Place*.
[143] Schmitt, "'Attack' as a Term of Art in International Law."
[144] Stavridis, "Incoming: What Is a Cyber Attack?"; Schmitt, "Armed Attacks in Cyberspace: A Reply to Admiral Stavridis."
[145] Given the scope of this paper, the author will not go into further detail about the (legal) differences between 'the use of force' and 'an armed attack' in cyberspace. However, it is important to note that most scholars agree that the threshold under Art. 2(4) UN Charter is lower than under Art. 51 of the UN Charter. In other words, a particular cyber attack might breach Art. 2(4) but not rise to the threshold of allowing a state to invoke self-defense under Art. 51.
[146] United Nations, *Charter of the United Nations*.

cyberspace is still ongoing.[147] This leaves current politicians and policy-makers with a dilemma: How do you act in a situation in which precise legal definitions have not been generally agreed upon? For this reason, it is crucial to further clarify the applicability of international law in cyberspace. The Tallinn Manual was a success and helped this process move forward, though now a broader and more inclusive process is required to integrate actors such as China and Russia into the conversation. Russia has been promoting an International Code of Conduct for Information Security on the UN level[148], though it received fairly little traction so far given, especially among Western countries which disagree with the project given strong language on state control over Internet governance structures and content regulation.[149]

Based on the existing international legal framework, the further development of international legal norms requires a multilateral negotiation and development process; CBMs and capacity building can also be implemented on a regional level. Currently, the discussion on the scope of *existing* legal frameworks largely takes place within the United Nations UN and regional organizations. Parallel to that analysis, a discussion on the development of *new* legal norms for cyberspace, such as the potential international code of conduct for information security, is also taking place within the UN.[150] CBMs and capacity building are mostly taking place within regional organizations, such as the OSCE, the Organization for American States (OAS), and ASEAN. The

[147] NATO, *The Tallinn Manual on the International Law Applicable to Cyber Warfare*.
[148] For more than a decade, Russia has sought a treaty for broader international oversight of the Internet, banning deception or the embedding of malicious code, among other pressing measures of the cyber domain. But the United States has argued that measures banning offense can damage defense against current attacks, and would be difficult to verify or enforce.
[149] McKune, "An Analysis of the International Code of Conduct for Information Security"; Grigsby, "Net Politics » Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?"
[150] Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, "Proposal for an International Code of Conduct for Information Security."

EU is also actively engaged in providing capacity building for its member states and its own institutions.

In their 2013 report, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) reached a milestone on cyber conflict. Their consensus report identified for the first time three ways to reduce conflict in cyberspace: legal norms, CBMs, and capacity building.[151] While this list contains an implicit hierarchy, all three methods are crucial to improving the effectiveness of any one of them. In fact, this paper argues that all three are reinforcing and supporting each other. Since that report, the UN GEE has been trying to identify ways to deal with cybersecurity challenges on an international level. In July 2015, the UN GEE released its latest report which proposes additional norms of responsible state behavior and includes comments on how international law applies in cyberspace.[152] However, the new norms and principles of the 2015 report focus on ICTs and nation-states' critical infrastructure.

It is unfortunate that the latest UN GEE report "did not reconcile the ongoing tensions over the scope of state sovereignty with respect to the Internet"[153]. This challenge remains a core issue that cannot be addressed without extensive and constructive contributions from a variety of nation-states and non-state actors. This growing frustration on the limited power of the UN GEE, which is technically a UN working group that relies on an annual renewal of its mandate, is oftentimes reflected in calls for the establishment of a body with more authority.[154] However, given the

[151] United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013.
[152] United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015.
[153] Meyer, "Seizing the Diplomatic Initiative to Control Cyber Conflict."
[154] Meyer, "Another Year, Another GGE? The Slow Process of Norm Building for Cyberspace."

extensive amount of uncertainty and sources of instability described in Chapter One, key actors such as the United States, China, and Russia have a few incentives to give away national authority to influence the international agenda on cybersecurity toward an international organization they cannot control as much.

Norms help enter a new area of activity where existing laws are inapplicable or non-existent. They help pave the way through non-binding principles. Even if they do not give rise to a new law, norms create expectations and foster discussion among actors. In fact, norms shape expectations, which are critical for states to rationally calculate their interests and define behavior. Shared expectations through norms help avoid the cost of conflict, because they reduce friction and create greater predictability, which reduces transaction costs. However, there is no clear-cut hierarchy among the many norms that govern cyber activities; this confusion is why scholars like Joseph Nye refer to this environment as a regime complex.[155]

When it comes to states' efforts to reduce conflict in cyberspace, international legal norms have received considerable attention in recent years. This is particularly true for states that believe in the value and relevance of the current international legal order.[156] In fact, the international community largely agrees that existing international law applies in cyberspace. However, "the guidelines on how this should be done in practice are only beginning to emerge."[157] Several key state actors, such as China and Russia, disagree with the Western approach to the ILO and are making efforts to adjust it according to their preferences.[158] Their efforts to implement an

[155] Nye, "The Regime Complex for Managing Global Cyber Activities."
[156] ILO refers to the body of law that governs the legal relations between or among states or nations. For an extensive discussion on the current state of the international legal order see: Kennedy, "The International Symposium on the International Legal Order."
[157] Pawlak, "Cyber Diplomacy," 2.
[158] Lindsay, "The Impact of China on Cybersecurity"; Beach, "China and Russia Support 'Cyber Sovereignty.'"

international code of conduct for information security are the most prominent, but not the only example of such efforts.[159]

Under current circumstances, 'cyber security' and 'information security' are the two main themes that are discussed and debated among states. For the United States, cybersecurity largely relates to the "[p]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."[160] In contrast, China defines information security as an issue that "involves not only the risks arising from the weakness and interconnected nature of the basic information infrastructure, but also the political, economic, military, social, cultural, and numerous other types of problems created by the misuse of information technology. On the other hand, Russia is most concerned about the principles of non-interference in the internal affairs of states via their national information space. It therefore not only considers the physical effects to assets, but the ability to influence a state's information space, which has the potential to alter the public's opinion. These different approaches are worthy of concern when studying the issue of information security."[161] Comparing them, one notices that while some portions of both themes have overlap, there is considerable disagreement about the very idea of 'security'. Having significantly diverging perspectives at the core issue at hand prevents the development of more meaningful conversations. Overcoming these differences is

[159] Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, "Proposal for an International Code of Conduct for Information Security."
[160] Department of Defense, "Department of Defense Dictionary of Military and Associated Terms," 58.
[161] Permanent Representative of the People's Republic of China, "Submission to the United Nations General Assembly Resolution A/62/98."

therefore crucial for the success of international legal norms in preventing military escalation in cyberspace.

Beyond the political disagreements among states, the technical constraints outlined in Chapter One further complicate the development of effective legal norms. This implication further leads to the question of whether the current emphasis on international legal norms is in fact helpful to solve the challenge of conflict in cyberspace. Would international legal norms help prevent, or at least reduce conflict in cyberspace? There is a wide spectrum[162] of scholarly work on this topic and the key conclusion that can be drawn is that international cooperation is understood to be "essential to reduce risk and enhance security", just as the UN GGE Report stated already in 2013.[163] Nevertheless it remains disputed what kind of cooperation is necessary, which actors will be involved, and how this cooperation can be institutionalized.

Another effort to reduce the likelihood of military escalation in cyberspace could be the complete demilitarization of cyberspace, inspired by the Antarctic Treaty that forbids any military activity in Antarctica. Such a push might be very difficult to implement at this point, though the establishment of certain demilitarized zones that are internationally recognized are still feasible. The current debate about a norm around non-interference with critical infrastructure in peace time is an excellent example of these efforts.[164] While small in scope and oftentimes only narrowly applied, combined they contribute significantly toward preventing military escalation in cyberspace.

---

[162] Maurer, "Cyber Norm Emergence at the United Nations"; Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law"; Watts, "Cyber Norm Development and the United States Law of War Manual"; Selin, "Governing Cyberspace"; Hurwitz, "The Play of States."
[163] United Nations, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013.
[164] Hanson, "Waging (cyber)war in Peacetime."

To summarize, the key conditions on the global level that would help reduce the likelihood of military escalation in cyberspace are the complete demilitarization of cyberspace, an effective conflict prevention mechanism through the UN or other international organizations to address root causes of international disputes, a clear and precise understanding of how public international law applies to military operations in cyberspace, clarity about what 'cyber warfare', an 'armed attack', or 'the use of force' in cyberspace mean, sufficient capacity building among international organizations to effectively cope with crises originating in cyberspace, and the codification of international legal norms surrounding the limitations on military operations in cyberspace.

4.4 Solutions on the Cyber Infrastructure Level

Most causes for military escalation in cyberspace are not related to cyber infrastructure per se. In fact, its borderless design probably helped restrain states from using more aggressive means in cyberspace so far. Data package flow ignores national boundaries – to the frustration of many nations who want to impose tighter control on what their citizens have access to. This obliviousness toward national sovereignty raises the costs of military escalation for all actors that take advantage of digital innovations, which applies to most nations with advanced military cyber capabilities. Maintaining one single cyberspace and preventing regional independent networks is therefore a key effort in preventing military escalation in cyberspace. While this does not address the root causes or reduces friction, it maintains a high threshold.

To summarize, the key condition on the cyber infrastructure level that would help reduce the likelihood of military escalation in cyberspace is to maintain a global borderless cyberspace environment.

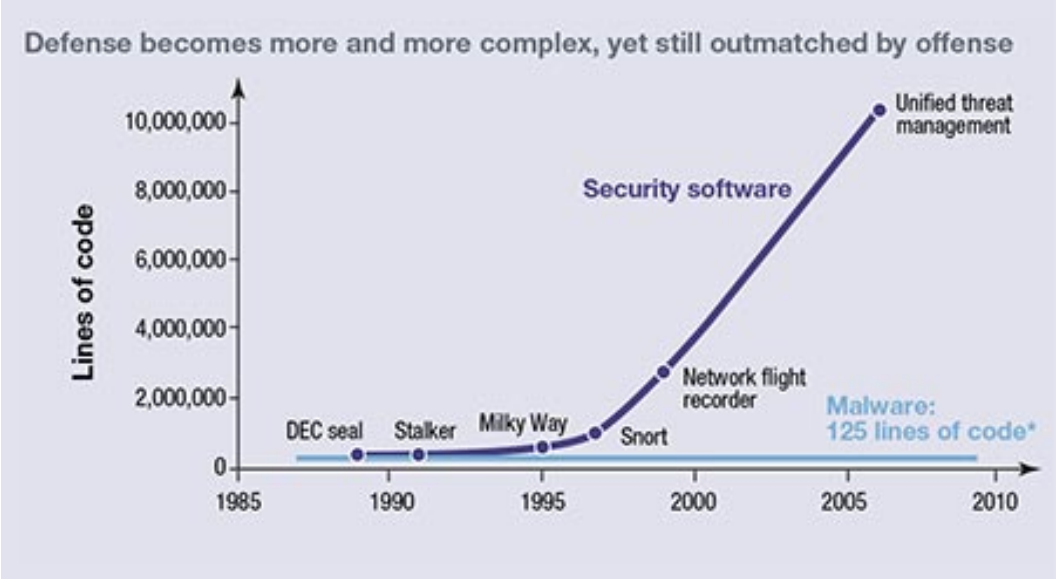
4.5 Cross-Cutting Solutions

Generally, increased globalization and economic interdependence between nations have a positive effect on the likelihood of military escalation in cyberspace because they increase the costs for the perpetrator. If an offensive cyber operation potentially has negative second or third tier effects on its own economy, financial market or cyberspace infrastructure, a perpetrator might be less inclined to take this risk. While it is unlikely that states will increase interdependencies for the sake of reducing the likelihood of military escalation in cyberspace, this connection is important to keep in mind for the following cross-cutting solutions.

An important step toward a more secure cyberspace environment can be done by "simple processes focused on ensuring internal security, basic computer hygiene practices, and logical network security protocols."[165] These steps would significantly increase the threshold for success of hacks or intrusions. As Figure Six depicts below, until today one of the key frustrations for cyber scholars and policy-makers at large is the imbalance between offensive and defense operations in cyberspace. McGraw argues that "cyber war, cyber espionage, and cyber crime all share the same root cause: our dependence on insecurity networked computer systems"[166] This dilemma is reflected in Figure Six below, which highlights how, on average, malware continues to be fairly easy to code, while security software is becoming exponentially more complex.

[165] Valeriano and Maness, *Cyber War versus Cyber Realities*, 209.
[166] McGraw, "Cyber War Is Inevitable (Unless We Build Security In)," 111.

Figure Six: Comparison between complexity of offensive and defensive software[167]



Source: DARPA, "Brief to Defense Science Board (DSB) Task Force", May 2011.

Fixing vulnerabilities, especially 'low-hanging fruit', or at least decreasing the overall amount of vulnerabilities would be a key feature of reducing all three threats because it would increase the costs for the attacker and reduce the likelihood of success.[168] Calls for improved 'cyber hygiene' are spiked in the last years and are receiving more attention by the public and business sector. For example, the latest Global Cyber-Vulnerability Report describes that "…cyber-vulnerability of countries as a whole is positively correlated to the number of downloaded binaries and negatively correlated with per capita GDP"[169] and concludes that "…practicing good cyber hygiene should be taught in elementary schools from the age of 6 onwards."[170] They further recommend that "…governments and businesses should make a 1-hour cyber-hygiene video that

[167] DARPA, "Brief to Defense Science Board (DSB) Task Force" Data through 2010.
[168] Valeriano and Maness, *Cyber War versus Cyber Realities*, 222.
[169] Subrahmanian et al., *The Global Cyber-Vulnerability Report*, 2.
[170] Ibid.

explains best practices for their employees and encourage them to share these habits with their family, friends, and professional colleagues."[171] Such suggestions sound fairly trivial, but remain underappreciated by most governments. Interestingly, the report places a higher priority on fostering education on 'cyber hygiene' than the development national cyber defense capabilities.[172] While it is unlikely that many nations will follow this prioritization, it reflects the scholarly acknowledgement on the importance of educating the general public about cyber hygiene.

Moreover, the current offensive-defensive imbalance can be addressed by creating an environment that incentivizes national resilience over deterrence strategies. Scotland was the first country in the world that published a national cyber resilience strategy in 2015.[173] The strategy includes proposals for the Scottish government, the public sector at large, the private sector and the third sector (such as NGOs).[174] The strategy is based on four pillars: 1. Leadership and Partnership Working 2. Awareness Raising and Communication 3. Education, Skills and Professional Development 4. Research and Innovation. For each pillar, specific proposals for different actors are put forward. Significant funding, awards and other incentives are created to facilitate the implementation of their strategy. The current roadmap aims for a complete implementation of all proposals until 2020.[175] While this strategy is focused on addressing risks caused by cyber-crime and less by military cyber operations, it reflects the growing awareness among governments toward resilience as a core component of cyber security.

In a similar effort to improve cyber resilience among private actors, the U.S. Department of Homeland Security (DHS) launched the Cyber Resilience Review (CRR), to "…help [U.S.]

[171] Ibid.
[172] Ibid., 26–27.
[173] The Scottish Government, "Safe, Secure and Prosperous: A Cyber Reslience Strategy for Scotland."
[174] Ibid., 18.
[175] Ibid., 36–27.

critical infrastructure providers understand their operational resilience and ability to manage cyber risk" in 2014.[176] The initial report showed, among other aspects, that:

- "…only 31% of organizations have implemented threat monitoring procedures";[177]
- "…only 38% of organizations implement methods (whether technical, administrative, or physical inspection) to actively discover changes to their technology assets [within their Configuration and Change Management]";[178]
- and "…even though 73% of organizations identify their services and roughly 60% to 83% inventory their assets, approximately 35% to 50% of organizations do not associate inventoried assets to the critical services they support."[179]

The results reflect the actuality of how incomplete resilience components among private entities are in the United States. However, based on the CRR, DHS is now able to tailor future efforts on cyber resilience toward the exact needs and weaknesses of private entities in the United States. Hopefully more nations will follow suit and implement comparable resilience analysis projects.

To summarize, the key cross-cutting solutions creating conditions that reduce the likelihood of military escalation in cyberspace are an increase in globalization and economic interdependence among nations, and a higher threshold of success for attackers in cyberspace. The threshold could be raised by: more sophisticated and widespread 'cyber hygiene' practices; an

[176] Scolieri and Vrtis, "A Scorecard for Cyber Resilience: What We Have Observed - Department of Homeland Security - CERT," 5.
[177] Ibid., 37.
[178] Ibid., 29.
[179] Ibid., 26.

overall change in the imbalance between offensive and defensive operations in cyberspace; the absence of 'low-hanging fruit' or a reduction in software vulnerabilities; an international environment that encourages states to focus on improving national resilience instead of concentrating exclusively on deterrence strategies; and strong network resilience among private actors.

Chapter 5 – Recommendations for Implementation

The potential solutions to reduce the risk of military escalation in cyberspace outlined in the previous Chapter are ineffective without proper and sustainable implementation. While most of them need to be implemented by governments, international organizations play a key role in increasing the incentives and facilitating the implementation process.

Current regional and international institutions largely lack the authority to take over this role. For this reason, existing international platforms such as the UN GGE need to receive a stronger mandate that is not limited to a yearly renewal through the UN General assembly. The negotiations have reached a level of complexity where internal capacity building, especially on the technological side, is crucial for further discussion. The discussion about international legal norms, laws of war in cyberspace, and CBMs should be further expanded beyond current fora such as the OSCE. Moreover, international organizations should receive a stronger mandate to monitor activities in cyberspace. This would provide policy-makers, diplomats, and researchers a rich database to back up future decisions on policy reforms with data that reflects the actual developments within cyberspace. Simultaneously, such a reform should also provide nations with an increasingly large portion of cyberspace users — such as India, Brazil, and China — with more room to express their political, legal, and technological concerns through diplomatic channels. This would likely lead to more buy-in and increased trust among nation-states.

Additionally, by providing the government representatives with a more sustainable framework for international negotiation and collaboration, it will also be easier to include private actors in the discussion. While the current regional and international collaboration frameworks give some room for their voices, they are not sufficiently well integrated into discussions. By opening the door to Internet businesses (such as Internet service providers), technology experts,

and other private actors, future policy decisions are more likely to be technologically feasible to implement. Once states accept that the inclusion of private actors help reduce conflict and increases trust internationally, the frameworks for collaboration should be gradually expanded toward broader participation. Cybersecurity expert Jason Healey argues that the inclusion of private actors should go even further in the United States by changing the Department of Defense and National Security Agency's role from "in command" toward "supporting command" when it comes to cyber defense and resilience.[180] While such a proposal is unlikely to get implemented anytime soon, it reflects the growing desire among scholars to reduce the emphasis of military cyber power within the United States and put more emphasis on non-military defense options.

A core task for national governments is to address the sources of insecurity on the cognitive level. As outlined in the previous Chapter, this could be done by a significant increase in national capacity building among current diplomats and policy-makers to help them understand the technological characteristics of cyberspace. The same holds true for information technology experts who lack a legal or policy background. Such efforts would contribute significantly toward the demystification of cyberspace described in the previous Chapter. Additionally, by bringing more technical experts from around the world together, a shared understanding of technical terms and knowledge can develop across countries. Such efforts exist within some countries and regions, but there needs to be more effort put into such projects, especially across ideological regions.

A potential role for civil society and academic scholars lies with in cognitive level as well. By acknowledging the importance of the human element within this development, not just for today but for many generations to come, it is easy to understand why efforts to train future

[180] Healey, "Taking Stock of the Latest Dynamics of Cyber Conflict."

generations of policy-makers, lawyers, and technology experts about the interdisciplinary challenges of governing conflict in cyberspace are crucial. Oxford University's Center for Doctoral Training in Cyber Security and the ASPIRE program at New York University Law School are among the first institutional programs of their kind. Hopefully there will be more such programs in the future.

A joint effort by private entities, government bodies and international organizations should be made to maintain one single cyberspace. Avoiding the disintegration of cyberspace remains key to prevent military escalation in cyberspace. The economic opportunities that a global cyberspace offers cannot maintained in a segregated cyberspace. By raising awareness of the strong nexus between economic prosperity and cyberspace, future negotiations will generate more responsibility, hopefully furthering an even better understanding of global cyberspace. Increased awareness and contact will also promote interdependence among states in terms of managing the infrastructure and maintenance of cyberspace.

Academic scholars, NGOs and private sector representatives also play a key role in promoting the advantages of a stable, borderless, and secure cyberspace. They are positioned to pressure states to further establish transparency measures, promote improved national 'cyber hygiene' programs, increase economic and political dependencies among nations.

National policy-makers should further promote a military cyber strategy based on restraint, rather than uncontrolled operations. Case studies of this paper indicate that this seems to be the case for most nations. However, more work should be done to roll back the increasingly 'military' discourse about cyberspace. This is especially relevant for policy-makers in the United States who are exposed to extensive media reports that oftentimes reflect more fear than real facts about incidents in cyberspace. Moreover, policy-makers should increase the incentives within their

military to further explore how the current imbalance between offensive and defensive operations in cyberspace can be shifted. Ideally, technological adjustments in software and hardware development, improved resilience, and less uncertainty within military response plans can lead to an environment that reduces the likelihood of military escalation in cyberspace.

To summarize, the conditions that help reduce the likelihood of military escalation in cyberspace outlined in the previous Chapter need to be implemented by international organizations, states, and non-state actors. International organizations should press for a stronger mandate to facilitate the implementation process of global solutions. They should also receive the authority to develop more inclusive and effective platforms for negotiation between states, private businesses, and non-state actors. States should develop more sophisticated frameworks for collaboration with private businesses, increase their national capacity building among diplomats and policy-makers, and put stronger emphasis on shifting the current imbalance between offensive and defense military operations in cyberspace. Non-state actors should develop more training opportunities for policy-makers, lawyers, and technology experts about the interdisciplinary challenges of resolving conflict in cyberspace. Academics and NGOs are uniquely positioned to pressure states to improve transparency measures and promote better 'cyber hygiene' programs that go beyond governmental efforts. Representatives of the media and academia should roll back their 'military' discourse about cyberspace. All entities should make sure that cyberspace remains global and borderless. Avoiding the disintegration of cyberspace is key to reducing the likelihood of military escalation in cyberspace.

All of the aforementioned steps would improve the conditions that would reduce the likelihood of military escalation in cyberspace. It is now a matter of political will to implement these suggestions and maintain such commitments.

Conclusion

There is reason to worry about military confrontation in cyberspace, be it in a full scale cyber war or a component of a larger military activity. It is reasonable to assess that militarization of cyberspace is on the rise. Fortunately, so far states have restrained their military and intelligence operations in cyberspace. The case studies in Chapter Three have shown that states are testing the boundaries of what is politically and legally possible within cyberspace without crossing an escalation threshold. This observation highlights how important it is to establish a clear understanding of where the threshold lies to prevent military escalation in cyberspace. The *high* and *medium* risk case studies indicate that the main conditions that cause military escalation in cyberspace originate outside of cyberspace, namely through geopolitical disputes and large-scale military confrontation between adversaries.

The conditions that help reduce the likelihood of military escalation in cyberspace are divided between the cognitive, the state, and the global levels. Cross-cutting conditions are presented separately. First, the key conditions on the cognitive level that help reduce the likelihood of military escalation in cyberspace are increased efforts toward improving the understanding of cyberspace among policy-makers and similar efforts to help computer scientists better understand the implications of their work for political decision-making, both domestic and international. Second, the key conditions on the state level that help reduce the likelihood of military escalation in cyberspace are: increased transparency measures about military operations in cyberspace; a precise understanding of the applicability of cross-domain deterrence strategies in cyberspace; and the further development of CBM efforts focused on military operations in cyberspace. Third, the key conditions on the global level that help reduce the likelihood of military escalation in cyberspace are: the complete demilitarization of cyberspace, an effective conflict prevention

mechanism through the UN or other international organizations to address root causes of international disputes; a clear and precise understanding of how public international law applies to military operations in cyberspace; clarity about what cyber warfare, an 'armed attack', or 'the use of force' in cyberspace means; sufficient capacity building among international organizations to effectively cope with crises originating in cyberspace; and the codification of international legal norms surrounding the limitations on military operations in cyberspace. Fourth, the key conditions that help reduce the likelihood of military escalation in cyberspace originating out of cross-cutting solutions are: an increase in globalization and economic interdependence among nations and a higher threshold for success for attackers in cyberspace. The threshold could be raised by: more sophisticated and widespread 'cyber hygiene' practices; an overall change in the imbalance between offensive and defensive operations in cyberspace; the absence of 'low-hanging fruit' or a reduction in software vulnerabilities; an international environment that encourages states to focus on improving national resilience instead of concentrating exclusively on deterrence strategies; and strong network resilience among private actors.

International organizations, states, private businesses and other non-state actors play a crucial role in creating the aforementioned conditions. First, international organizations should press for a stronger mandate to facilitate the implementation process of global solutions. They should also receive the authority to develop more inclusive and effective platforms for negotiation between states, private businesses, and non-state actors. Second, states should develop more sophisticated frameworks for collaboration with private businesses, increase their national capacity building among diplomats and policy-makers, and put stronger emphasis on shifting the current imbalance between offensive and defensive military operations in cyberspace. Third, non-state actors should develop more training opportunities for policy-makers, lawyers, and technology

experts about the interdisciplinary challenges of resolving conflict in cyberspace. Academics and NGOs are uniquely positioned to pressure states to improve transparency measures and promote better 'cyber hygiene' programs that go beyond governmental efforts. Representatives of the media and academia should roll back the 'military' discourse about cyberspace. Fourth, all entities should ensure that cyberspace remains global and borderless. Avoiding the disintegration of cyberspace is key to reducing the likelihood of military escalation in cyberspace.

Overall, technological developments will continue to outpace policy and legal discussions. It is therefore important that policy-makers, technologists, businessmen, academics, and civil society representatives deepen the exchange of perceptions, ideas, and trends around conflict in cyberspace. Given cyberspace's borderless design, these exchanges should take place on an international level, facilitated, but not dominated, by states. Moreover, the identified conditions and measures would increase awareness of the political, legal, technological, and economic nexus in cyberspace, thus reshaping discussions about military escalation in cyberspace at large. Ultimately, such efforts will reduce the likelihood of military escalation within cyberspace. They will also create conditions in which dialogue among states can be more effective, sophisticated, and sustainable. Cyberspace has become a fundamental and inextricable realm of governmental activity. Maintaining a stable cyberspace is therefore not simply an interest, but a necessity.

In conclusion, the likelihood of military escalation in cyberspace can be significantly reduced. However, beyond the state-based activities in cyberspace, non-state actors with little or no ties to a state deserve further analytical attention since the threshold to acquire sophisticated offensive capabilities in cyberspace is slowly lowering. Restraints that apply to states in cyberspace only partially apply to hackers and criminals. Their actions have the potential to significantly destabilize cyberspace and foster an environment of instability.

Bibliography

Apps, Peter, and Jim Finkle. "Suspected Russian Spyware Turla Targets Europe, United States." *Reuters*. March 7, 2014. http://www.reuters.com/article/2014/03/07/us-russia-cyberespionage-insight-idUSBREA260YI20140307.

Arquilla, John. "Cyberwar Is Already Upon Us." *Foreign Policy*. February 27, 2012.

ASEAN. "ARF Work Plan on Security of and in the Use of Information and Communications Technologies." ASEAN, May 7, 2015.

Beach, Sophie. "China and Russia Support 'Cyber Sovereignty.'" *China Digital Times*, May 11, 2015, online edition.

Belson, Ken. "Senator's Slip of the Tongue Keeps on Truckin' Over the Web." *The New York Times*, July 17, 2006, sec. Business / Media & Advertising. http://www.nytimes.com/2006/07/17/business/media/17stevens.html.

Berlich, Christoph. *Schlachtfeld Internet? Eine Analyse Moderner Kriegsführung Am Beispiel Des Russisch-Georgischen Krieges 2008*. Hamburg: Diplomica, 2016.

Brake, Benjmanin. "Strategic Risks of Ambiguity in Cyberspace." Contingency Planning Memorandum. New York, USA: Council on Foreign Relations, May 2015.

Cardozo, Nate, and Eva Galperin. "What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?," May 28, 2015.

Chernenko, Yelena. "Global Cybersecurity: 6 Questions on the Key Issues as Seen from Moscow." *Russia Beyond The Headlines*. August 19, 2015. http://rbth.com/international/2015/08/19/global_cybersecurity_6_questions_on_the_key_issues_as_seen_from_48615.html.

Clapper, James R. "Worldwide Threat Assessment of the US Intelligence Community." Washington D.C.: Office of the Director of National Intelligence, February 26, 2015.

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. Vol. als eBook. New York City: Ecco, 2010.

DARPA. "Brief to Defense Science Board (DSB) Task Force." Defense Advanced Research Projects Agency (DARPA), May 2011.

Deeks, Ashley. "Tallinn 2.0 and a Chinese View on the Tallinn Process." *Lawfare Blog*, May 31, 2015. https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process.

Department of Defense. "Department of Defense Dictionary of Military and Associated Terms." Department of Defense, November 15, 2015.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. "W32.Stuxnet Dossier." Symantec, n.d.

Gallagher, Sean. "Encryption 'would Not Have Helped' at OPM, Says DHS Official." *Ars Technica*, June 16, 2015. http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/.

———. "Why the 'biggest Government Hack Ever' Got Past the Feds." *Ars Technica*, June 8, 2015. http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2 (October 2013): 41–73. doi:10.1162/ISEC_a_00136.

Geers, Kenneth, Darien Kindlund, Ned Moran, and Rob Rachwald. "World War C: Understanding Nation-State Motives behind Today's Advanced Cyber Attacks." Technical report, FireEye, 2014. http://ver007.com/tools/APTnotes/2013/fireeye-wwc-report.pdf.

Giles, Keir, and William Hagestad. “Divided by a Common Language: Cyber Definitions in Chinese, Russian and English.” In *Cyber Conflict (CyCon), 2013 5th International Conference on*, 1–17. IEEE, 2013. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6568390.

Goldman, Emily O., and John Arquilla. “Cyber Analogies.” Monterey, California, Naval Postgraduate School, 2014. http://calhoun.nps.edu/handle/10945/40037.

Goldsmith, Jack. “Can We Stop the Global Cyber Arms Race?” *The Washington Post*, February 1, 2010, sec. Opinions. http://www.washingtonpost.com/wp-dyn/content/article/2010/01/31/AR2010013101834.html.

GReAT. “The Epic Turla Operation Solving Some of the Mysteries of Snake/Uroburos.” *SecureList*, August 7, 2014. https://securelist.com/analysis/publications/65545/the-epic-turla-operation/.

Grigsby, Alex. “Net Politics » Will China and Russia’s Updated Code of Conduct Get More Traction in a Post-Snowden Era?” *Council on Foreign Relations - Net Politics*, January 28, 2015. http://blogs.cfr.org/cyber/2015/01/28/will-china-and-russias-updated-code-of-conduct-get-more-traction-in-a-post-snowden-era/.

Haley, Christopher. “A Theory of Cyber Deterrence.” *Georgetown Journal of International Affairs*, February 6, 2013. http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/.

Hanson, Fergus. “Waging (cyber)war in Peacetime.” *The Brookings Institution*, October 22, 2015. http://www.brookings.edu/blogs/up-front/posts/2015/10/22-cyberwar-in-peacetime-hanson.

Healey, Jason. “Cyber Deterrence Is Working.” *Defense News*. July 30, 2014, online edition.

———. “Stuxnet and the Dawn of Algorithmic Warfare.” *The Huffington Post*, 19:15 400AD. http://www.huffingtonpost.com/jason-healey/stuxnet-cyberwarfare_b_3091274.html.

———. “Taking Stock of the Latest Dynamics of Cyber Conflict.” The Fletcher School of Law and Diplomacy, April 11, 2016.

Healey, Jason, and Karl Grindal, eds. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Wien: Cyber Conflict Studies Association, 2013.

Healey, Jason, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Youd. “Confidence-Building Measures in Cyberspace - A Multistakeholder Approach for Stability and Security.” Washington D.C.: Atlantic Council, 2014.

Hirschfeld Davis, Julie, and David Sanger E. “Obama and Xi Jinping of China Agree to Steps on Cybertheft.” *New York Times*. September 25, 2015, online edition. http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html.

Hollis, Duncan. “Is a Use of Force the Same as an Armed Attack in Cyberspace?” *Opinio Juris*, December 8, 2015. http://opiniojuris.org/2012/04/28/is-a-use-of-force-the-same-as-an-armed-attack-in-cyberspace/.

Hurwitz, Roger. “The Play of States: Norms and Security in Cyberspace.” *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 322–31. doi:10.1080/10803920.2014.969180.

Joint Chiefs of Staff. “Cyberspace Operations.” Joint Publication 3-12 (R). Washington D.C.: Department of Defense, February 5, 2013.

———. “Information Operations.” Joint Publication 3-13. Washington D.C.: Department of Defense, November 20, 2014.

Kanuck, Sean. “Sovereign Discourse on Cyber Conflict Under International Law.” *Tex. L. Rev.* 88 (2009): 1571. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tlr88&section=56.

Kaspersky. “Kaspersky Lab Identifies Operation ‘Red October,’ an Advanced Cyber-Espionage Campaign Targeting Diplomatic and Government Institutions Worldwide.” *Virus News*, January 14, 2013. http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_Identifies_Operation_Red_October_an_Advanced_Cyber_Espionage_Campaign_Targeting_Diplomatic_and_Government_Institutions_Worldwide.

———. “The Epic Turla (snake/Uroburos) Attacks | Virus Definition.” Accessed April 23, 2016. http://www.kaspersky.com/internet-security-center/threats/epic-turla-snake-malware-attacks.

Kaspersky Lab Global Research and Analysis Team. “The Epic Turla Operation: Solving Some of the Mysteries of Snake/Uroboros.” Kaspersky, August 6, 2014.

Kennedy, David. “The International Symposium on the International Legal Order.” *Leiden Journal of International Law* 16, no. 4 (December 2003): 839–47. doi:10.1017/S0922156503001523.

Kenneth Geers, ed. *Cyber War in Perspective*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015.

Kissel, Richard. “Glossary of Key Information Security Terms.” National Institute of Standards and Technology, May 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

Krebs, Brian. “Catching Up on the OPM Breach — Krebs on Security,” June 15, 2015. http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/.

Langner, Ralph. “To Kill a Centrifuge - A Technical Analysis of What Stuxnet’s Creators Tried to Achieve.” Arlington | Hamburg | Munich: Langner Group, November 2013.

Lemieux, Frederic, ed. *Current and Emerging Trends in Cyber Operations*. Palgrave Macmillan, 2015. http://www.palgraveconnect.com/doifinder/10.1057/9781137455550.

Libicki, Martin C. “Would Deterrence in Cyberspace Work Even with Attribution.” Georgetown Journal of International Affairs, April 22, 2015. http://journal.georgetown.edu/would-deterrence-in-cyberspace-work-even-with-attribution/.

Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” *International Security* 39, no. 3 (January 2015): 7–47. doi:10.1162/ISEC_a_00189.

Markoff, John. “Vast Spy System Loots Computers in 103 Countries.” *New York Times*. March 28, 2009. http://www.nytimes.com/2009/03/29/technology/29spy.html.

Marks, Joseph. “U.N. Body Agrees to U.S. Norms in Cyberspace.” *Politico*. July 9, 2015. http://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900.

Maurer, Tim. “Cyber Norm Emergence at the United Nations.” *Cambridge, MA: Belfer Center for Science and International Affairs*, 2011. http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf.

McGraw, Gary. “Cyber War Is Inevitable (Unless We Build Security In).” *Journal of Strategic Studies* 36, no. 1 (February 2013): 109–19. doi:10.1080/01402390.2012.742013.

McKune, Sarah. “An Analysis of the International Code of Conduct for Information Security.” *Citizenlab Blog*, September 28, 2015. https://citizenlab.org/2015/09/international-code-of-conduct/.

Messmer, Ellen. “Stuxnet Cyberattack by US a ‘Destabilizing and Dangerous’ Course of Action, Security Expert Bruce Schneier Says.” *Network World*, June 18, 2012. http://www.networkworld.com/article/2189472/security/stuxnet-cyberattack-by-us-a--destabilizing-and-dangerous--course-of-action--security-expert.html.

Meyer, Paul. “Another Year, Another GGE? The Slow Process of Norm Building for Cyberspace.” *ICT for Peace Foundation*, September 4, 2015. http://ict4peace.org/another-year-another-gge-the-slow-process-of-norm-building-for-cyberspace/.

———. “Seizing the Diplomatic Initiative to Control Cyber Conflict.” *The Washington Quarterly* 38, no. 2 (April 3, 2015): 47–61. doi:10.1080/0163660X.2015.1064709.

Morgan, Forrest E., Project Air Force (U.S.), and United States, eds. *Dangerous Thresholds: Managing Escalation in the 21st Century*. Rand Corporation Monograph Series. Santa Monica, CA: RAND Project Air Force, 2008.

Mudrinich, Erik. “Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem.” *Air Force Law Review 68* 68 A.F. L. Rev. (2012).

National Intelligence Council. “Iran: Nuclear Intentions and Capabilities.” National Intelligence Estimate. Office of the Director of National Intelligence, November 2007.

NATO. *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Edited by Michael N. Schmitt. Cambridge: Cambridge University Press, 2013.

New America Foundation. “Global Cyber Definitions Database.” *New America*. Accessed May 10, 2016. https://www.newamerica.org/cyber-global/cyber-definitions/.

Nye, Joseph. *The Future of Power*. New York: PublicAffairs, 2011.

Nye, Joseph S. “The Regime Complex for Managing Global Cyber Activities,” 2014. http://dash.harvard.edu/handle/1/12308565.

Nye Jr, Joseph S. “Nuclear Lessons for Cyber Security.” DTIC Document, 2011. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA553620.

Organization for Security and Co-operation in Europe Permanent Council. “Decision No. 1106 Initial Set Of OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies.” 975th Plenary Meeting. Vienna, Austria: OSCE, December 3, 2013.

Pawlak, Patryk. “Cyber Diplomacy.” Briefing. Brussels, Belgium: European Parliament, October 2015.

Perlroth, Nicole. “Cyberattack on Saudi Oil Firm Disquiets U.S.” *The New York Times*, October 23, 2012. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

Perlroth, Nicole, and David E. Sanger. “North Korea Loses Its Link to the Internet.” *The New York Times*, December 22, 2014. http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html.

Permanent Representative of the People’s Republic of China. “Submission to the United Nations General Assembly Resolution A/62/98,” 2008.

Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan. Formal letter to the UN Secretary General - A/66/359. “Proposal for an International Code of Conduct for Information Security.” Formal letter to the UN Secretary General - A/66/359, September 14, 2011.

Peterson, Andrea. “The Government Is Headed back to the Drawing Board over Controversial Cybersecurity Export Rules.” *Washington Post*. July 29, 2015, online edition.

Rantapelkonen, Jari, Mirva Salminen, and others. “The Fog of Cyber Defence.” *Julkaisusarja 2. Artikkelikokoelma N: O 10*, 2013. http://www.doria.fi/handle/10024/88689.

Rid, Thomas. *Cyber War Will Not Take Place*. Vol. als eBook. New York City: Oxford University Press, 2013.

RiskBasedSecurity. “A Breakdown and Analysis of the December, 2014 Sony Hack,” December 5, 2014. https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/.

Rõigas, Henry, and Tomáš Minárik. “2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law.” Incyder News. Tallinn, Estonia: CCDCOE, August 31, 2015.

Roth, Andrew. “Russia and China Sign Cooperation Pacts.” *New York Times*. May 8, 2015, online edition. http://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0.

Sanger, David E., and Martin Fackler. “N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say.” *The New York Times*, January 18, 2015. http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html.

Schmitt, Michael N. “Armed Attacks in Cyberspace: A Reply to Admiral Stavridis.” *Lawfare Blog*, January 8, 2015. https://www.lawfareblog.com/armed-attacks-cyberspace-reply-admiral-stavridis.

———. “‘Attack’ as a Term of Art in International Law: The Cyber Operations Context.” In *Cyber Conflict (CYCON), 2012 4th International Conference on*, 1–11. IEEE, 2012. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243981.

Schneier, Bruce. “Attack Attribution and Cyber Conflict - Schneier on Security.pdf.” *Schneier on Security*, March 9, 2015. https://www.schneier.com/blog/archives/2015/03/attack_attribut_1.html.

———. “Computer Network Exploitation vs. Computer Network Attack.” *Schneier on Security*, March 10, 2014. https://www.schneier.com/blog/archives/2014/03/computer_networ.html.

———. “We Still Don’t Know Who Hacked Sony.” *The Atlantic*, January 5, 2015. http://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/.

Scolieri, Philip A., and Bob Vrtis. “A Scorecard for Cyber Resilience: What We Have Observed - Department of Homeland Security - CERT.” Carnegie Mellon University, October 14, 2015.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs, 2016.

Selin, Sean. “Governing Cyberspace: The Need for an International Solution.” *Gonz. L. Rev.* 32 (1996): 365. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/gonlr32&section=18.

Shackelford, Scott J., J. D. Scott Russell, and Andreas Kuehn. “Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors.” *Kelley School of Business Research Paper*, no. 15–64 (2015).

http://works.bepress.com/cgi/viewcontent.cgi?params=/context/scott_shackelford/article/1016/type/native/&path_info=.
Sheldon, John B. "Geopolitics and Cyber Power: Why Geography Still Matters." *American Foreign Policy Interests* 36, no. 5 (September 3, 2014): 286–93. doi:10.1080/10803920.2014.969174.
Singer, P. W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford ; New York: Oxford University Press, 2014.
Sputnik International. "UN Cybersecurity Report Compromises on Self-Defense Issue - Russian Official." *Sputnik International*, August 17, 2015, online edition. http://sputniknews.com/politics/20150817/1025819426/UN-cybersecurity-report-compromises-on-self-defence.html.
Stahl, William M. "Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity, The." *Ga. J. Int'l & Comp. L.* 40 (2011): 247. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/gjicl40&section=12.
Stavridis, James. "Incoming: What Is a Cyber Attack?" *Armed Forces Communications and Electronics Association Magazine*, January 1, 2015. https://www.afcea.org/content/?q=incoming-what-cyber-attack.
Sternstein, Aliya. "The Pentagon Still Hasn't Decided Who's In Charge If America Comes Under Cyberattack." *Defense One*, April 4, 2016. http://www.defenseone.com/technology/2016/04/pentagon-still-hasnt-decided-whos-charge-if-america-comes-under-cyberattack/127224/.
Subrahmanian, V.S., Michael Ovelgonne, Tudor Dumitras, and B. Aditya Prakash. *The Global Cyber-Vulnerability Report*. Terrorism, Security, and Computation. Cham: Springer International Publishing, 2015. http://link.springer.com/10.1007/978-3-319-25760-0.
Swire, Peter. "The Declining Half-Life of Secrets." *New America Cybersecurity Fellows Paper Series* 1, no. 1 (2015). https://static.newamerica.org/attachments/4425-the-declining-half-life-of-secrets/Swire_DecliningHalf-LifeOfSecrets.f8ba7c96a6c049108dfa85b5f79024d8.pdf.
Tatam, Robin. "Cracking the Problem of Endpoint Security." Helpsystems, December 19, 2014. http://www.helpsystems.com/powertech/cracking-endpoint-security-problems.
Techopedia. "What Is Stuxnet? - Definition from Techopedia." *Techopedia.com*. Accessed April 29, 2016. https://www.techopedia.com/definition/15812/stuxnet.
The Department of Defense. "The DoD Cyber Strategy," April 2015.
The Scottish Government. "Safe, Secure and Prosperous: A Cyber Reslience Strategy for Scotland." Scotland: The Scottish Government, November 2015.
Tiezzi, Shannon. "Report: 'Highly Sophisticated Cyber Espionage' Group Linked to Chinese Intelligence." *The Diplomat*. October 29, 2014. http://thediplomat.com/2014/10/report-highly-sophisticated-cyber-espionage-group-linked-to-chinese-intelligence/.
Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2008.
United Nations. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." New York, USA: United Nations, June 24, 2013.

———. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” United Nations, July 22, 2015.

United States District Court - Western District of Pennsylvania. “Peoples Liberation Army Indictment,” May 2014.

Valeriano, Brandon, and Ryan C. Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford ; New York: Oxford University Press, 2015.

von Solms, Rossouw, and Johan van Niekerk. “From Information Security to Cyber Security.” *Computers & Security* 38 (October 2013): 97–102. doi:10.1016/j.cose.2013.04.004.

Watts, Sean. “Cyber Norm Development and the United States Law of War Manual.” In *NATO Cooperative Cyber Defence Centre of Excellence, International Cyber Norms Development*, by Anna-Maria Osula. Tallinn, Estonia: ATO Cooperative Cyber Defence Centre of Excellence, 2016.

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