UNIVERSITY OF MACEDONIA

SCHOOL OF SOCIAL SCIENCES, HUMANITIES AND ARTS

Department of International & European Studies

Master's Degree in International Studies

Student's Name: Georgiadis Anastasios, Master's Degree Class of 2020-21

Thesis Title: Cyberpower and Weaponization of Cyber Proxies

April 2022

ABSTRACT

The escalated development of cyberspace reveals several new threats in human, domestic and international security among others. The new vulnerabilities that are being introduced can result in significant impacts on our safety and well-being in general, as cyberspace accounts for a fruitful environment for criminality and fraud to flourish, and challenge the traditional notions of privacy. Nationally, cybersphere can affect public decision-making through misinformation or manipulation of democratic procedures, while internationally can escalate crises and lead to conflict among actors.

The necessary initiatives to be integrated will consist of sophisticated technical endeavors -adequate to protect linked devices from malicious activities, behavioral transformation regarding the way we respond to threats, legal updates to ensure a higher quality protection of critical infrastructures and privacy, and international cooperation in order to establish norms that address cyber activity.

The actors operating in the cyber realm, as well as the interaction among them, are also a complex aspect of this domain. In conventional domains we have noticed the well-established presence of states, as the primary actors with power, capabilities, and resources. What is interesting about cyberspace is the active participation of non-state actors and their role in assisting states to project even more power. The so-called ‘proxies’ are not an innovating parameter in international relations, as they have been under scope since the era of Thucydides, in ancient Greece. Yet, in the cyber realm they acquire skills and capabilities which transform them to considerable actors -at times even more vital than states per se-.

Examining cyber proxies as non-state actors, including the benefits and risks that may result from their cooperation with states, and the different forms of relationship between states and proxies, will be an asset to the comprehensive understanding of cyberspace overall. Furthermore, a conceptualization of ‘state-proxy’ relationships can be an efficient tool for political decision-makers, as well as a solid guideline for future research in aspects regarding cyber proxies and cyberspace.

LIST OF ACRONYMS AND ABBREVIATIONS

AID	Actor and Intent Definition
C2	Command and Control
CBM	Confidence-Building Measure
CCI	Cyber Capability Index
CII	Cyber Intent Index
CNA	Computer Network Attacks
COG	Centers of Gravity
CPNI	Centre for Protection of National Infrastructure
CYBERCOM	U.S. Cyber Command
DDoS	Distributed Denial of Services
DHS	Department of Homeland Security
DNS	Domain Name System
DoD	Department of Defense
DPRK	Democratic People’s Republic of Korea
IC	U.S. Intelligence Community
ICBM	Inter-Continental Ballistic Missile
ICT	Information & Communication Technology
IO	Information Operations
IoT	Internet of Things
IP	Internet Protocol
IRC	Internet Relay Chat
IRGC	Islamic Revolutionary Guard Corps
ISP	Internet Service Provider
IT	Information Technology
NASDAQ	National Association of Securities Dealers Automated Quotations
NATO	North Atlantic Treaty Organization
NBC	Nuclear, Biological, and Chemical Weapons
NCPI	National Cyber Power Index
NCSC	National Cyber Security Centre
OS	Operating System
OSINT	Open Source Intelligence
R&D	Research and Development
RBN	Russian Business Network
SEA	Syrian Electronic Army
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
USSR	Union of Soviet Socialist Republics

LIST OF FIGURES AND TABLES

Figure 1.1., Actor and Intent Definition Model 15
Figure 2.1., Hacker Categories and Motives 24
Figure 2.2., Motivation and its factors 30
Figure 2.2.1., Capabilities and their factors 32
Figure 2.2.2., Restraints and their factors 34
Figure 2.3., Levels of attribution 36
Figure 3., NCPI equation 49
Figure 3.1., The Most Comprehensive Cyber States in 2020 50

Table 1.1., Libicki's seven forms of information warfare 10
Table 1.2., Beneficiary-Proxy Relationships 17
Table 2.1., Main non-state actors in cyber attacks 22
Table 3.1., Top 5 Intent Ranking by Objective 51
Table 3.1.1., Top 5 Capabilities Ranking by Objective 52
Table 3.2., Politically vs Financially Motivated Cyber Proxies 65
Table 3.3., Optimal choice of Cyber Proxies 68

TABLE OF CONTENTS

ABSTRACT **2**

LIST OF ACRONYMS AND ABBREVIATIONS **3**

LIST OF FIGURES AND TABLES **3**

CHAPTER I **7**

INTRODUCTION **7**

Research Question 8

Thesis Structure 8

Methodology 9

Key Concepts 9

Information warfare 9

Cyberspace 11

Cyber warfare 12

Cyber War 16

Proxy and Cyber Proxy 16

CHAPTER II **19**

EMERGING CYBER THREATS: HOW THEY AFFECT THE INTERNATIONAL & DOMESTIC SECURITY? **19**

What is new in international security? How does it affect the states? **19**

Actors in cyberspace 19

States in Cyberspace 20

Non-state actors in Cyberspace 21

What are the forms of cyber threats? How can they be developed and proliferated? **27**

Cyber Weapons 27

Development and Proliferation 29

Attribution issues 35

How states respond to cyber threats? **37**

Cyber arms control 37

Cyber Deterrence 40

CHAPTER III **45**

USE OF PROXIES TO PROJECT CYBERPOWER IN INTERNATIONAL RELATIONS **45**

Power and Cyberspace 46

How to measure Cyberpower? 48

Comparing traditional forms of power with Cyberpower 53

Cyberpower defined and implemented by Great Powers: Case Studies 54

Cyberpower through traditional political concepts 57

Contribution to Offense and Defense 59
How to build Cyberpower? 59
State and Proxies 61
Why proxies over alliances and mercenaries in cyberspace? 61
Mutual Benefits 63
Categorization: Politically vs Financially Motivated Proxies 65
Criteria for Choosing Cyber Proxies 66
Promethean Dilemma and Dilemma of Inadvertent Crisis Escalation 68
Categorization: Distinguished types of relationship 69

CHAPTER I

INTRODUCTION

In this part of the dissertation, I will review a variety of definitions and terms that I consider significant, in order to further understand the concept of cyberspace. It is essential to establish a common ground concerning crucial aspects of this domain, due to their complexity and arising challenges. As I review several phenomena that usually already exist in conventional domains, I will further examine them in the context of the cyber realm.

Both nature and actors operating in the cyber realm are quite complex, due to unique correlation and attributes existing in this domain. When states conduct cyber operations, there are also implications in international stability, as well as consequences to targeted states or non-state actors. So far, there is not a clear legal framework defining the severity, or any guidelines that correspond to an analogous response to a cyber operation, and thus escalation to conventional level is likely to occur, under specific circumstances.

Non-state actors in cyberspace sometimes can be considered as important as states, and it is very common to establish a proxy relationship, where both parties gain advantages on their behalf and promote their interests. For example, some states do not acquire inherent technical cyber capabilities to conduct a cyber operation, hence they cooperate with a sophisticated non-state group to maximize the quality level. For example, DPRK proves exactly this allegation, as the country itself maintains obsolete IT capabilities, yet its cooperation with cyber proxies results in highly sophisticated cyber operations. On the other hand, non-state actors may receive direct financial support, or domestic legal protection by the state providing thus powerful motives to cyber proxies. Some of the most notable operations of cyber proxies are the DDoS attacks to Estonian networks in 2007, to Georgian networks in 2008, and to Kyrgyzstan in 2009, all allegedly conducted by Russian proxies. What remains is to examine the type of relationship, the motives, the goals, and the risks of a 'beneficiary-proxy' relationship in the cyber realm.

Research Question

States today use proxies -specifically non-state actors- in order to project their power in cyberspace. Examining the relationship between beneficiaries and proxies could potentially contribute to a better understanding of the cyber domain as a new field of competition, and provide a rational explanation of what are the motives and benefits in the establishment and the continuation of such a relationship in cyberspace. The expected outcomes from a deeper analysis of state-proxy relationships will also facilitate the enhancement of methods of deterrence, international monitoring, and the adoption of a clearer understanding on the legal norms necessary for a more comprehensive control over the cyber realm.

The questions needed to be targeted during my research upon the state-proxy relationships are among others: what are the different types of relationships? How are these relationships being organized? Why does a state choose a proxy to project cyberpower and how is it going to achieve it?

Thesis Structure

This thesis consists of four major chapters. Chapter I initiates with an introduction to the examining topic, seeking to familiarize the reader with related terms and key concepts. It also provides information related to practical issues of research, such as the purpose, along with the process of obtaining the relevant information for this assignment, which can be described as the methodology that I have used to approach and critically analyze academic papers, books, articles, and governmental publications.

Chapter II focuses on the forms of cyber threats, their attributes and characteristics introduced because of its nature. Besides these new arising threats and their attributes, this chapter underlines states' attempts to confront them.

Chapter III describes the concept of cyber power in international relations, as well as the non-state actors who act as proxies. There are distinct types of cyber proxies and I underline the state's necessity of choosing the adequate ones, depending on goals, motivation, capabilities, and so on. These actors can be a crucial addition to a state's overall power, hence their correlation accounts for a significant aspect to be examined.

Finally, I summarize my thesis providing some conclusions, including answers to initial research questions and issues to be further analyzed in future research.

Methodology

To accomplish the overall objective of this research, I have examined numerous academic articles, books, reports, governmental and media releases, based on a keyword search. Focusing merely on the Western digital databases, I reviewed journals from disciplines such as law, international relations, international security, defense, and IT. Prioritization was given to sources coming from well respected organizations or authors that are specialized in specific issues, and thus they are truly aware of these phenomena. Finally, for establishing terminology, I used solid sources that are universally accepted in the international community, while for reporting incidents and critically analyzing issues, I prefered more recently published sources.

The main documents that I based my research on were the articles: "Cyber Warfare: Issues and Challenges" by Michael Robinson et al., "Proxies and Cyberspace" by Tim Maurer, and "Interventions in Cyberspace: Status and Trends" by Jawwad Shamsi et al.
I also gained a lot of information from the books: "Cyber Power" by Joseph Nye, and "Cyber Mercenaries: The State, Hackers, and Power" by Tim Maurer.

Last but not least, several tables and data were taken from the "National Cyber Power Index 2020: Methodology and Analytical Considerations" report by Julia Voo et al.

Key Concepts

Due to the high complexity of cyberspace per se, it is essential to provide some definitions regarding the related aspects. The research community has already defined the most relevant terms, which in my opinion are the following: Information Warfare, Cyberspace, Cyber Warfare, Cyber War, Cybercrime and Proxy/Cyber Proxy. Although it is challenging to maintain a clear point of view, as most of the time these terms are characterized by vagueness and ambiguity, it is crucial to comprehend and better understand them in order to further proceed into the cyber realm.

Information warfare

This term was used for the first time in 1976 by Thomas Rhona who referred to it as:

> *"The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and*

> *reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives.*"[1]

Another interesting explanation of information warfare is the one that Dorothy Denning mentioned as a competitive game between attackers, who attempt to overcome confidentiality, integrity and availability, and defenders, who seek ways to protect information and ensure the attacker's failure[2].

Martin Libicki found the aforementioned terms too broad and provided his own definition, consisted by seven forms[3], as shown below:

Form	**Description**
C2	Attacks on command centers, or commanders themselves to disrupt command effectiveness
Intelligence-based	Increasing your own situational awareness while reducing your opponent's
Electronic	Use of cryptography and degrading the physical basis for transferring information (e.g. radar jamming)
Psychological	Use of information against the human mind. Propaganda to demoralize troops or influence civilian populations.
Hacker	Exploitation of viruses, logic bombs and trojan horses to attack computer systems.
Economic information	Possessing and being in control of information leads to power
Cyber	Information terrorism, semantic attack, simula-warfare, Gibson-warfare

Table 1.1., Libicki's seven forms of information warfare

These forms reveal a significant polymorphism that includes activities from traditional hacking to propaganda and so on. It is obvious that cyberspace constitutes a part of information warfare, although it may be something more. In order to acquire a better understanding of this relationship it is necessary to proceed with more definitions.

[1] M. Libicki, *What is information warfare?*, ACT and National Defense University, 1995, pp.4.

[2] D. E. Denning, *Information Warfare and Security,* Addison Wesley Professional, 1998.

[3] M. Libicki, *What is information warfare?*, ACT and National Defense University, 1995, pp. x.

The fundamental characteristic of information warfare is its asymmetric ability to convert the enemy's perceived strength into a weakness. The great powers of the 21th century see information warfare as a measure to strike with almost no risk of total engagement. The principle of the term "asymmetric" can be linked to the Japanese martial art of jujutsu, where the goal is to utilize an adversary's strength against itself[4]. Conducting information warfare and using its tools is considered quite accessible to everyone, unlike -for instance- nuclear weapons that require both resources and capability of production and management.

China's perception regarding information warfare is that information and C2 have alternated the battlefield[5], making thus the information dominance a vital part of successful and victorious battles in the future, through the element of surprise.

Russia's perception has been demonstrated through its Military Doctrine of 2010, that underlines the information space as a crucial domain which requires protection against outside threats. Already since 2000, Russia's Doctrine mentioned the promotion of patriotic values and the protection of information against adversaries as an inextricable part of the national security goals[6]. The adequate Russian response to such threats involves actions in many sectors, such as political, economic, cultural, military and so on. For Russia, information warfare is more about influencing the public and controlling information sources . For instance, "Arab Spring" and "Color Revolutions" are considered by Russia as examples of failed information and control.

The U.S. approach is quite different from the aforementioned, as it perceives IO with a technological perspective, compared to China's/Russia's combination of both human and technological aspects. Furthermore, the U.S. -through CYBERCOM- maintains a discrete procedure on its IO campaigns[7], separating the latter into several parts, while China.Russia operates in a totally different environment, more vague regarding its parts and outcomes.

Cyberspace

The first term under examination is cyberspace. Daniel Kuehl intersected numerous definitions given by the academic community and the US DoD. The outcome of his research led him to present his own point of view:

[4] Breen M. and Geltzer J., Asymmetric Strategies as Strategies of the Strong, *The US Army War College Quarterly: Parameters*, vol. 41, no. 1, 2011.

[5] Yichang L, ed., *On High-Tech War*, Military Sciences Publishing House: Beijing), 1993, pp. 272.

[6] Doctrine of Information Security of the Russian Federation (2010).

[7] DoD, Department of Defense's Strategy for Operating in Cyberspace (2011).

> "*[Cyberspace is] A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies.*"[8]

Presenting this definition, Kuehl provides a comprehensive approach, pointing out four characteristics of cyberspace: communication between people and/or organizations, operation with electromagnetic activity, massive mobility, management and exploitation of information, and last but not least, strong interconnectivity.

The major challenge to be confronted in cyberspace is achieving control over it, given the architecture of its networks and the number of users. Current networks -compared to early ones in the 1960s- are constantly growing and provide a tremendous flow of information. It is not only the active participation of humans, but devices themselves are able to connect to the internet and contribute to this particular situation of information flow (e.g. surveillance cameras, cars, household appliances). The so-called "IoT" increases the interconnectivity exponentially.

Controlling such extended terrain is extremely difficult to achieve. The more information that can be found in networks, the greater the motive for perpetrators to attempt to manipulate them, as they can discover more vulnerabilities. Currently, no country can maintain effective control over cyberspace due to three reasons: the architecture of the networks -that is based on packet switching method with decentralized structure, where monitoring process requires too much effort-, the nature of participating actors -private companies operating as ISPs, limited state authority outside its territory, and so on-, and the lack of attribution of attacks, due to relatively easy procedure of misdirection from the part of attackers, the so-called "false flag[9]".

Cyber warfare

There are a variety of definitions concerning this particular topic. Some of them are too broad to offer a concrete understanding while others are complementary, responding and

[8] D. T. Kuehl, From Cyberspace to Cyberpower: Defining the Problem, in *Cyberpower and National Security*, Potomac Books and National Defense University, 2009, pp. 24-42.

[9] Fruhlinger J., What is a false flag? How state-based hackers cover their tracks, *CSO*, January 9, 2020.

providing answers about vital aspects of the term. Alford’s definition links the utilization of cyber warfare with the country's national agenda, a characteristic which is not always present. Particularly, Alford’s definition states that:

> “*Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system*.”[10]

The motive which drives someone to conduct cyber warfare is not necessarily national, as such operations could initiate from non-state actors with religious or political ideologies and so on. A more apt definition regarding the nature of the operator is the one supported by Cornish et al.:

> “*Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them intended target.*”[11]

Jeffrey Carr believes that cyber warfare is:

> “*...the art and science of fighting without fighting; of defeating an opponent without spilling their blood*.”[12]

Considering the possible physical consequences of a cyber attack, someone could argue with Carr’s definition, as blood can in fact be spilled, especially when the target is a critical infrastructure. This was the case of a patient who lost her life in a German hospital after a ransomware attack in 2020.[13]

The aforementioned definitions about cyber warfare are a tiny sample of the existing academic effort to establish a widely accepted term, yet some of them are either too broad to

[10] Alford L. D., Cyber warfare: A new doctrine and taxonomy, US Air Force, *Journal of Defense Software Engineering*, 2001.

[11] Cornish P., Livingstone D., Clemente D. and Yorke C., *On Cyber warfare*, Chatham House, 2010.

[12] Carr J., Inside Cyber Warfare, O’Reilly Media Inc, 2011.

[13] Tidy J., Police launch homicide inquiry after German hospital hack, *BBC News*, September 18, 2020.

be accurate or too specific to cover the whole spectrum of cyber warfare. One suggested solution regarding the methodology of definition is the actor and intent definition model.

The AID model has been used by Michael Robinson et al.[14], suggesting the division of the hostile cyber situations into subconcepts in which there is a direct link among them. To begin with, the model considers an actor launching a cyber attack in order to cause harm, whether this is economic, psychological, physical, reputational etc. Defining the intent of this attack is the next objective of the model. For instance, a crime might be held for personal gain via illegal means, or espionage may target the acquisition of political or military details anonymously.

The most accurate estimation of the situation is combining the actor with the intent. It is common to expect a specific intent when it comes to specific actors. For example, a state as an actor can be related more aptly to warfare-like intents, a terrorist group to terrorism-like intents and so on. Nevertheless, this accounts for an estimation and certainly needs further examination, as the obvious may not be the reality.

Using the same logic, the model suggests that cyber warfare is indeed the use of cyber attacks with a warfare-like intent. The figure below describes the logic behind this model (see Figure 1.1).

[14] Robinson M., Jones K. and Janicke H., *Cyber Warfare: Issues and Challenges*, Computers & Security, vol. 49, 2015, pp. 70-94.

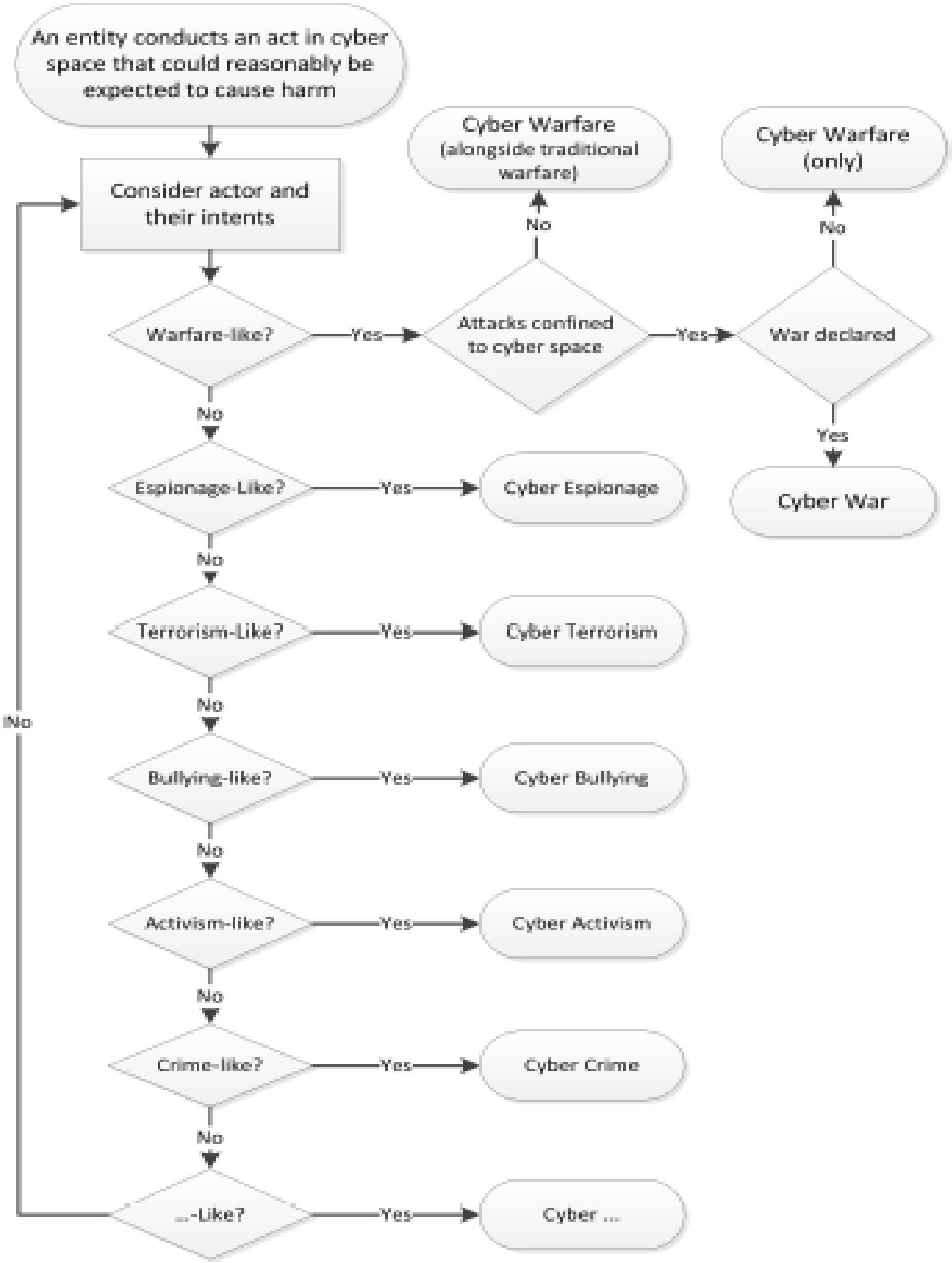


Figure 1.1., Actor and Intent Definition Model[15]

[15] Ibid, pp. 16.

Cyber War

Michael Robinson et al. and their AID model goes further and separates the term "cyber warfare" and "cyber war", where the first one could be described as an activity, and the latter as a situation, a state of being. For instance, some actors may be at war (situation), but they perform warfare (activity). The only case that these two terms are synonyms is when a war is being conducted only with cyber attacks (cyber war). Otherwise, if there are kinetic operations or air strikes, it is a war where cyber warfare takes place.

To sum up, M. Robinson et al. support that:

> "*Cyber War occurs when a nation state declares war, and where only cyber warfare is used to fight that war.*"[16]

Keeping that in mind, we could argue that one more helpful definition of cyber war that makes the approach more comprehensive is the one provided by Greathouse, stating that:

> "*Cyber War is the use of network based capabilities of a state or non-state actor to disrupt, deny, degrade, manipulate or destroy information resident in computers or networks themselves. It also can undermine the credibility of information within society through the distribution of alternative information through cyberspace that can destabilize governance and or society.*"[17]

The last part of Greathouse's definition was added due to incidents like the Arab Spring, which has demonstrated the significance of distributing alternative information that stands against the government's perspective[18].

Proxy and Cyber Proxy

The term "proxy" was defined by the Merriam-Webster dictionary as:

> "*(1) an agency, function, or office of a deputy who acts as a substitute for another, (2a): authority or power to act for another, (3) a person authorized to act for another.*"[19]

A proxy actor in the International Relations literature has been given different focus over the years, depending on the relative situation in the international system. For instance, during the Cold War, proxies were linked to one of the dominant superpowers, usually described as

[16] Ibid. pp. 14.

[17] Greathouse C., «Drinking from a Fire Hydrant: Information Overload As a Cyber Weapon» in *Cyber Weaponry: Issues and Implications of Digital Arms*, Springer, 2018, pp. 60.

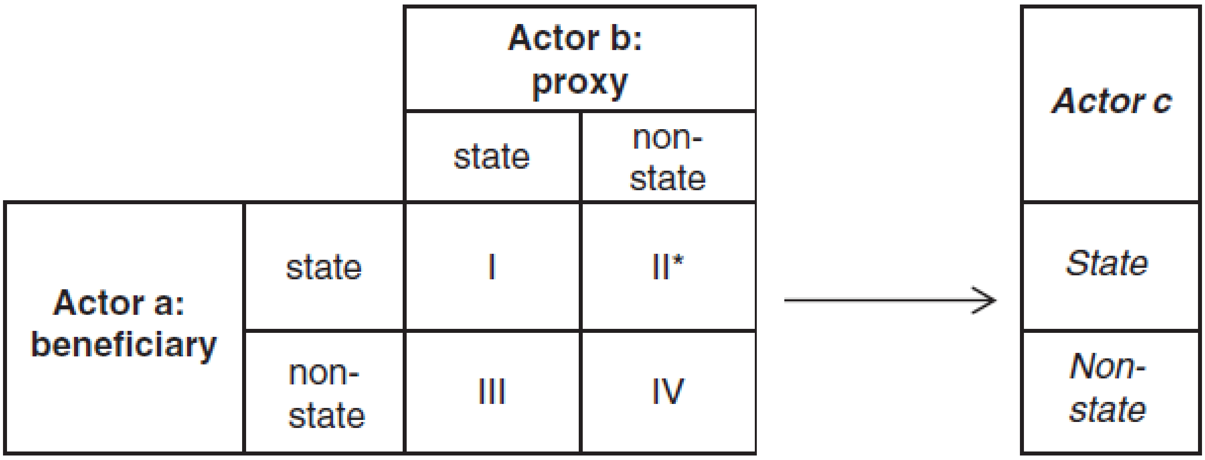
[18] Miladi N., Social Media and Social Change, *Domes: digest of Middle East Studies*, vol. 25, no.1. 2016, pp. 36-51.

[19] "Proxy", Merriam-Webster.

"satellites" or "client" states as well[20]. However, more recently non-state actors are the primary proxies, which is clear in Hughes's book, where he describes proxy as:

> "*a non-state paramilitary group receiving direct assistance from an external power*"[21]

A general perspective of a proxy is an Actor B acting for Actor A, which exists an unequal relationship between (at least) two actors, and that is why we differentiate a proxy from a partner or ally[22]. Thus, in this very relationship, (at least) an actor is the beneficiary and the other one is the proxy or satellite[23] or auxiliary[24] or surrogate[25] actor, and so on. These actors can be either state or non-state ones, yet since the post-Cold War era it is usual for the beneficiary actor to be a state and the proxy to be a non-state group.



		Actor b: proxy	
		state	non-state
Actor a: beneficiary	state	I	II*
	non-state	III	IV

Actor c
State
Non-state

Table 1.2., Beneficiary-Proxy Relationships[26]

Describing every situation on Table 1.2., every possible combination of Actors A,B, and C are presented. As we can notice, Actor A is considered the beneficiary one and Actor B the proxy. The first two scenarios (I,II) are the ones that have been observed the most, where Actor A is a state and Actor B is either a state or a non-state. During the Cold War it was more common to maintain a beneficiary-proxy relationship where both actors were states (I), nevertheless, in recent years scenario (II) is more frequent, where a state uses a non-state actor as a proxy, for

[20] Klare M., Subterranean Alliances: America's Global Proxy Network, *Journal of International Affairs*, vol. 43, no. 1, 1989, pp. 97-118.

[21] Hughes G., *My Enemy's Enemy: Proxy Warfare in International Politics*, Sussex Academic Press, 2014, pp.11.

[22] Duner B., Proxy Intervention in Civil Wars, *Journal of Peace Research*, vol.18, 1981, pp. 357.

[23] Ibid, pp. 354.

[24] Thucydides, Chapter XIII 'Seventh and Eighth Years of the War- End of Corcyrean Revolution- Peace of Gela- Capture of Nisaea', *History of the Peloponnesian War*, Penguin Books, 1974.

[25] Klare M., (n.26), pp. 97-98.

[26] Maurer T., 'Proxies' and Cyberspace, *Journal of Conflict & Security Law*, vol.21, no.3, 2016, pp. 388 (Table 1.).

instance a scholarship on private security companies provided by a country can be found into this category. In both aforementioned cases, there is a high possibility of including a third actor (Actor C), which is the beneficiary's and -consequently- the proxy's target. At most of the cases Actor C is a state, although it can be a non-state actor, and a potential intervention against it, is described as "proxy war[27]" or "proxy warfare[28]" among others. Regarding scenarios (III, IV), they account for circumstances when the beneficiary is a non-state actor influencing either a state or a non-state. These are two approaches which stand away from the state-centric one, and as examples can be given the 'weak states' or the 'mafia states', due to their incapability to control the organized crime within their sovereignty area. It is worth mentioning to quote Atanasov's words as he was describing the situation in Bulgaria:

> "*other countries have the mafia; in Bulgaria the mafia has the country*[29]"

What is remarkable about scenarios (III, IV) is that in these cases the non-state actors maintain greater and more sophisticated cyber capabilities than states themselves, and thus they can handle a country's infrastructure for their own benefit. In the last approach (IV), a potential scenario would be a hacking group (non-state actor) having a decisive impact on another group (non-state actor), or -in terms of cooperation- a company that hires an individual hacker to target the Actor C.

As a cyber proxy, it can be considered:

> "*an intermediary that conducts or directly contributes to an offensive cyber action that is enabled knowingly, whether actively or passively, by a beneficiary*[30]."

Just like proxies, cyber proxies are under the control of their beneficiaries, either through a tight leash or through indirect support and tolerance.

[27] Cragin R., Semi-Proxy Wars and U.S. Counterterrorism Strategy, *Studies in Conflict & Terrorism*, vol.38, no.5, 2015, pp. 312.

[28] Mumford A., *Proxy Warfare*, Polity, 2013, pp. 56.

[29] Naim M., Mafia States: Organized Crime Takes Office, *Foreign Affairs*, vol. 91, no. 3, 2012, pp.100.

[30] Maurer T., Cyber Proxies and Their Implications for Liberal Democracies, *The Washington Quarterly*, vol. 41, no. 2, 2018, pp.173.

CHAPTER II

EMERGING CYBER THREATS: HOW THEY AFFECT THE INTERNATIONAL & DOMESTIC SECURITY?

In this chapter I examine the challenges found in cyber warfare and cybercrime. The weaponization of cyberspace through malicious cyber activities is not a simple process to confront and usually perpetrators exploit the existing gaps in order to achieve their goals effortlessly.

The examining topics initiate with the types and roles of actors, either states or non-state individuals and groups. The significance of such a distinction among actors is crucial, in order to underline the different roles and characteristics, as well as to understand "what is 'new' in international security and how it affects the security of states". Then, presenting and analyzing cyber weapons can provide information on "what are the forms of these (cyber) threats" and "how they can be developed and proliferated". Last but not least, examining attribution issues may conclude a comprehensive estimation regarding challenges and attributes of cyber threats.

What is new in international security? How does it affect the states?

Actors in cyberspace

Cyberspace as a domain has provided wide access to internet services to individuals as interconnected actors. This characteristic directly leads to the outcome that the presence of individuals and non-state actors in general, needs to be seriously considered in the cyber realm. When it comes to warfare, it is commonly believed that state actors are the main players, however a potential cyber attack or even cyberwar could be held by non-state actors, as complementary key players to states, or as their solely independent initiative.

Strategies that follow cyber actors are mainly based on the attribute of anonymity, a fact that facilitates the emergence of numerous actors besides states.

States in Cyberspace

States in cyberspace, as in traditional domains, maintain a significant role, mainly due to their excessive resources, compared to non-state actors. Their cyber activity can be traced in three fields: law enforcement, intelligence services, and armed forces.

When it comes to domestic security, most countries prioritize actions that ensure the protection of their citizens against crime, through the implementation of rule of law. Currently, there are many states that are internet-enabled and provide their services to citizens through cyber platforms, a fact that requires an efficient application of cyber law enforcement. The uncountable possibilities that the internet offers to users has created the need to confront emerging cybercrime. In order to do so, states have to acquire technical and legal solutions, either through the use of their inherent regulatory power over their domestic market (e.g. access to encrypted data), or by gaining special software that intercepts communications, similar to malware techniques, and hence to implement skills that they are not capable of. For this specific reason, it is a common thing to call on specialized private companies for support, or to develop their own capabilities, if possible. Challenges against cybercrime often require a more radical approach by the law enforcement agencies, which means that they use similar techniques and technologies as cyber criminals, yet with different goals and high level of legitimacy.

A similar field of action for states in cyberspace is the one of the intelligence services. Specifically, the use of espionage among states is considered a traditional activity and is commonly accepted as a State practice, even though some countries have criminalized it in their domestic penal systems. Hence, intelligence agencies generally make use of all their available methods and means, in order to get to the desired information[31]. Cyberspace provides useful information through interception of data or spying methods and accounts for a prosperous environment for intelligence agencies to operate more efficiently.

The concept of cyber warfare is distinct from the ordinary malicious activities in cyberspace and it is quite important to maintain a clear perspective of what cyber warfare is referred to[32]. The armed forces of a state in traditional domains are the backbone of its power, however in cyberspace the number of troops is not that significant as the technological military capabilities. This field of action is crucial for states, as it describes the cyber warfare capabilities and the threats that can be posed by an adversary. The first case of use of cyber

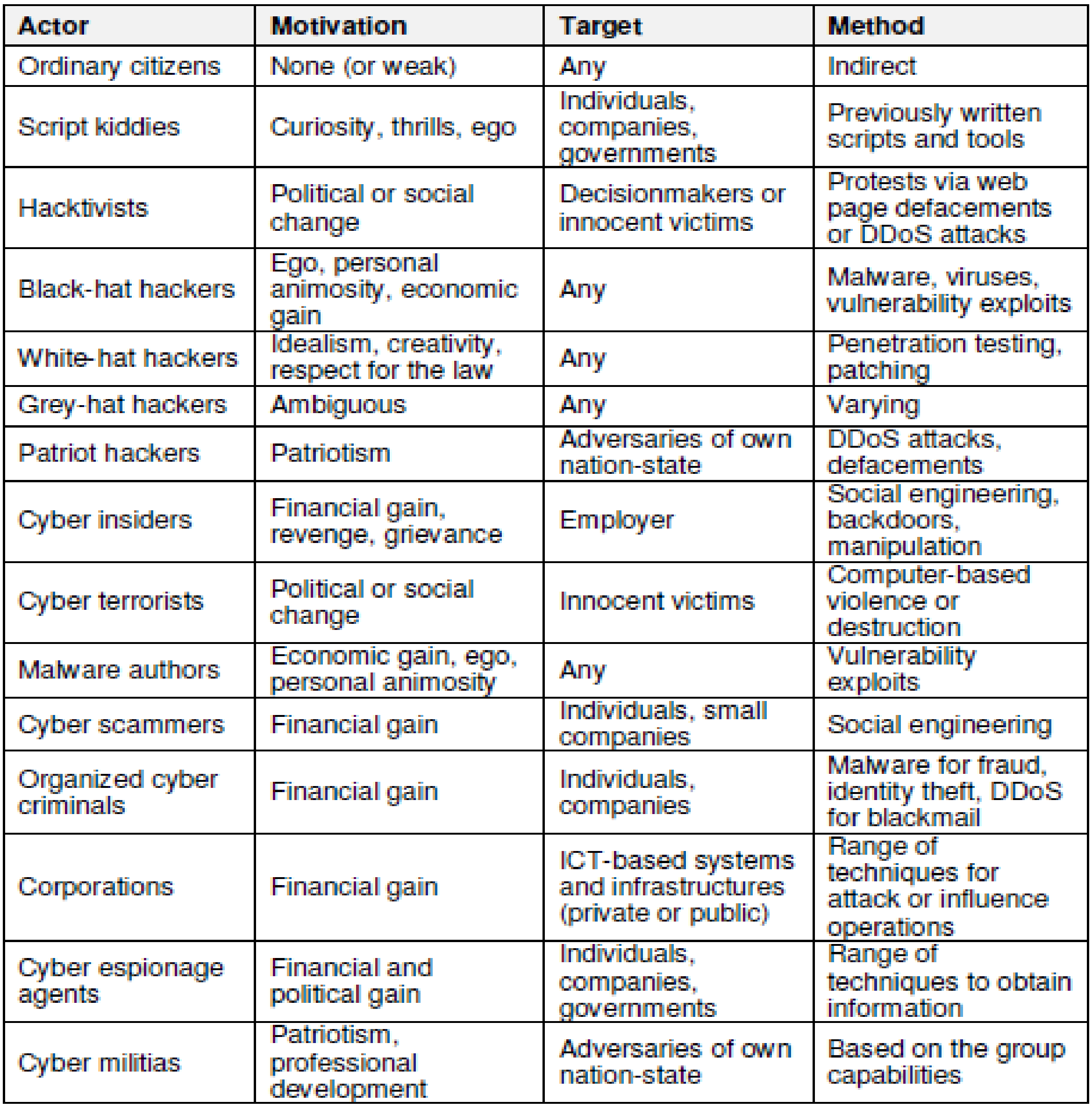
[31] Pelican L., Peacetime Cyber-Espionage: A Dangerous but Necessary Game, *CommLaw Conspectus*, vol. 20, pp. 363-471.
[32] see pp. 15, Chapter I- Cyber Warfare.

means from a state against another one was probably in 1982, when a logic bomb was supposedly placed in a gas drilling equipment causing an explosion, known as the Trans-Siberian Pipeline incident[33]. Also, in the first Iraq war. various cyber attacks were on the table as a possible addition to conventional operations by the U.S, although such attacks never took place, due to the fear of unpredictable collateral damage and side effects[34]. Hence, in 2008 it was the first known incident of both kinetic and cyber operations combined in an international conflict between Georgia and Russia[35]. Usually, the examples of Georgia and Estonia are being used to describe the aspect of cyber warfare among states, and to promote cyberspace as an independent warfare domain. Overall, as the technology is constantly evolving and new methods of military capabilities emerge, it is vital for states to develop systems and capabilities in order to operate in cyberspace. However, according to scholars, the pressure of developing cyber capabilities facilitates a new arms race situation, where the competition among states will be intense[36].

Non-state actors in Cyberspace

The availability of numerous devices (e.g. computer, smartphone, smart tv, etc.) ready to be connected to the internet is an endless possibility for different non-state actors with varying motives, goals, and intentions to act and get involved in malicious attacks. This can be achieved through the creation of formal structures (e.g. cyber gangs) or via the 'lone wolf' approach of individuals. An attempt to categorize the main non-state actors was made by Sigholm J. (see Table 2.1.).

[33] Keller B., 500 on 2 Trains Reported Killed By Soviet Gas Pipeline Explosion, *New York Times*, June 5, 1989.
[34] Markoff J. and Shanker T., Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk, *New York Times*, August 1, 2009.
[35] Tikk E., Kaska K. and Vihul L., International Cyber Incidents: Legal Considerations, *CCD COE Publication*, pp. 130.
[36] Jellenc E., Explaining Politico-Strategic Cyber Security: The Feasibility of Applying Arms Race Theory, *11th European Conference on Information Warfare and Security*, 2012, pp. 151-162.



Actor	Motivation	Target	Method
Ordinary citizens	None (or weak)	Any	Indirect
Script kiddies	Curiosity, thrills, ego	Individuals, companies, governments	Previously written scripts and tools
Hacktivists	Political or social change	Decisionmakers or innocent victims	Protests via web page defacements or DDoS attacks
Black-hat hackers	Ego, personal animosity, economic gain	Any	Malware, viruses, vulnerability exploits
White-hat hackers	Idealism, creativity, respect for the law	Any	Penetration testing, patching
Grey-hat hackers	Ambiguous	Any	Varying
Patriot hackers	Patriotism	Adversaries of own nation-state	DDoS attacks, defacements
Cyber insiders	Financial gain, revenge, grievance	Employer	Social engineering, backdoors, manipulation
Cyber terrorists	Political or social change	Innocent victims	Computer-based violence or destruction
Malware authors	Economic gain, ego, personal animosity	Any	Vulnerability exploits
Cyber scammers	Financial gain	Individuals, small companies	Social engineering
Organized cyber criminals	Financial gain	Individuals, companies	Malware for fraud, identity theft, DDoS for blackmail
Corporations	Financial gain	ICT-based systems and infrastructures (private or public)	Range of techniques for attack or influence operations
Cyber espionage agents	Financial and political gain	Individuals, companies, governments	Range of techniques to obtain information
Cyber militias	Patriotism, professional development	Adversaries of own nation-state	Based on the group capabilities

Table 2.1., Main non-state actors in cyber attacks[37]

Ordinary citizens are the most common actors, as they use the Internet and online services either for lawful reasons or not. Their motives and goals are not harmful and arise from pure curiosity and their involvement in cyber attacks emerges either indirectly, as a botnet has taken control over their system, or voluntarily by allowing their resources to be used from another actor in the context of a broder cyber attack.

There are also the script kiddies, who could be described as vandals of the Internet. They have fundamental knowledge to handle programming and security technologies, however they adopt an immature behavior, defined by ego-gratification motives. They seek to

[37] Sigholm J., Non-State Actors in Cyberspace Operations, *Journal of Military Studies*, vol. 4, no. 1, 2013, pp. 11.

demonstrate their work to various IRC channels or other forums and usually they cause indiscriminate damage, with no estimation and lack of understanding. Target selection is also irrational, as they could possibly attack a government agency or a small business, with no specific criteria.

Hacktivism is an important aspect in cyber attacks as well. In a broad term, hacktivism includes legal or illegal activities in order to protest or express a certain political agenda in the cyber realm. It is a common thing to use website defacements[38], URL redirects[39], DDoS, information theft, and other cyber-sabotage activities. Hacktivists as groups can maintain loose formation where anyone at any time can join or leave, given the fact that their only bond is their political agenda.

Hackers are widely known non-state actors of cyberspace and account for individuals with a high level of computer understanding, techniques, and interaction among network, hardware and software. They are considered to be younger individuals who engage in hacking out of curiosity and personal ambition, targeting mostly noteworthy victims and leaving some proof of their actions. Depending on their motives and goals, they can be categorized as black-hat, white-hat, and grey-hat hackers (see Figure 2.1.).

The first category, consist of hackers with the most malicious intentions, as they seek to exploit computer networks and systems for their own profit, either by intervening to a computer's system and directly stealing credit card numbers, or by selling the gained information to a third party. These hackers have no interest in applying and respecting the law or the negative impact that they have on their victims.

On the contrary, white-hat hackers maintain moral standards and contemplate societal norms. Their task is to test the security of information systems -in private or public (government) sector- through validation methodologies, and provide information about existing vulnerabilities, as well as potential patches to confront them.

Last but not least, grey-hat hackers are considered to be white-hat ones who occasionally choose to act away from the law context and manage a cyber attack of their interest at their own will. Sometimes they also violate the law with the purpose of gaining knowledge regarding the system's design and security. In the past, hacking was not a criminal act, given the fact that many national penal codes did not involve it. However, in the late 90s initiated a mass process of criminalisation, as numerous Western countries implemented cybercrime

[38] Imperva, *Website Defacement Attack*.
[39] Ntchosting, *URL Redirection*.

legislation in an attempt of international harmonization, such as the Convention on Cybercrime[40], among others.

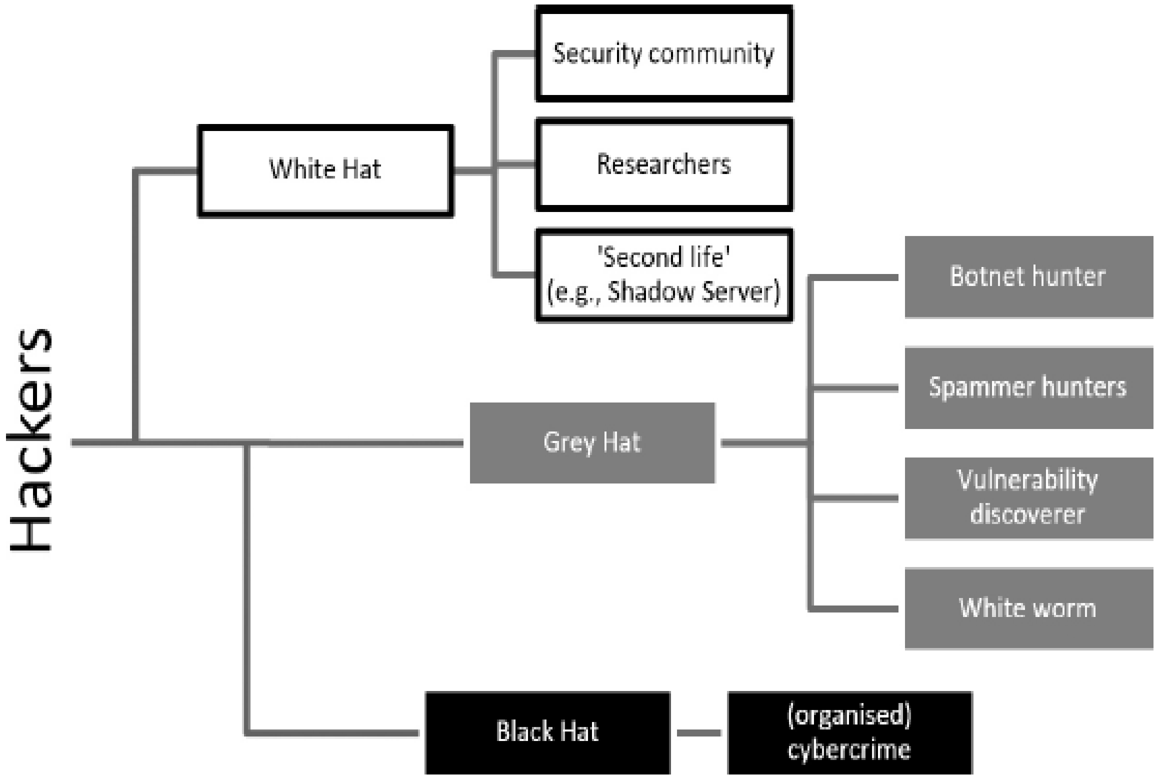


Figure 2.1., Hacker Categories and Motives[41]

Patriot hackers are those who assist their countries during a conflict or war -usually in conventional domains- via the execution of disruptive operations against the adversary. Such hackers can be widely found in China[42], where they have formed an alliance known as “Red Hacker Alliance” or the “Honker Union of China”, along with their official manifesto that signifies their mission[43]. Russian patriot hackers have significant presence as well, given the DDoS attacks in Estonia in 2007[44] and in Georgia in 2008. It is also worth mentioning that Russian patriot hackers executed numerous web defacements in Kosovo during the conflict, as well as other cyber attacks against Israel, Chechnya, Belarus, Kyrgyzstan, among others[45].

[40] Council of Europe, Convention on Cybercrime, 2001.

[41] Ziolkowski K. (ed.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, *NATO CCD COE*, 2013, pp. 4.

[42] Hvistendahl M., China’s Hacker Army, *Foreign Policy*, March 3, 2010.

[43] Amorosi D., Chinese State of Denial, *Infosecurity*, vol. 8. no. 6., 2011, pp. 4-7

[44] Denning E., Cyber Conflict as an Emergent Social Phenomenon, in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, IGI Global, 2011. pp. 178-181.

[45] Karatzogianni A., Blame It on the Russians: Tracking the Portrayal of Russian Hackers during Cyber Conflict Incidents, *Digital Icons: Studies in Russian, Eurasian and Central European New Media*, no. 4, 2010. pp. 127-150.

Cyber insiders belong to non-state actors as well. They account for individuals who have legitimate access to networks and computers, however they are willing to exploit this authority against their employer, in order to acquire financial and other benefits for their own. They can act as a 'trojan horse' providing access to perpetrators, steal and share information, classified documents, and/or sell corporate or national secrets. The identification and mitigation of cyber insiders is challenging, as the exploit is not based on an existing vulnerability in the system, but on a legitimate and undetected access within the security boundary. In order to combat such actors, governments deploy relative agencies to provide adequate protective measures, such as the U.S. DHS and its initiatives[46].

Just like terrorists in physical domains who use extreme means and violence to cause massive damage indiscriminately, cyber terrorists follow the same pattern in cyberspace by using computer and network technologies to achieve their goals. An example of cyber terrorism is the case of SEA in Syrian civil war, which used DDoS attacks and defacements against Syrian opposition and Western websites, including penetration in The Financial Times, The Telegraph, The Washington Post, and Al Arabia [47].

Malware authors are characterized by a high level of skills related to computer programming and detection evading against antivirus, anti-spyware and spam-filtering software. They could be categorized along with black-hat hackers, yet they are more specialized, given the fact that they create malware and determine its delivery methods, payloads and means of propagation[48].

Cyber scammers are not so skilled actors related to others and they seek to deceive their victims using information technology. Their methods consist of random spamming and ways that may be luring for victims to fall for the scam (phishing). For instance, such tricks may include fake lottery winning, a large inheritance, a job offering with high salary, and so on. Their motives are mostly financial, as they can exploit victims' information and get access to their credit card numbers or other fundamental information. Subsection of phishing is the spear phishing, in which scammers are more sophisticated and organized, and thus proceed to a detailed analysis of their victims' profile -usually through stolen bank statements and social media- to identify if they possess any high value items.

Organized crime is present in cyberspace, as it is in the real world, and criminal organizations are another non-state actor who are ultimately favored by the anonymous nature

[46] DHS, *Insider Threat Mitigation*,

[47] Love D., 10 Reasons to Worry about the Syrian Electronic Army, *Business Insider*, May 23, 2013.

[48] Roberts P., UK's top ecrime investigator describes a life fighting cybercrime, *Sophos Naked Security*, September 25, 2012.

of the cyber realm, along with the lack of borders. Since the end of the 20th century there were significant investments and improvements in IT security, although due to the great number of interconnected individuals without serious protection and lack or low level of ICT security from the users' point of view, along with lack of attribution and international cooperation, organized cybercrime managed to prosper. The Internet allows criminals to connect from everywhere and participate in various criminal cyber activities[49]. A fundamental advantage for these actors, which is worth mentioning, is the vagueness regarding cyber law enforcement and, in general, the legal aspect of cyber operations. Their motivation is mostly financial gain and status, and they tend to prosper in conflict areas with high unemployment and low salaries. Thus, citizens are attracted to this kind of actions as a source of money and escape from poverty[50], given the fact that these developing countries cannot efficiently confront cybercrime with sanctions. Currently, there are various major cybercrime organizations (e.g. DarkSide and REvil among others) which account for a crucial threat of international security[51].

Corporations in cyberspace can facilitate a country's ambitions by serving its purpose directly (government contract) or indirectly (autonomous actions in favor of the government)[52]. Corporations and organized crime have both financial gain and market control as motives, yet the former are considered to be more law-abiding actors due to potential economic sanctions if cyber operations are efficiently attributed.

Cyber espionage is well established as a tool of intelligence gathering. Espionage operations are illegal in many countries, and thus the issue arises when the process of intelligence gathering, which is considered legal, is held through espionage. Specifically, espionage often requires the acquisition of classified information apart from the owner's permission, and can be achieved by numerous actors, such as agents, military forces, government institutions, companies, and so on[53]. From a legal point of view, actors who perform espionage have the approval of the government, unlike cyber criminals, due to the general belief that espionage accounts for a vital tool regarding national security of the state.

[49] United Nations Office on Drugs and Crime (UNODC), The Globalization of Crime: A Transnational Organized Crime Threat Assessment, *E.10.IV.6*, 2010.

[50] Hassan A,, Funmi D. and Makinde J., Cybercrime in Nigeria: Causes, Effects and the Way Out, *APRN Journal of Science and Technology*, vol. 2., no. 7, 2012, pp. 626-631.

[51] Musotto R., O'Shea B. and Haskell-Dowland P., Holding the world to ransom: The top 5 most dangerous criminal organizations online right now, *GCN*, July 7, 2021.

[52] Drew C. and Markoff J., Contractors Vie for Plum Work, Hacking for U.S., *The New York Times*, May 30, 2009.

[53] Lachow L., "Cyber Terrorism: Menace or Myth?", in F. Kramer, S. Starr and L. Wentz (eds.), *Cyberpower and National Security*, National Defense University Press, Washington, D.C., 2009.

Cyber militias are non-state actors who voluntarily participate in cyberattacks, as they seek to achieve a political goal[54]. They operate through common communication channels (e.g. social media, forums) and conceal their true identities. Due to the nature of the cyber realm it is difficult to clearly distinguish and successfully categorize each actor according to its activity, leading to the conclusion that there are significant grey areas among them.

What are the forms of cyber threats? How can they be developed and proliferated?

Cyber Weapons

The definition of cyber weapons is quite different from the one describing traditional weapons in kinetic warfare. Unlike traditional weapons, which are manufactured to kill, injure, disable people or cause damage to property, cyber weapons mainly tend to cause an indirect kinetic effect, which is possible to result in death, injury or damage. Hence, a cyber weapon's goal may be information collection or a way to facilitate a future attack. The specific definition requires both capability and intent examination in order to overcome the difficulty of its dual use nature (tool and code)[55]. Cyber weapons can vary regarding the severity and sophistication, targeting different goals such as espionage, theft, destruction, and being used solely as malware or as a weapon. Based on that, a cyber tool becomes a cyber weapon when it has both the capability, and the operator's intent to cause harm.

Another approach of cyber weapons can be seen in Sommer and Brown's work, where they argue with the term "weapon" in the spectrum of cyberspace and underline the distinction between cyber offensive military act and weapon. The latter, they suggest, is a directed force, it can be controlled, it is possible to predict its impact and it will not cause friendly fire or collateral damage so easily[56]. This is not the case for cyber offensive acts though.

Cyber weapons consist of two parts, a vulnerability and an exploit. Regarding vulnerability, it is a weakness that can be found in the information system, security processes, internal controls or implementation that could lead to exploitation by a perpetrator. The most relevant example of such a procedure is the 0-day vulnerability[57], which is unknown to the

[54] Ottis R., Proactive Defense Tactics Against On-Line Cyber Militia, in *Proceedings of 9th ECTW*, Thessaloniki, Greece, 2010.

[55] Arimatsu L, A treaty for governing cyber-weapons: Potential benefits and practical limitations, *4th International Conference on Cyber Conflict*, 2012, pp. 1-19.

[56] Sommer P. and Brown I., *OECD Study-Reducing Systemic Cybersecurity Risk*, pp. 28, 2011.

[57] See supra note 22, pp. 20

operator of the system but it can be fixed as soon as it is discovered. For instance, Microsoft once a month releases security patches to address the existing security gaps in its Windows OS[58]. In order to deal with vulnerabilities as an operator, it is vital to increase the capability of immediate discovery, and hence the perpetrator will have a shorter window of exploitation. Usually, vulnerabilities can be traced through self-initiated examinations, control notices driven by government or cybersecurity organizations (e.g. US-CERT, Symantec), and in response to an exploit. Thus, it is obvious that they are characterized by both expendability and obsolescence, as they are fixed once they are discovered[59].

As far as the exploits are concerned, they are operations or intelligence collection procedures that gather data from enemy's information systems or networks[60], and account for code, worm, virus or trojan horse that intrude through a vulnerability to cause damage and gather information. The most popular exploitation so far is the Stuxnet worm, which was used in the Iranian nuclear material enrichment facility and resulted in uncontrollability of the centrifuges[61]. Exploits are also obsolete and expendable for the same reasons as vulnerabilities -once they are discovered, they become ineffective-. They can be ineffective if they are too sophisticated as well. It is worth to mention the example of Stuxnet, where the OS managed to create a patch that efficiently confronted the code, and -using the same example- there were specific conditions for the Stuxnet to run (e.g. certain version of the OS, the logic controller, and the type of centrifuge), rendered the exploitation too sophisticated, and hence at any possible change of the facts, it would become useless. However, this very approach of targeting certain systems and characteristics may have limited impact on other computers and mitigate the potential collateral damage.

An exploit is highly possible to lead to some problems related to its nature. Specifically, when it is created it cannot be deleted or destroyed, and thus when it is discovered it can be either examined and modified for future use -even against its creator-, or be compared to other ones and expose a possible connection with more covert operations, by unveiling similarities of the modus operandi of an organization. In order to have a better understanding, I present a possible scenario where the DoD cooperates with the IC, and the former creates a cyber weapon which is used to provide data for the latter. In case where the exploit is discovered and the vulnerability is fixed, the IC's operation would become ineffective and possibly this exploit would have similarities to other IC's operations,

[58] Microsoft Security Tech Center, *Microsoft Security Bulletins*, 2017.

[59] Bartos C., Cyber Weapons are not created equal, *Proceeding*, vol. 142, no. 6, 2016.

[60] CNSS 4009, *Glossary,* pp. 25.

[61] Zetter K., An Unprecedented look at Stuxnet, the world's first digital weapon, *Wired*, November 3, 2014.

consequently exposing them to the international community by connecting them to the exploit.

The arising challenges due to cyber weapons are numerous and related to their nature. Specifically, cyber weapons may increase collateral damage[62], given that in the cyber domain the distinction between civilians and military targets is much more vague, compared to the kinetic domain. Additionally, cyberspace often uses civilian infrastructure to facilitate its operations, as a country's primary connectivity providers are based on civilian organizations. Furthermore, in cyberspace there is the element of uncontrollability, due to the nature of malware and its modus operandi on spreading automatically, even beyond its initial target.

The element of unpredictability accounts for a challenge too. Not only cyber weapons as a hardware or software per se, but the impact that they cause as well. Just by altering a firewall rule can result in an unpredictable outcome that most of the time is uncontrollable, a characteristic similar to the first challenge regarding collateral damage.

Last but not least, cyber weapons can be challenging due to the difficulty of damage assessment. All three major challenges are interconnected, as one leads to another. In this situation, the impact of a cyber weapon is extremely difficult to be noticed, unlike the damage of a traditional weapon, where there are immediate kinetic effects to be reviewed. For instance, the operation of an autonomous malware will not present an immediate impact on the system and the overall estimation of spreading will be challenging to measure. Thus, the damage assessment may be misleading, since the real effects can be subtle and spread throughout numerous systems in order to be hidden.

Given all the aforementioned attributes and challenges of cyber weapons, combined with the nature of cyberspace and limited or no advanced warning, it is obvious that defending such weapons is an extremely difficult process and almost impossible to achieve. The icing on the cake is the speed of cyber weapons' deployment which emerges faster than any other weaponry so far and renders the cyber arms control even more challenging.

Development and Proliferation

According to J. Silomon, there are three interlinked groups of factors that promote cyber weapons' development and proliferation, namely motivation, capability, and restraint. The significance and the impact of these sub-sets may vary depending on the nature of the actor and its aims. For instance, state actors possibly have different intentions, such as the

[62] Rowe N, The ethics of cyberweapons in warfare, *International Journal of Cyber Ethics*, Vol.1, No.1, 2010, pp.20-31.

creation of a Stuxnet-like weapon, from non-state actors that may be pursuing a medium or a low level interference[63].

Regarding motivation, it is the initiator factor to begin with, as with no motivation it is meaningless to further examine the capabilities, but the lack of motivation indeed can facilitate the restraint of an actor. In order for motivation to emerge, it is essential to exist other interlinked and competing factors that consequently result in motivation as an outcome. The main five factors are the following: scientific advancement, economic advancement, historic, religious, and political factors (see Figure 2.2.).

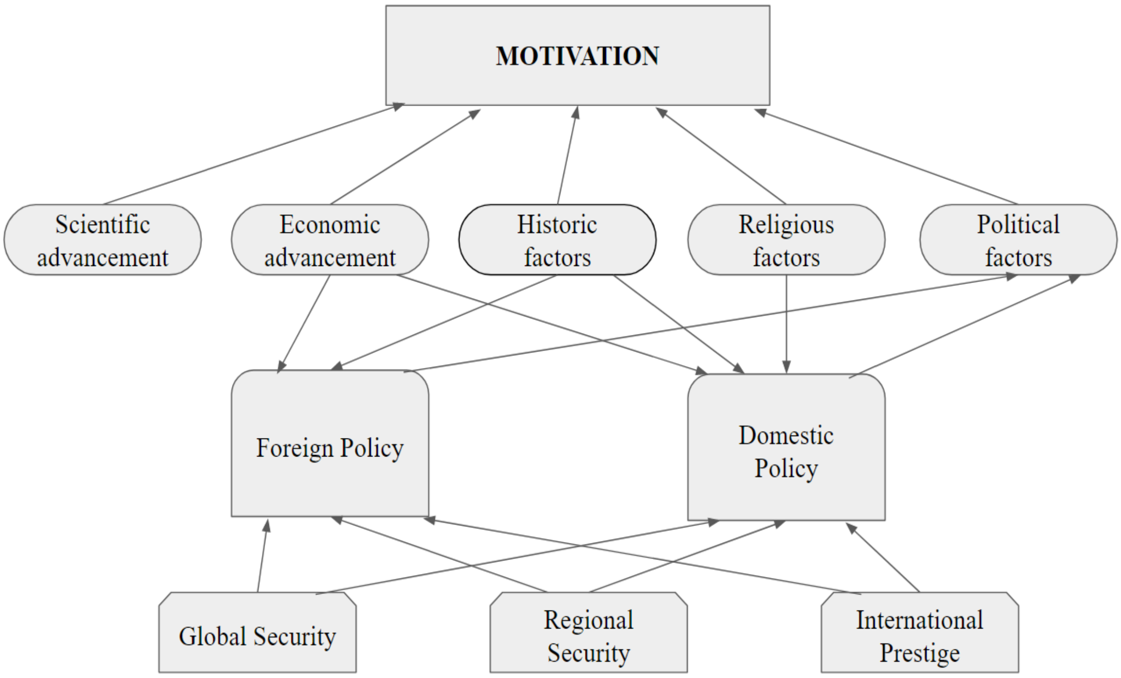


Figure 2.2., Motivation and its factors[64]

Scientific advancement is crucial for the implementation of sophisticated software usages as a weapon. Modern society provides numerous opportunities to new technologies, which further facilitate the motivation of development. For example, existing dual-use and civil applications that are promoted by state actors due to fear of being 'left behind', account for motivation caused by scientific advancement.

Similarly, economic advancement is a factor of motivation, as the arms industry is an incentive for a state actor by ensuring trade agreements with other countries and producing weapons for self-use (e.g. armed forces). Thus, a stable and safe technological environment

[63] Silomon J., Software as a Weapon: Factors Contributing to the Development and Proliferation, *Journal of Information Warfare*, vol. 17, no. 3, 2018, pp.112.

[64] Ibid, pp. 112.

results in financial benefits, affecting the foreign and domestic policy as well. Concerning unstable states, criminal organizations, terrorist groups, or individuals, they may have the intention to use malware in order to acquire financial gain, or get involved in grey and black market by trading botnets and 0-days exploits.

As far as the historic factors are concerned, it is a limited aspect of motivation's sub-set and it refers to history of a country (decisions and/or culture) as potential motive to develop or proliferate weapons. Although it may have decent applicability to conventional and nuclear weapons, it is arguable if the same goes on to the cyber domain.

About religious factors, they are part of the domestic policy and seem insignificant for most state actors, although they can be important for non-state actors. Some individuals support that religious factors can also have an impact to foreign policy, especially among non-state actors, given the changing distribution of power and actors, along with the unique asymmetric nature of cyberspace.

Last but not least, political factors are influenced by public opinion and national prestige that account for domestic policy. Non-state actors maintain a political agenda as well that serves their interests and often intend to actively participate in the regional or global arena. International prestige differs from actor to actor, as state actors seek to hide their capabilities regarding cyber weapons, in order to be able to deny any attribution in future attacks. On the contrary, non-state actors try to expose their successful exploits due to expected outcome, which is beneficial to their status and makes them a respected power.

Regarding capabilities, they are also a significant aspect of development and proliferation, as the lack of them means that the actors have to buy or steal cyber weapons. Just like motivation, capabilities are determined by five main factors: economic, tactical, research, technical, and reconnaissance (see Figure 2.2.1.).

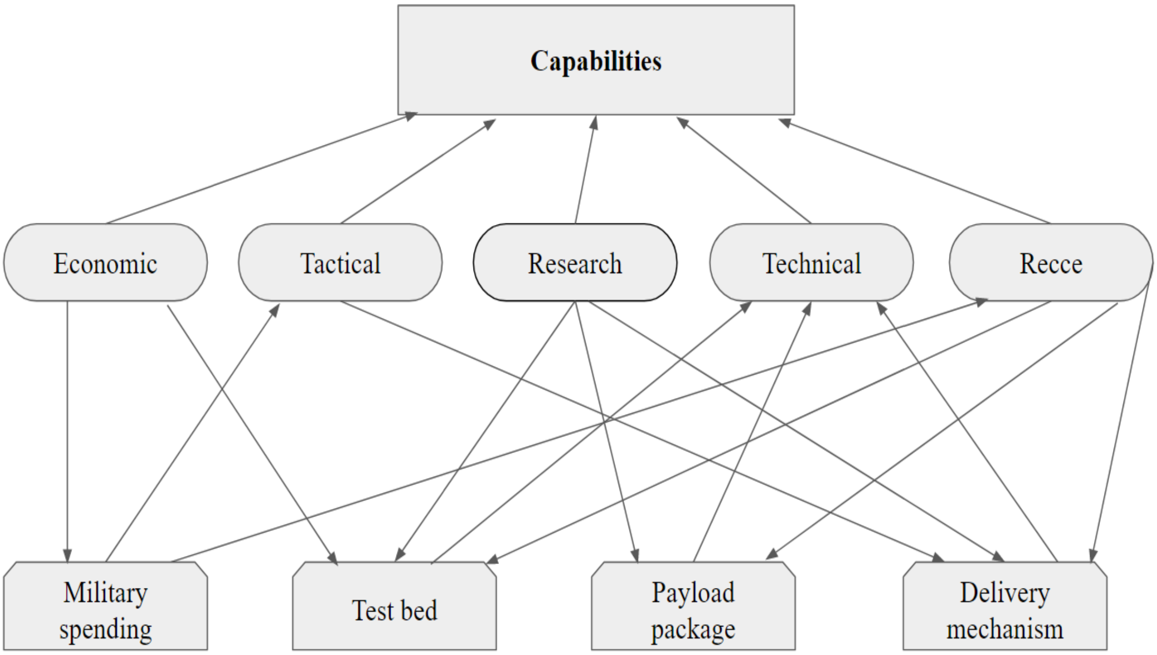


Figure 2.2.1., Capabilities and their factors[65]

A characteristic of cyber weapons, as I have mentioned before, is the low-cost production, compared to traditional conventional weapons. Nevertheless, a major downside is their single use and limited lifetime, along with their attribute to target certain systems only -if they are highly specialized-. Given that, it is obvious that cyber weapons cannot be produced massively at a large scale. Besides that, it is possible to be reused more than once, if the exploit will not be detected and the vulnerability will not be fixed. However, it is essential for an actor to have economic capabilities, due to the fact that the implementation of such weapons needs constant investment in R&D, information gathering, solid infrastructure, several tests, and a great amount of human resources among others. Also, economic capabilities affect the military spending of actors, however this is not necessarily true in every case. As technology evolves, the cost of supporting capabilities becomes more sustainable, especially when it comes to actors that are not keen on avoiding collateral damage and choose cheaper options such as hiring botnets or hackers[66]; Thus they are even less confined financially.

Tactical capabilities are all these elements that determine how the strategic goals will

[65] Ibid, pp. 114.

[66] Makrushin D., The cost of launching a DDoS attack, *SecureList*, March 23, 2017,
Putman C, Abhishta A. and Nieuwenhuis D., Business Model of a Botnet, *Proceedings of the 26th Euromicro international conference on Parallel, Distributed and Network-based Processing*, pp. 3.

be conducted. In the case of cyber weapons, these capabilities include -for example- the placement of USB sticks to server-target or the management of a certain attack in general. These capabilities directly influence the delivery mechanism, due to the need of physical access to remote locations, and at the same time they are restricted by the actor's military spending. State actors need to maintain a coherent framework that supports such operations, while non-state actors can follow a more 'fluid' approach, although they may lack significant resources and infrastructure, in order to train their personnel.

Every aspect of research -academic, industrial, governmental, etc.- is crucial to evolve capabilities by detecting vulnerabilities (defense) or exploits (offense) and improving technical aspects, such as test-bed, payload package, and delivery mechanism.

Technical capabilities include fundamental expertise to deliver attacks and are highly dependent on the test-bed, payload package, and delivery mechanism. Besides that, they also consider ways to reduce collateral damage and errors, especially state actors who are more responsible and obedient to international norms than non-state actors.

Reconnaissance (recce) accounts for the information gathering regarding adversary's hardware and software systems, location, and human elements. From a financial point of view, it is mitigated by military and intelligence services assets (state actors) or depends on purchase or theft of data for those actors lacking resources (non-state actors). Although this is a common procedure in conventional domain, in cyberspace the outsourcing option is more luring for most actors, due to its increased anonymity and deniability.

As far as restraints are concerned, they could be presented as the contrary of motivation. They are reasons not to develop and proliferate cyber weapons and can be formed by potential collateral damage, domestic safeguards, fear of retaliation, and international agreements (see Figure 2.2.2.).

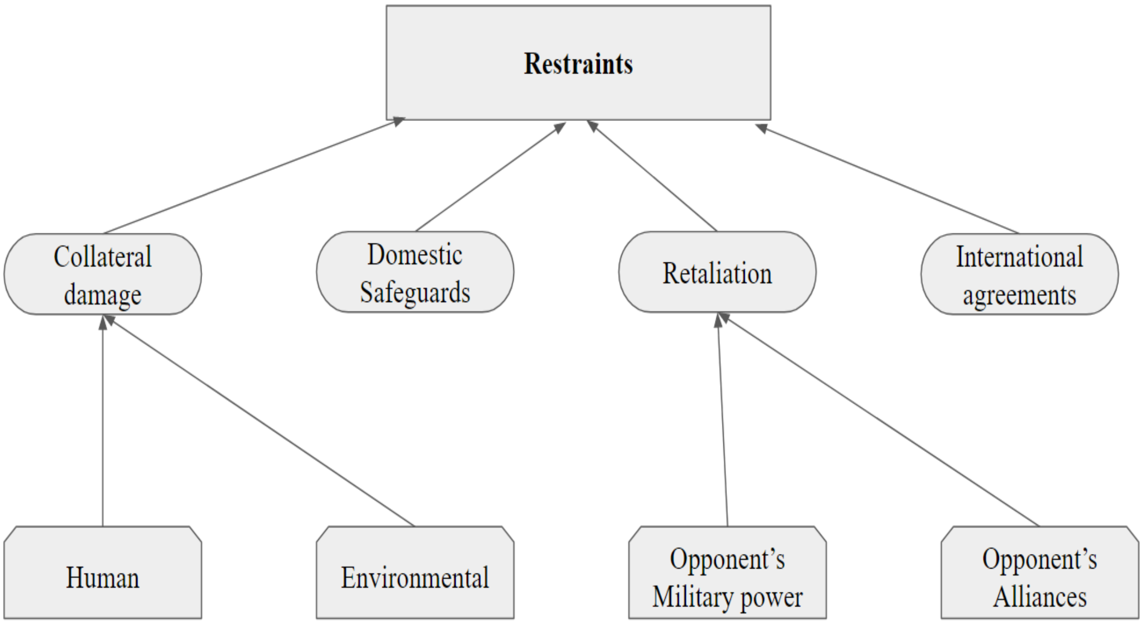


Figure 2.2.2., Restraints and their factors

Collateral damage includes both human and environmental unintended consequences as a result of an attack. When it comes to cyberspace, cyber weapons so far seem to result in less collateral damage compared to other weapons, yet this situation may change in the future.

Concerning state actors, it is possible that the development of weapons to confront domestic safeguards, especially when the country accounts for a democracy. Cyber weapons however, still do not face such issues, given the fact that they are an efficient alternative choice to NBC or conventional weapons.

Although every arising technology is a temptation for actors to acquire it, it is also a threat to the existing balance of power. Some actors envisage expected benefits and potential bargaining lead through the acquisition of weapons, however others consider the downsides. The fear of retaliation is also a factor that constrains actors to develop weapons. This fear emerges mainly from the adversary's military power and its alliances, but in cyberspace, due to problems of attribution and the lack of international agreements, the fear of retaliation is currently limited.

Attribution issues

The term 'attribution' is all about "*determining the location or the identity of an attacker or an attacker's intermediary*"[67]. Regarding attribution, there are two broad concepts in the research community, arguing on the importance of attribution per se in cyber warfare. Specifically, some researchers support the idea that attribution in cyberspace in general is an essential factor that determines the overall process of offensive techniques and cyber warfare. Hence for them, cyber operations, in order to be functional, require a source of attack which can be attributed with high confidence[68]. They also underline that without attribution, the procedure of cyber warfare is highly problematic.[69]

On the other hand, there are the rest of the researchers who believe that politics, due to their dynamic nature, can initiate retaliatory response procedures even with a reasonable suspicion of responsibility[70].

Unlike cyberwarfare, where there are still arguments on whether attribution is vital or not, attribution regarding cybercrimes is essential in order to pursue a criminal prosecution or a civil lawsuit against crime. Although anonymity can be beneficial in some cases like freedom of speech, political commentary, asking personal matters, purchasing products without revealing personal choices and so on, it is also a restraining factor that provides cybercriminals the necessary cover, either by using a fake identity, stealing or protecting identity[71]. For instance, it is relatively easy to create several fake accounts in social media, as Facebook reported in 2012 the existence of 83 million fake users on its platform[72]. Besides fake accounts, there are also various methods to hide an identity through fake email addresses, spoofed IPs, DNSflux and proxy servers that provide anonymity[73] and they pose even greater challenges in the process of attribution.

[67] Wheeler D. and Larsen G., *Techniques for cyber attack attribution*, Institute for Defense Analysis (IDA), 2003, pp. 1.

[68] Ibid, pp. 2.

[69] Friesen T., Resolving tomorrow's conflicts today: How new developments within the U.N. Security Council can be used to combat cyberwarfare, in *Naval Law Review*, Vol. 58, U.S. Navy Judge Advocate General's Corps, 2009, pp. 89-98.

[70] Hare F., The significance of attribution to cyberspace coercion: A political perspective, *4th International Conference on Cyber Conflict*, 2012, pp. 1-15.

[71] Armstrong H. and Forde P., Internet Anonymity Practices in Computer Crime, *Information Management and Computer Security*, vol.11, no.5, 2003, pp. 209-215.
Goel S., Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race, *Partnership for Peace Consortium of Defense Academies and Security Studies Institutes*, vol.19, no.1, 2020, pp. 87-95.

[72] Kelly H., 83 million Facebook accounts are fakes and dupes, *CNN*, 2012.

[73] Stone-Gross B. et al., Your botnet is my botnet: analysis of a botnet takeover, in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 635-647.

Practically, the procedure of attribution can be demonstrated on a three level construction that involves the necessary steps of an attack identification (see Figure 2.3.). Attribution can also be further categorized in technical one, where it aims to comprehend the host responsible for initiating an attack, and human one, where attempts are being made to identify the actual responsible individual for the attack.

According to Figure 2.3., it is absolutely indispensable to firstly identify Level 1 of the 'pyramid', which accounts for the technical aspect of the process. At this part, mechanism is the cyberweapon[74] and the goal is to distinguish which type has been used specifically. Then, Level 2 remains in technical perspective, although it contains characteristics from the human attribution, and targets to locate the country or city of the criminal. Lastly, Level 3, which is the most challenging to identify, is referred to the criminal him/herself and is linked only with human attribution.

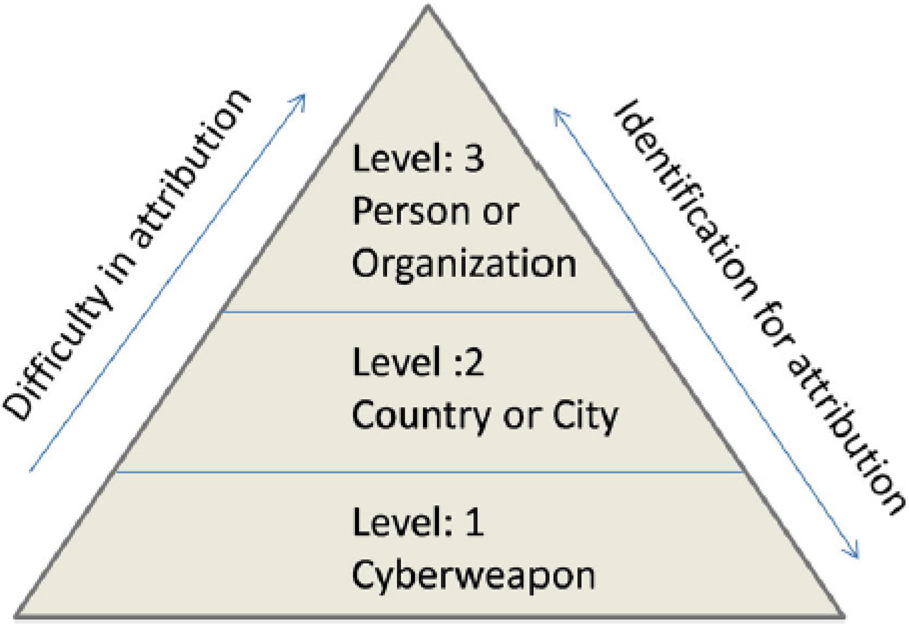


Figure 2.3., Levels of attribution[75]

Attribution techniques are continuously being improved, nevertheless they still need further research and advancement. In order to achieve a successful attribution process it is essential to reach at Level 3, something that cannot be achieved all the time. At the lowest

[74] for definition and characteristics see "Cyber Weapons", pp. 32.
[75] Shamsi J. et al., Attribution in cyberspace: techniques and legal implication, *Security and Communication Networks*, 2016, Figure 3. Levels of attribution.

level of the construction is only demanded analysis, yet as the level rises, so does the difficulty of identification through the existence of firm evidence.

As it was mentioned before, cyberspace itself accounts for a domain which by default is characterized by anonymity. Monitoring this complex sector is possible at some point, but emerging privacy issues and human rights violations render such endeavor as prohibitive.

In order for attribution to be applied and active, it is necessary to exist prepositioning of trust[76], a fact that is quite challenging to achieve in international relations due to competition among countries and companies, differing languages, laws, commercial rivalry and so on. Thus, even though network administrators have to cooperate in a trustful environment and develop a CBM regime in order to track the source of an attack, this scenario faces numerous obstacles that eventually sabotage the process. Nevertheless, a possible solution of such an issue can be resolved through the adoption of industry standards, where there will be a level of attribution, legally agreed by the actors, acting like a set of tools that preposition trust by default. Yet again, those standards may not be enough to deal with attribution challenges overall, because technical attribution has to be translated into human one[77]. Just the fact that, from a technical perspective, it is possible to find the responsible IP address does not necessarily mean that the perpetrator was found as well. Another step is needed to actually identify the person responsible for the cyber operation.

How states respond to cyber threats?

Cyber arms control

The endeavor of arms control accounts for a political reaction against the dynamics of armaments in the international system. In fact, Den Dekker explains it as:

> "*unilateral measures, bilateral and multilateral agreements as well as informal regimes...between States to limit or reduce certain categories of weapons or military operation in order to achieve stable military balances and thus diminish tensions and the possibility of large-scale armed conflicts*[78]".

[76] Wheeler D. and Larsen G., *Techniques for cyber attack attribution*, Institute for Defense Analysis (IDA), 2003, pp. 43-44.

[77] Boebert W. E., A survey of challenges in attribution, in Proceedings of a Workshop on 'Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, 2010.

[78] Den Dekker G., The Effectiveness of International Supervision in Arms Control Law, *Journal of Conflict and Security Law*, vol. 9, no. 3, 2004, pp. 316.

These agreements take place mostly through legally binding treaties, in order to control some aspects of military capabilities, not by completely disarming the participating countries, but by planning and monitoring them. Hence, the main goal of such treaties is to prevent and reduce the possibility of future wars, to limit the outcome of armed conflicts and to reduce military costs. To support this multilateral goal, agreements usually seek to discourage preventive or preemptive strikes and reduce weapons that can be used on a large scale or can result in massive destruction.

Moreover, the aforementioned agreements take into consideration several principles and measures, such as transparency regarding military capabilities, effective communication among treaty-parties through CBMs, prohibition of proliferation of related weapons and/or technologies, measures of verification to further enhance the agreed compliance, and sharing information procedures. Of course, these principles vary depending on the nature of agreement and the level of commitment that states are willing to achieve.

Due to overall mistrust or existing uncertainties among states, usually accompanied with ideological differences and limited official communication, each one expects the worst case scenario and gets prepared for that, boosting the process of cyber arms race and resulting in unstable circumstances. To deal with these uncertainties, as I mentioned before, the international political community proceeded to the establishment of CBMs, firstly introduced during the Cold War from CSCE, in order to develop active channels of communication and further fortify stability, through understanding of the opponent's security aims and fears[79]. The initiative of CBMs can facilitate the convergence of the ideological gaps, starting from a common threat such as technical accidents and possible civil society damage, and reach the acceptance of reducing or abolishing specific weaponry. In practice, they can be placed in a spectrum of supervising methods, such as aerial imaging, seismic sensors or measuring facilities, and exchanging data regarding stockpiles.

However, cyberspace is a sphere with unique characteristics that maintain inherent challenges even in developing cyber arms control treaties. From a practical point of view, following the existing prototypes is not an effective way to achieve a successful cyber treaty, as there are challenges regarding the duality of use, the obstacles of measuring cyber weapons quantitatively and so on. There is also a different perception among states considering the range of cyberspace and what accounts for state sovereignty. For instance, the EU and the US

[79] CSCE, *Document of the Stockholm Conference on Confidence-and Security-Building Measures and Disarmament in Europe Convened in Accordance with the Relevant Provisions of the Concluding Document of the Madrid Meeting of the Conference on Security and Co-Operation in Europe*. 1986.

underline the aspect of IT infrastructure, human rights and the freedom of speech in cyberspace, while countries like Russia and China focus on the state's right to regulate the distribution of information, including censorship.

Indeed, in such a domain, where there are no physical borders to specify the state's sovereignty, the issue becomes even more complex. Another challenge in cyber arms control is the lack of officially recognised classification of cyber weapons, or cyber tools in general. This very issue leads to intensification of cyber armament due to unpredictability that sabotages the stable balance of military cyber power. Thus, it is vital for states to understand and find a common ground on what and how they try to control exactly. The spectrum of cyberspace is so wide that eventually leads to a dead-end, if we attempt to regulate it all in once. It is more wise to prioritize what can be regulated and what will have a beneficial impact for the goal of cyber arms race, instead of proceeding with a generic cyber weapons ban[80]. For this purpose, a distinction between low-level activities -like cybercrime and hacktivism- and operations that cause damage and result in high impact, should be established, with only the latter to be involved in arms control treaties. A further distinction should be among a narrow conception that emphasizes solely to CNAs, and a broader one that involves a variety of actors and information regarding the digital environment. Once again, a more narrow perspective may be more useful and easier to handle in a cyber arms control treaty. A final distinction should be between protecting critical systems and infrastructure, and preventing malicious activities, where the former accounts for a specific, well-defined goal to target, rather than stopping every possible malicious initiative.

Succeeding in arms control agreements in cyberspace requires a combination of formal and informal mechanisms, in order to deal with the variety of issues and problems found in the cyber realm. Regarding formal mechanisms, they refer to existing legally binding bilateral or multilateral agreements, or even unilateral public statements, governmental doctrines and capabilities. On the other hand, informal mechanisms are less tangible, nevertheless they can equally contribute to managing other kinds of problems in cyberspace. They account for the aforementioned CBMs and communication channels.

To sum up, cyber arms control should be based on common definitions among state-parties, they will be different from the traditional ones that we have seen during the Cold War, and they should not cover the whole range of cyber realm, due to difficulties that broad perspective brings on the table. Moreover, a combination of both formal and informal

[80] Khalip A., UN chief urges global rules for cyber warfare, *Reuters*, February 19, 2018.

initiatives would be more effective, along with innovative ideas from the part of analysts, policymakers and scholars, since the nature of cyberspace is extremely complex[81].

Cyber Deterrence

As in traditional deterrence, in cyber deterrence the ultimate goal is to discourage an aggressor from proceeding to an attack. Following the same logic with traditional one, cyber deterrence can be described as the capability in cyberspace to ensure that the adversaries are convinced that they will receive a cyber attack as a response, if they launch one in the first place[82]. According to Henry Kissinger, the equation of deterrence can be described as following:

$$D = C*R*B$$

The components that result in deterrence (D) are the capability (C) -the technical ability to act, for instance weapons, retaliatory systems etc.- multiplied by the resolve (R) -accounts for the willingness of an actor to retaliate and implement the threat- and the belief (B) -enemy's persuasion that the threat of retaliation is credible and the technical ability is adequate to provoke harm-[83].

Besides the similar purpose and invariants, such as the conviction that the expected costs will outweigh the benefits, nuclear and traditional deterrence differ a lot from the cyber one, as the former may have been proven significant in maintaining de-escalated tension during the cold war, nevertheless the cyber deterrence faces a number of challenges, as cyber attacks are generally characterized as low-cost, low-consequence, and non-attributable.

First of all, the issue of attribution in cyberspace sabotages the deterrence itself, due to the fact that the attacker may believe that he/she will not be traced, and thus he/she will not receive the retaliation response. Another challenge is the vagueness regarding the risk assessment. The attacker is highly possible to underestimate the adversary's capabilities to retaliate, or overestimate his/her own security systems and the ability to defend. Again, if the risk cannot be recognised properly, cyber deterrence fails.

Furthermore, the tools that provide deterrence are crucial for the credibility of the effect per se. Specifically, kinetic weapons maintain a repeatability, as they ensure deterrence for every potential attack (e.g. missile strikes). On the contrary, cyber weapons once they are used become obsolete, as the adversary can easily deal with the vulnerability. This very

[81] Futter A., What does cyber arms control look like? Four principles for managing cyber risk, *European Leadership Network*, 2020, pp. 8-9.

[82] Libicki M., *Cyberdeterrence and Cyberwar*, RAND Corporation, 2009. pp. 47.

[83] Kissinger H., The necessity for choice: Prospects of American foreign policy, Harper Collins, 1961.

characteristic of cyber weapons discourages a long term cyber deterrence. Moreover, due to the nature of cyberspace and the lack of unanimously established laws, it is unclear which actions cross the line and are capable of legitimizing a retaliatory response. One more challenge is that, unlike traditional deterrence, in cyber one some countries may be less vulnerable to retaliatory response, as they have underdeveloped cyber infrastructure and thus the risk for them is minimal, rendering the effect of cyber deterrence practically useless. This is the case of North Korea. Finally, it is difficult -at the first place- to find out who conducted a cyber attack (identity) and, even worse, if it is a non-state actor, it is challenging to interfere into the sovereignty of another state to deal with the situation[84].

In order to confront the existing challenges, it is essential to apply a toolkit that limits the benefits of a cyber attack and increases the risks of initiating one. Hence, an extremely vital step to take is the enhancement of the cyber security posture of critical systems and infrastructure. States, indeed, need to invest in their network architectures, as the last could be a deterrent factor itself, limiting the impact of a successful attack and increasing the cost to launch it. By accomplishing the architectures defensible, states deprive perpetrators' accessibility and mitigating the undesired outcome. Such initiative accounts for the NIST Cybersecurity Framework by supporting the critical infrastructure[85]. Solely protection of critical infrastructure is a decent measure, yet it can be even more effective if educational campaigns take place as well. Through these campaigns, users can be taught how to handle and protect themselves from cyber threats, creating simultaneously a cyber-security culture for the next generation[86].

Another important aspect of improving deterrence capability for states is by rendering their systems resilient and quickly reconstructable. Besides their active defense and enhancement, they have to be able to recover fast and at low cost in case of an attack. This characteristic can be achieved through innovative technological research and development, such as microgrid technology which decentralizes electricity generation and transmission, and mitigates accompanying risks[87].

One more respectively simple and low-cost step for states is to maintain a clear perspective of the types of cyber attacks that are able to trigger a response, and what kind of activities would be included in this response. By clearer communication regarding each

[84] Sterner E., Retaliatory deterrence in cyberspace, Strategic Studies Quarterly, 2011, pp. 62-80.

[85] NIST, *Framework for improving critical infrastructure cybersecurity*, US Department of Commerce, Washington, DC, US, 2018.

[86] Denning D. and Strawser B., «Active cyber defense: Applying air defense to the cyber domain», in *Understanding cyber conflict: Fourteen analogies*, Georgetown University Press, Washington, DC, US, 2017.

[87] US Department of Energy, *The role of microgrids in helping to advance the nation's energy system*, 2017.

country's perception of threat and potential response, the risk of miscalculation and escalation could be significantly reduced. However, the declared retaliation must not deviate from the principles of deterrence, and thus it has to be credible and inside the spectrum of state's capabilities in order to convince the attacker. The whole process of statement could be held by public or private statements, such as NATO's Warsaw summit in 2016 recognizing cyberspace as:

> "*...a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea*"[88].

Nevertheless, it lacks clear measures of response in a potential act of cyber aggression against NATO allies.

I have already mentioned the significance of attribution of cyber attacks in a previous section. Attributing such an attack and identifying the attacker can also improve cyber deterrence, as it raises the cost for the perpetrator. A possible way of detection of a cyber attack is by victims' reports, yet large financial institutions or private companies are not motivated to admit these incidents, due to potential reputational harm or fears that they account for liability and vulnerability. Hence, states should optimize motivation by establishing a confidential and lenient environment in order to overcome the aforementioned obstacles. Although an additional step to enhance attribution and consequently deterrence is investing in international law enforcement coordination and capabilities, there will still be a variety of attacks that are challenging to be attributed in adequate time for a response. It is also necessary to publicly condemn a perpetrator when the victim has evidence of proof. A solid and highly confident capability to identify the attacker, along with the "public shaming" can be a great lesson to result in cyber attack limitation. By publicly exposing the perpetrator state there is quite possible to create coalitions against it and damage its reputation and ability to negotiate. For instance, the Obama Administration made accusations against North Korea regarding the cyber attack on Sony Corporation, leading to imposing international sanctions against it[89].

The promotion of economic sanctions enforcement as a measure of deterrence should be introduced as well, considering some characteristics when implemented, such as the fact that they are more efficient at a broad scope, not imposed to specific individuals or companies, and they can lure the participation of the international community into a multilateral sanctions regime, if the incriminatory evidence are robust enough. Furthermore,

[88] NATO, *Warsaw summit communique*, Sec. 70, 2016.
[89] White House, *Remarks by the President in Year-End Press Conference*, 2014.

states with vulnerable, export-oriented economies can be targeted more effectively by the economic sanctions. In any case, solely imposing sanctions to increase deterrence is not the optimal method for states to achieve their goal, but it can be effective enough if accompanied by other tools of pressure, such as diplomatic participation.

Similar to the reinforcement of cyber defense, cooperation can provide a robust deterrent environment, as the would-be adversaries would worry about the consequences coming from the united capabilities of a comprehensive coalition, alliance and/or international institution. The existing defense agreements among countries in several sectors, such as economic and political cooperation can also be functional in cybersphere. Hence, the investment in collaboration and implementation of counter-cyber arrangements would mitigate and -at the same time- increase the costs for perpetrators.

Establishing treaties and arms control regulations could potentially support deterrence. The existing mutually agreed norms in different issues (e.g. nuclear stability) may be a satisfying initial point, yet due to different construction and means of achieving goals, some treaties provide a great example and are characterized by high level of applicability to cyber conflict. It is worth mentioning reviewing some particular treaties and their potential benefit to a new cyber one. Starting with the Nuclear Test Ban Treaties. they could not be characterized as equivalent, as there is no possible way to mitigate testing of a cyber weapon, just like the former did to nuclear weapons. Nevertheless, these treaties can offer a context of multilateral norms and a culture of sharing information that stand against unacceptable state behaviors. Accordingly, SALT, ABM and START cannot be related to the cyber realm, due to their focus on numerical limitations and bipolar structure. On the contrary, the BWC and the CWC could be a great example of applicability, due to their provision of open-ended definitions regarding the weapons they control and prohibition measures depending on state intent. Hence, the state intent definitions, the internationalized post-incident investigations of violations, along with the establishment of confidence-building initiatives, could contribute a lot to cyber stability.

To conclude, regarding cyber deterrence and state collaboration, countries should prioritize the definition of prohibited behaviors, such as actions that account for a danger to civilian population or conflict escalation. States could also commit to avoid attacks against adversaries' critical infrastructure or sensitive defense-related facilities in general, and proceed even further by creating an international body, just like the OPCW or the CTBTO, in order to review the compliance and support the victim state concerning a cyber attack. To ensure efficiency, states have to provide access and information to the verification body, to a certain level where sensitive information of the victim state is not threatened[90]. Beside the aforementioned suggestions, a future cooperation at this level is uncertain given the fact that it requires trust and partial concession of power.

[90] Donnelly DA. et. al., A Technical and Policy Toolkit for Cyber Deterrence and Stability, *Journal of Information Warfare*, vol.18, no.4, 2019, pp. 65.

CHAPTER III

USE OF PROXIES TO PROJECT CYBERPOWER IN INTERNATIONAL RELATIONS

Considering the characteristics and attributes of cyberspace, the internet has deeply influenced the international relations among nation-states. The impact on the international system arises from multiple factors, such as the ability to remove physical proximity and cause effects remotely, the new methods of attack which can be substantial to conventional weapons, as well as the variety of different actors.

The systemic impacts are the outcome of increased uncertainty and escalatory risks caused by the attributes of cyberspace. Specifically, what results in uncertainty and mistrust is the combination of -previously mentioned- attribution problems, lack of clear perception of what accounts for espionage and attack, and cyber tools providing unique characteristics and capabilities.

Regarding attribution problems, it is quite challenging to effectively attribute a cyber attack with a high degree of confidence. In recent years this process has become easier -from a technical point of view- mainly because nations and private sector firms have highly sophisticated tools in their disposal, however attribution usually confronts political barriers. As far as the lack of perception between espionage and attack, it is an issue that comes from the existing legal gap and gray zones of the cyber realm. As I have mentioned in Chapter II, there are various types of cyber attacks that could possibly exceed the limits of data collection and cause destructive results. The uncertainty comes when the defender cannot be sure about the attacker's intentions[91], and thus takes into consideration all possible scenarios. The nature of cyber weapons also lead to mistrust among countries and influence international relations, through their 'use and lose' and dual-use character. 'Use and lose' describes -in fact- the 0-day vulnerability as a method of operation. The window of opportunity in this kind of vulnerability is tiny and the actors tend to hide their capabilities relative to such exploits. The dual-use attribute refers to both military/civilian distinction, and to broad use by law enforcement and intelligence agencies, companies in the private sector, and so on. Hence, a

[91] Buchanan B., *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*, Oxford University Press, 2016. pp. 2-3.

cyber weapon can be used by numerous actors for various reasons[92] -either legitimate or illegitimate- and that is exactly what provokes uncertainty and mistrust.

There is also high risk of escalation due to the number of actors that can have access to the internet. The growing interdependence brings new sources of insecurity, as the internet was created to perform, not to be secure[93]. State actors may actively engage in cyber operations themselves, or may use non-state actors as proxies -such as hacktivists, private companies, etc. (see Chapter II-Actors)- a fact that further complicates the process of attribution and possibly increases the risk of escalation, given that the true motives of perpetrators may be difficult to identify.

The reduction of physical barriers and geographic distances as an effect of globalization has proven that new threats emerge, which can effectively cause notable damage and introduce new security variants to take into consideration. For instance, until some years ago it was considered that North Korea could harm the U.S. soil only through the use of ICBM, by developing its nuclear program. However, North Korean hackers managed to achieve an attack on Sony Pictures Entertainment in Hollywood. Of course, the outcome of such an attack cannot be compared to a nuclear hit in terms of physical destruction, yet it can bring results[94].

The existing systemic impacts of cyberspace characteristics raise crucial questions regarding future understanding of what account for use of force and armed attack, whether the latter has to include a more comprehensive approach of harm -not primarily death or physical damage- or not.

Power and Cyberspace

The concept of power is a significant aspect of international relations since the ancient times, when philosophers from Greece -such as Thucydides- were interested in it (e.g. Peloponnesian War[95]). Moreover, Joseph Nye is one of the modern era experts who has distinguished soft from hard power, providing various forms of power behavior (e.g. from command to co-option). It is clear that in the process of defining cyberpower some difficulties emerge, encompassing three variables, such as the nature of the operational capabilities,

[92] Maurer T., Internet Freedom and Export Controls: Briefing before the Commission on Security and Cooperation in Europe, *Carnegie Endowment for International Peace*, 2016.

[93] Perlroth N., Reinventing the Internet to Make It Safer, *Bits* (blog), *New York Times*, December 2, 2014.

[94] Sanger D., Schmidt M. and Perlroth N., Obama Vows a Response to Cyberattack on Sony, *New York Times*, December 19, 2014.

[95] Thucydides, *History of the Peloponnesian War*, Rex Warner (trans.), Harmondsworth:Penguin Books, 1972/

which is the outcome of the convergence of diverse fields[96] (e.g. computer science, physics, military theory, economics, etc.), the immaturity of cyberpower as a concept of international politics[97], and the information hiding or misinformation from behalf of states, regarding their cyber capabilities. These difficulties introduce communication challenges and vagueness related to basic terms, uncertainty regarding the lack of testing cyberpower in a geo-strategic realm, and misunderstanding and/or overestimation of cyber threats[98] (especially by the media) accordingly.

In order to successfully define cyberpower like the traditional ones (e.g. military, economic power) it is necessary to examine both the foundational resources and the exercise of (cyber) power. The first one encompasses the material aspect, which is the outcome of the economic, scientific, technical and military resources invested in cyberspace by the states. The second one describes the ability of a state to achieve its goals and national priorities by leveraging cyber resources and forcing other actors to comply with it and follow its interests.

There is no universally recognised definition of cyberpower so far, however for the purpose of this dissertation I will follow the one described by Joseph Nye. According to him, cyberpower is:

> "*...the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power. Cyberpower can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace.*[99]"

Although this definition focuses on the strategic level and does not include the capabilities of the tactical level, nor the number of cyber weapons available in the state's arsenal, 0-day vulnerabilities, etc., it is -in my opinion- one of the best definitions available.

In the 21th century, power can be further divided and examined by researchers into the transition and diffusion of power. Regarding the transition of power, Nye focuses on the shift of power among states (e.g. from a great power to another), that ultimately determines the polarity of the international system. Hence, in the first decade of the 21th century the international system faced a transition of power from a bipolar to a uni-multipolar one, given the collapse of the USSR. On the other hand, the diffusion of power accounts for a

[96] Starr S., Towards an evolving theory of cyberpower, *Cryptology and Information Security Series*, vol. 3, 2009, pp. 18-52.

[97] Rid T., Cyber War will not take place, *Journal of Strategic Studies*, vol. 35, no. 1, 2012, pp. 5-32.

[98] Newton B., The Flawed Strategic Discourse on Cyber Power, *The Army War College Review*. vol. 1, no. 3, 2015, pp. 26-37.

[99] Nye J., Cyberpower, *Harvard Belfer Center for Science and International Affairs*, 2010, pp. 3-4.

mechanism of diffusion from states to non-state actors[100]. It is clear that in cyberspace non-state actors become way more important than in other domains, narrowing thus the gap between them and states. As significant examples are the Arab Spring, where social media critically influenced individuals and small groups towards the revolutions, and the role of Iranian hackers against financial institutions in the U.S.[101]

The Internet, as an international system in cyberspace, is an open, minimalist and neutral system with no central authority, that favors asymmetrical relations through the opportunity to non-state actors to actively engage in world politics and exercise hard and soft power, in comparison with the other traditional domains. So far, no actor, nor state neither non-state, managed to fully control and govern cyberspace due to highly demanding resources and expertise required in order to regulate the globalized networks[102].

How to measure Cyberpower?

To examine a more practical aspect of cyberpower, it is necessary to discover the objectives which a country seeks to achieve in cyberspace, along with the available capabilities that it maintains. To do so, I will focus on the NCPI report, which takes into consideration an 'all-of-country' approach by including every aspect under governmental control, such as national strategies, cyber offensive and defensive capabilities, resource allocation, innovation, private sector and so on. The report distinguishes seven national goals related to cyberpower, and thus provides an overall framework of the components of cyberpower. The seven goals are the following[103]:

1. Surveillance and monitoring of domestic groups,
2. Strengthen and enhancement of national cyber defenses,
3. Control and manipulation of the information environment,
4. (Foreign) Intelligence collection for national security matters,
5. Commercial advantage and/or enhancement of domestic industry growth,
6. Destructure or defacement of adversary's infrastructure and capabilities,
7. Definition of international cyber norms and technical standards.

[100] Nye J., *The Future of Power*, New York: Public Affairs, 2011, pp. 113.

[101] U.S. Department of Justice, *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector*, no. 16-348, 2016.

[102] Choucri N. and Reardon R., Cyberspace in International Relations: A View of the Literature, *Paper Prepared for the 2012 ISA Annual Convention,* 2012, pp. 14-15.

[103] Voo J. et al., National Cyber Power Index 2020: Methodology and Analytical Considerations, *Belfer Center Harvard Kennedy School*, 2020, pp. 1.

The NCPI equation (see Figure 3.) takes into account two factors that measure the "comprehensiveness" of a state as a cyber actor in pursuing one or more of the aforementioned goals. The first one is the country's intent to use cyberspace as an operational environment for these objectives, and the second one is the cyber capabilities of a country in cyberspace.

Concerning the intent, it accounts for the quality and quantity of planning activities of the government, such as the national strategies regarding cyber security, crisis plans, and so on. Practically, it results from the behavior of a country when it comes to cyber issues[104]. As far as capabilities are concerned, they represent a country's efficiency related to one or more of the cyber objectives that have been mentioned above.

$$National\ Cyber\ Power\ Index\ (NCPI) = \frac{1}{7}\sum_{x=1}^{7} Capability_x * Intent_x$$

Figure 3., NCPI equation[105]

It is worth noting to present a graph of the most comprehensive (combination of both intent and capabilities) cyber states in 2020, according to the Belfer Center's report:

[104] Bodeau D. et al., How Do You Assess Your Organization's Cyber Threat Level, *The MITRE Corporation*, 2010, pp. 3.

[105] "x" represents one of the seven national objectives, Ibid, pp. 2.

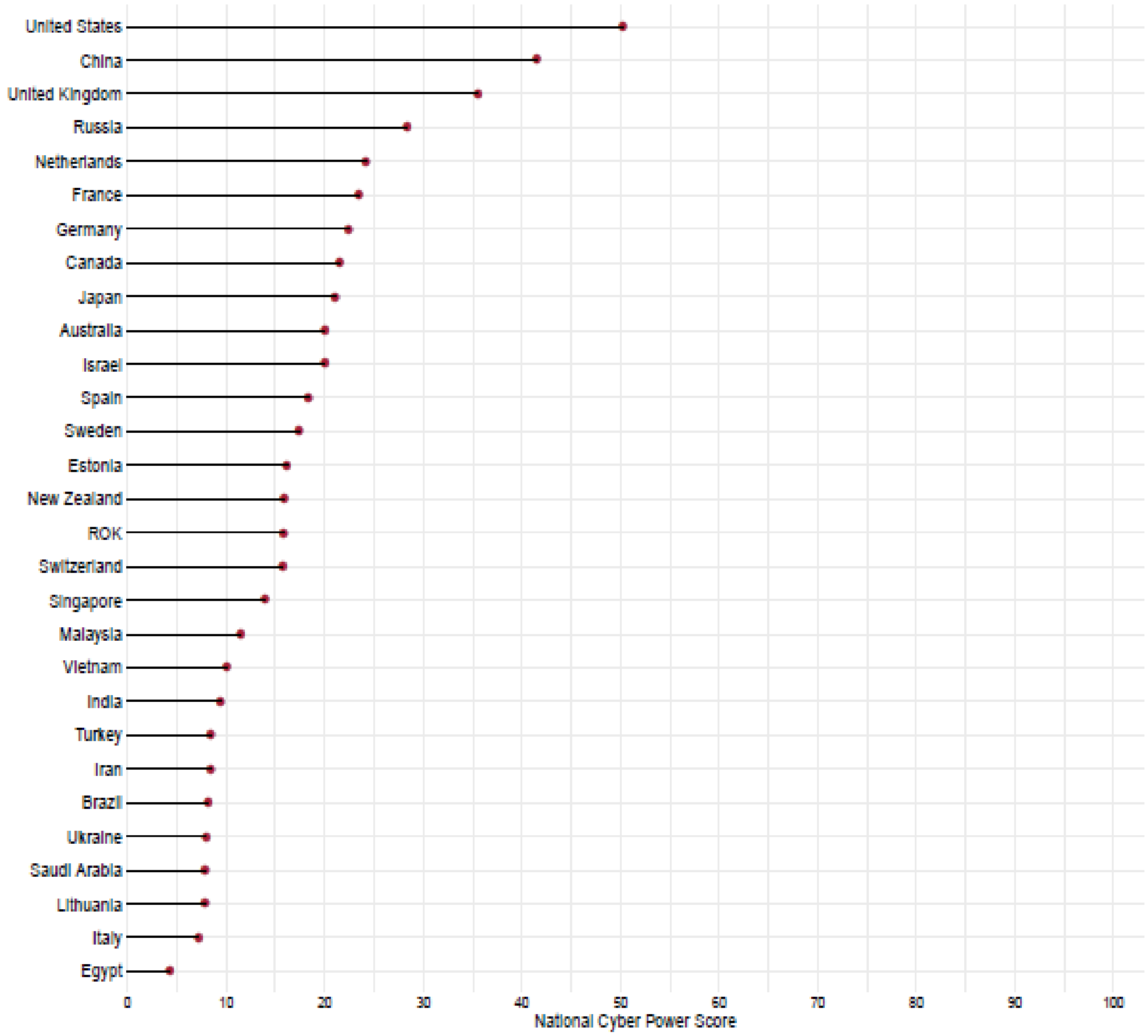
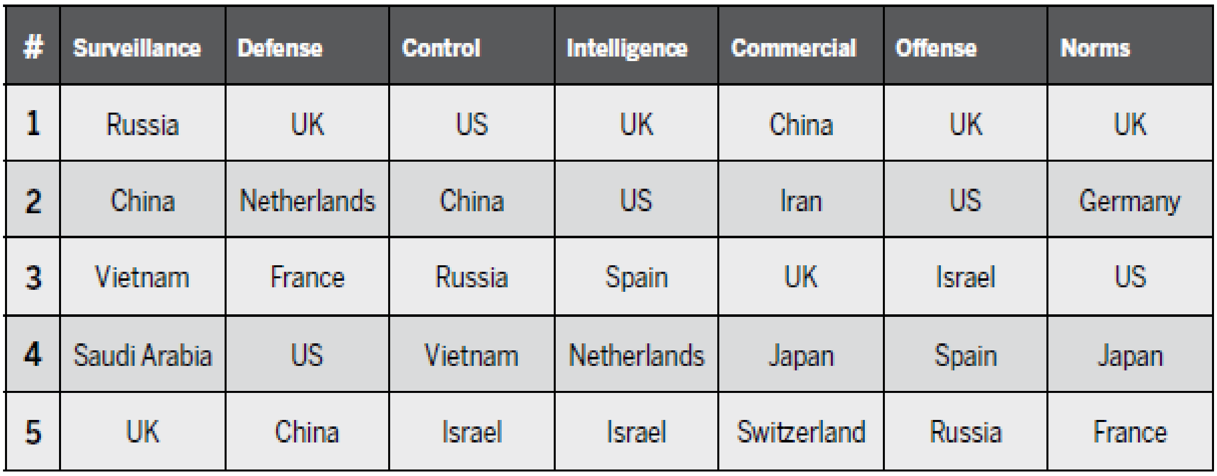


Figure 3.1., The Most Comprehensive Cyber States in 2020.

As we can notice, the U.S. along with China and the U.K.seem to strive for achieving one or more of their national goals through cyberspace, while at the same time they possess a high level of cyber capabilities. On the other hand, Egypt maintains the lowest score on the board, which means that it has neither the intent nor the capabilities to pursue its goals through the cyber realm. Since this index includes two factors, we should keep in mind that some countries may lack in one of them and fulfill the criteria of the other one. For example, South Korea is a country that possesses a high level of cyber capabilities, yet it purposely avoids making use of them. On the contrary, Russia, Iran, the Netherlands, and others, may be motivated to be more active in the cyber domain, however either they do not have the capabilities to achieve it yet, or they intentionally hide them, or even they have focused only on one aspect of examining national objectives.

Besides the NCPI, we can further focus on each one of its components and isolate them as a distinct index. For instance, there is the CII which examines solely the intent of a country, and the CCI which presents its capability. For the CII, the five countries with the greatest intent to be active in cyber activities in general were China, the U.S., the U.K., Russia, and the Netherlands. However, it is significant to demonstrate the ranking by objective, as it will provide us with vital information regarding the priorities of each country.



#	Surveillance	Defense	Control	Intelligence	Commercial	Offense	Norms
1	Russia	UK	US	UK	China	UK	UK
2	China	Netherlands	China	US	Iran	US	Germany
3	Vietnam	France	Russia	Spain	UK	Israel	US
4	Saudi Arabia	US	Vietnam	Netherlands	Japan	Spain	Japan
5	UK	China	Israel	Israel	Switzerland	Russia	France

Table 3.1., Top 5 Intent Ranking by Objective[106]

Unsurprisingly, Russia and China place high in surveillance and control cyber operations, as they prioritize information technology and control through their official cyber documents. Control can be seen as an element with dual purpose. Firstly, it signifies the effective confrontation of extremist components in the country, and secondly, reflects the domestic propaganda and the spread of disinformation abroad. In the case of the U.S., this high positioning represents the disruption of ISIS's communication with its fighters, while China and Russia conducted several disinformation campaigns.

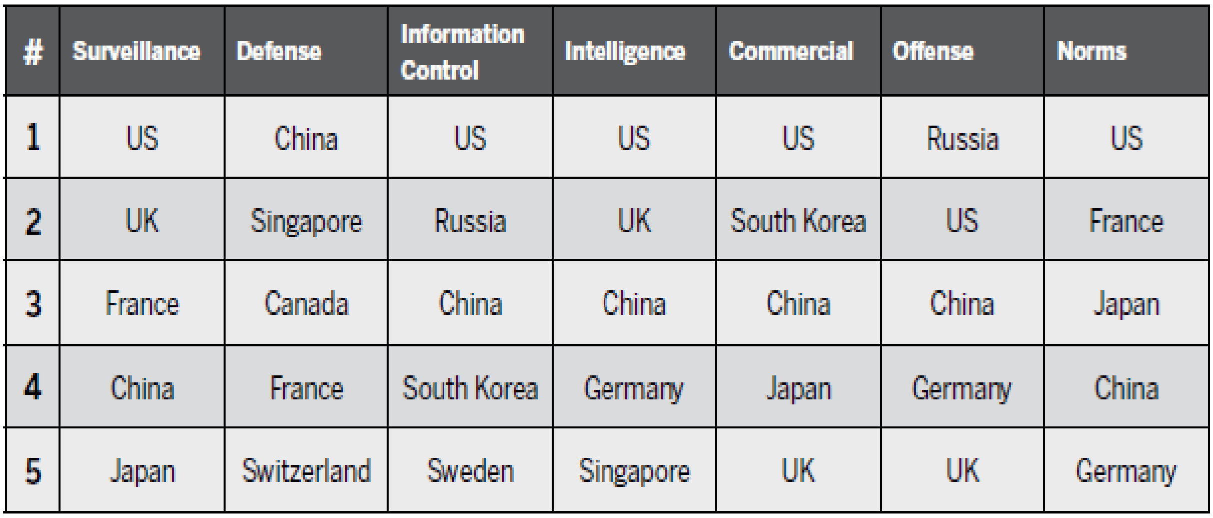
Although China's ranking is high only in surveillance, control and commercial activities, it possesses the first place overall, due to the use of attributed attack data as a parameter on this index. Observing the offense component of Table 3.1., we can notice that the U.K. and the U.S. rank higher, while Russia stands in the fifth position. However, in this particular objective there are limitations and misperceptions, as it accounts for a sensitive aspect of governmental goals and many countries either indeed do not pursue offensive operations, because of the high level of technical competence required, or they avoid expressing their

[106] Ibid, pp. 31.

intents, due to the existing vagueness regarding the compliance of cyber offensive operations and international law on armed conflict. In addition, transparency is a critical element when it comes to destructive cyber offensive operations, and both the U.S. and the U.K. as liberal democracies could be characterized as more transparent than other states, that arguably we would expect them to rank higher.

Observing the intent on forming cyber norms, it is obvious that the western countries tend to maintain their motivation on establishing rules of better communication, efficient international institutions and capacity building initiatives.

As far as the CCI is concerned, Table 3.1.1. demonstrates the top 5 countries with the greatest capabilities on each one of the specific aspects of cyberpower.



#	Surveillance	Defense	Information Control	Intelligence	Commercial	Offense	Norms
1	US	China	US	US	US	Russia	US
2	UK	Singapore	Russia	UK	South Korea	US	France
3	France	Canada	China	China	China	China	Japan
4	China	France	South Korea	Germany	Japan	Germany	China
5	Japan	Switzerland	Sweden	Singapore	UK	UK	Germany

Table 3.1.1., Top 5 Capabilities Ranking by Objective[107]

The U.S. dominates in five out of seven aspects of cyber activities, and hence this proves its undoubtable leadership in cyber capabilities. Although China managed to reach the top 4 in every aspect of cyber objectives, an achievement that signifies the great advancement of R&D of technologies during the last years, it still remains behind the U.S. in most areas[108].

Russia places first in cyber offensive operations, as the country has performed numerous disruptive cyber attacks so far[109], and its position in this specific objective underlines the capability to destroy and disrupt infrastructure.

[107] Ibid, pp. 40.

[108] Cheung T.M., The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities, *Journal of Cyber Policy*, vol. 3, no. 3, 2018, pp. 306-326.

[109] Cyber Operations Tracker, *Council on Foreign Relations*.

Comparing traditional forms of power with Cyberpower

As I have mentioned before, the concept of cyberpower is still immature in terms of historical experience, and thus it is quite difficult to fully understand even the nature of cyberspace per se, as it is rapidly evolving. Nevertheless, it is possible to compare sea, air, land, and space power with cyber one, in order to identify similarities that can lead to an adequate construction of norms and attributes.

To begin with, sea power is defined as:

"*a nation's ability to enforce its will upon the sea*[110]"

and lies in both military seafaring ability and maritime trade, as equally important aspects of sea power. Hence, sea power is not only the military power of a state, or the arms' domination in the sea, but also the maintenance of peaceful commerce as well[111]. From this perspective, it is vital to maintain control over an environment and demonstrate power through active presence. As sea power's environment is the oceans, cyberpower's environment could be considered fiber-optic cables and satellites, and thus an aspect of cyberpower could be the ability to control access to cyberspace. If a state succeeded in such an endeavor, it would mean that it could project power through restricting access to its adversaries, and use this privilege to develop e-commerce, which is the economic aspect of cyberpower.

About air power, I will follow the definitions of Richard Kohn and Billy Mitchell, who describe it as:

"*the use of space off the surface of the earth to decide war on the surface*[112]"
and "*the ability to do something in the air*[113]" accordingly.

The most important lesson to be learnt from the comparison of air power with cyberpower is expectations. To be specific, when air power was introduced during World War I, it was considered a game-changing tool that would provide dominance to the one acquiring it over its enemies, as bomber airplanes could hit more easily and effectively the adversary's national resources. However, these theorists failed to presage the development of radar technology and other intercepting mechanisms that could balance the overwhelming effects of air power at that time. Similarly, when examining cyberpower we should consider the future countereffects, in order to avoid such misperception.

[110] Stevens W. and Westcott A., *A history of sea power*, Doran company: New York, 1920, pp. 444.

[111] Mahan A., *The Influence of Sea Power upon History, 1660-1783*, Dover Publications, Revised Ed. Edition, 1987.

[112] Douchet G., *The Command of the Air*, Air University Press: Alabama, 1953, pp. 30.

[113] Westenhoff C., *Military air power: the CADRE digest of air power opinions and thoughts*, University Press of the Pacific, 2002.

Land power has been examined from many military theorists through the years, such as Carl von Clausewitz and Sun Tzu, as it was the only aspect of a state's power many years ago. Theorists of land power usually focus on terrain analysis, which consist of geographical and strategic points, and terrains of decisive battle. In the forefront of land power, there are two clashing theories, where the first one focuses on the mobilization of resources throughout the domestic area of a state as a crucial factor to decide the terrain of warfare (high chance of victory)[114], while the other focuses on the population and material goods as the essential source of power[115]. Following the same pattern, a cyberpower theory should determine the vital resources, strategic terrain, and adequate points for resource mobilization.

Space power as a definition can be presented as:

> "*the ability of a state or non-state actor to achieve its goals and objectives in the presence of other actors on the world stage through…exploitation of the space environment*"[116].

During the Cold War, space power was considered a symbol of economic and technological strength, and at the same time it signified the ability of an actor to hit at the adversary's core or COGs with the consequence of paralyzing the enemy's kinetic operations and secure a relatively easy dominance[117]. More broadly, I could argue that space power is the ability of an actor to operate and influence activities to, in ,through, and from space. The attempt to affect an outcome from space, that takes place on earth, follows a similar process with the cyber realm, as the latter operates via transportation of information by overcoming physical and geographical barriers. Hence, space power theory underlines the importance of determining how cyberpower affects the physical environment.

Cyberpower defined and implemented by Great Powers: Case Studies

An equally -and arguably a more- effective way to understand and define cyberpower is through the process of observing how great powers comprehend this very term. This accounts for a more practical perspective which provides a realpolitik element, through monitoring of disposed national budgets in cyber capabilities, national public statements by political and military figures, unclassified documents expressing the implemented strategy

[114] Rattray G., "An environmental approach to understanding cyberpower", in *Cyberpower and National Security*, Kramer D. et al., National Defense University Press, 2009, pp. 253-274.

[115] Spykman N., *Geography of the Peace*, Archon Books: Hamden, CT, 1944.

[116] Hyatt J. et al., Space Power 2010, Research Report no. 95-05, *Air Command and Staff College*, 1995. pp. 5

[117] Harter M., Ten Propositions Regarding Space Power:The Dawn of a Space Force, *Air and Space Power Journal*, vol. 20, no. 2., 2006, pp. 68.

and so on. Of course, transparency of information among countries is subjective, yet we have to proceed according to available sources.

To begin with, China is a country that keeps most of its capabilities and military doctrines in the dark, rendering monitoring procedures pretty challenging. However, especially for cyber capabilities, there are a lot of public statements on behalf of China's ambitions and expectations by the Chinese leadership. There are times that China's policy focuses on the foundational aspects (e.g. economic, scientific, military resources of the country) and others that prioritize the dynamic ones (e.g. coercive activities to pressure adversaries)[118]. In 2014, President Xi Jinping established a cyber security and information taskforce in order to enhance the policy on cultural, social, economic and military cyber topics. The President's goal was to convert China into a cyber-power by maintaining its own technology[119]. In 2016, President Xi Jinping insisted on the necessity of achieving a great scientific and technological capacity, a fact that underlines an element that lacks from the definitions mentioned above, which is no other than the acquisition of domestic mechanisms of technology production and development. In the same year, there was a public release of six points of policy guidance documents, defining China's priority areas[120]. The points embodied an overall promotion of IT technologies in all levels of decision making, defining the roles of the market and the government, as well as significant issues of informationization in different fields. Other points were the development of core technologies, the application of informatization in fields like economics, politics, society, national defense, military and so on. Among them, priority was the insurance of national cyber security through the promotion of China's role in the global cyber affairs, and the establishment of a people-oriented approach in the process of implementation of the cyber strategy.

Having a look at Russia's public statements, it is worth mentioning the fact that the word "cyber" is rarely mentioned by decision makers. The most relevant term that Russians prefer to use is "informationization[121]", however in 2008 policy on "The Strategy of Information Society Development in Russia" some significant outcomes can emerge for Russia's perspective regarding cyberpower. In contrast with western approaches that underline the technical capabilities and infrastructures, Russia prioritizes information

[118] Austin G., Mapping and Evaluating China's Cyber Power, *Lau China Institute Policy Paper Series*, *King's College London*, 2016, pp. 4.

[119] Tiezzi S., Xi Jinping Leads China's New Internet Security Group, *The Diplomat*, February 28, 2014.

[120] The State Council The People's Republic of China, *State Council Releases a five-year plan on informatization*, 2016.

[121] Thomas T., "Nation-state cyber strategies: examples from China and Russia", in Kramer D. et al., *Cyberpower and National Security*, Protomac Books, Inc., 2009, pp. 475-476.

technology in a way that accounts for a vital component of social, psychological, economic and military power. The bottomline is that Russia focuses on the cognitive and psychological domain of cyberpower.

Just like Russia, Europe rarely uses the term "cyberpower" in its official statements and documents, due to EU's more pacifistic approach to cyberspace in general[122]. The EU faces a lot of restrictions regarding the establishment of a cyberpower policy, due to the nature of the Union, which is characterized by the lack of a collective vision in many aspects of security policy. The decisions of this intergovernmental structure is the result of a lowest common denominator and not the one of a centralized decision making procedure. For this reason, the EU can be described mostly as a civilian power, and promotes the exchange of information and best practices regarding information security, instead of focusing on cyber offensive and defensive measures[123]. The fact that the EU does not follow a coercive cyberpower strategy, does not necessarily mean that it is an incapable cyber power, as it possesses other cyber capabilities, such as voluntary agreements, incentives, platforms for cooperation, as well as mandatory cyber governance mechanisms[124]. Hence, cyberpower for the EU signifies indirect control of cyberspace via institutions, and the process of establishing norms and standards for the formation of the cyber environment[125].

Concerning the U.S. approach of cyberpower, it is mainly expressed along with military power, and more specifically the way that the two are combined in operations. This was clear in the CYBERCOM in 2009, part of the U.S. Strategic Command, which consequently became the 10th combatant command in the armed forces in 2019[126]. Officially, in 2011 a policy document was released, focusing on more than solely military cyberpower, underlining the significance of cyber norms existence, in order to guide the international cyber actors. This document supported that in the majority of cases, the existing international norms could effectively apply to cyber activities conducted by states, and thus there was no need to reinvent customary laws or undermine the existing ones. Yet, some characteristics may require additional effort and clarification, in order to be efficiently applicable to the cyber realm[127]. This aspect of the U.S. approach to cyberpower is similar to the EU's, as it

[122] Cavelty D., Europe's Cyber Power, *European Politics and Society*. vol. 19, no. 3, 2018, pp. 304-320,

[123] Sliwinski K., Moving beyond the European Union's weakness as a cyber-security agent, *Contemporary Security Policy*, vol. 35, no, 3, 2014, pp. 468-486.

[124] Christou G., The EU's Approach to Cyber-Security, *University of Essex Online Paper Series*, 2017, pp. 1-13.

[125] Krzysztof S., European Union-Cyber Power in the Making, *Asia-Pacific Journal of EU Studies,* vol. 12, no. 1, 2014, pp. 1-22.

[126] Ferdinando L., CYBERCOM to elevate to combatant command, *U.S. Army*, 2018.

[127] United States, White House Office, & Obama B., International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, *White House*. 2011, pp. 9.

pursues the monitoring of major international institutions, where the cyber environment is built. However, for the U.S. this unique nature of cyberpower accounts for a risk, rather than an opportunity, and hence, the U.S. intends to incorporate the cyber sphere into the frame of formal institutional norms, where it maintains the upper hand and dominates.

Cyberpower through traditional political concepts

Cyberpower is not a concept that can be clearly noticed, such as a legal, political or economic status. There are no formal advantages as an aftereffect of this possession, only facilitation of strategic outcomes and priorities. In order to fully understand the importance of cyberpower it is necessary to examine the fields of politics, international relations, and international law.

The first concept is power as a goal unto itself. This approach was supported by classical theorists such as Niccolo Machiavelli and Hans Morgenthau among others, and signifies the pursuit of power as the ultimate goal of the international system. As classical realism and Morgenthau argues:

> "*We assume that statesmen think and act in terms of interest defined as power, and the evidence of history bears that assumption out[...]The concept of interest defined as power imposes intellectual discipline upon the observer infuses rational order into the subject matter of politics, and this makes the theoretical understanding of politics possible[...]A realistic theory of international politics, then, will guard against two popular fallacies: the concern with motives and the concern with ideological preferences.*[128]"

Thus cyberpower, as a different form of power, contributes to the overall power that a state possesses.

Next, there is the concept of power as influence. This is an easier and more familiar approach, where power is described as the ability to have impact on the international system via targeting actors and events. Basically, it is based on Robert Dahl's definition presenting power as the ability of A to convince B to do something that he/she would not[129]. Of course,

[128] Morgenthau H., *Politics Among Nations: The Struggle for Power and Peace*, Knopf: New York, 1978, pp. 4-15.

[129] Dahl R., The concept of power, *Behavioral Science*, vol. 2, no. 3, 1957, pp. 201-215.

the outcome could be achieved coercively or non-coercively, through force, threat, or other forms of power projection[130]. Consequently, a state that possesses cyberpower can:

> "*Economically exploit or undermine other nations; gather political and military intelligence more efficiently than pre-digital espionage; interfere in foreign political discourse online; degrade an adversary's warfighting capabilities; sabotage critical infrastructure and industrial mass production, and even cause mass casualties. All of this can be done through the clever application of digital technology and without necessarily deploying military forces or human spies.*[131]"

Another concept is power as a means of security, which was developed by a later school of realism who supported that power is a requirement for the states, in order to survive in the international system. John J. Mearsheimer, as a supporter of structural -and more specifically, offensive- realism accurately presents this perspective through his following statement:

> "*In a system where there is no higher authority that sits above the great powers, and where there is no guarantee that one will not attack another, it makes eminently good sense for each state to be powerful enough to protect itself in the event it is attacked. In essence, great powers are trapped in an iron cage where they have little choice but to compete with each other for power if they hope to survive*[132]".

As Mearsheimer defines it, it is the natural human desire for security that feeds a limitless pursuit of power, yet the more power a state acquires, the more it becomes a target for the adversaries, due to the anarchic nature of the international system. According to this perspective, cyberpower can contribute to a defensive level, as critical infrastructure and national security is based on cyber capabilities. For a state, cyberpower is a vital part of its military power, and thus it enhances national power and national security overall.

Power can also be seen as control over resources and capabilities, which accounts for a more quantitative aspect of power. More specifically, power from this point of view is the access to crucial resources, such as gross national product, population, technological prowess

[130] Langer R., Cyber Power- An Emerging Factor in National and International Security, *Center for International Relations and Sustainable Development (CIRSD)*, 2016.

[131] Ibid.

[132] Mearsheimer J., "Structural realism", in Dunne T. et al., *International relations theories: Discipline and diversity*, Oxford University Press, 2016, pp. 83.

and so on. However, power as control over resources lacks in terms of qualitative element incorporation, as it is not easy to take into consideration attributes such as willpower and national unity, among others. Adopting this perspective into the cyber realm, acquiring cyberpower would signify the possession of cyberpower capabilities.

Contribution to Offense and Defense

A state that possesses significant cyberpower can also enhance its overall offensive and defensive capabilities. Perhaps cyber capabilities alone cannot easily result in an armed conflict, yet they can accelerate this process by escalating the tensions already established. This means that a state capable of sophisticated cyber offensive operations is favored from the ability to strike with less risk compared to traditional kinetic means, at less cost, along with the attribute of anonymity. Furthermore, by conducting cyber operations the state does not physically emplace its soldiers in the field of battle and it is more likely to not engage into a military conflict at all[133].

On the other part, possessing cyberpower has also crucial defensive value for a state, due to the digitalization of critical infrastructure systems and the consequent importance of successfully defending them[134]. By achieving security of these systems, the state maintains a relative military advantage. However, there is a disadvantage in relying the military, economic and social institutions on cyber systems, as it accounts for a possible vulnerability which can be exploited by other state or non-state actors[135].

How to build Cyberpower?

There are some ways for the state actors to enhance their cyberpower, such as to develop their own capabilities, to rely on the adequate industry to provide them the necessary capabilities via services and/or recruit experienced and skilled individuals, to rely on volunteers, and to take advantage of existing cybercrime and hacktivism in a way that favors them. Of course, these methods can vary from state to state, or they can be combined depending on the circumstances. For instance, most of the Western countries avoid using the method of recruiting cybercriminals and hacktivists, and prefer engaging their national resources through the use of ICT services. Furthermore, states usually establish adequate instruments in order to facilitate the cooperation with the industry, as well as norms of

[133] Farwell JP & Rohozinski R., Stuxnet and the future of cyber war, *Survival*, vol. 53, no. 1, 2011, pp. 23-40.

[134] Langer R. supra note 135.

[135] Nye J., supra note 111.

information-sharing regarding the threats and attackers. There are initiatives that encourage the private sector to report any cyber incidents to national authorities, along with others that combine both public and private sector, in order to reduce the costs of such activities. In this context, the UK has developed the CPNI as a mechanism to counter any threat against the country, and especially the NCSC, which works in partnership with the former, to ensure the maximum level of security[136].

The groups of volunteers in the internet today account for a significant part of the attribution process. They work independently from states and consist of individuals who operate as investigators who are dedicated to publicly expose perpetrators with their investigation results, in comparison with states, which are restricted by the political impact of potential accusations and usually they are more skeptical in revealing their sources of information. As an example, the Project Grey Goose, which is an OSINT initiative[137], managed to collect and expose reasonable evidence of the Russian engagement in cybercrime elements that took place in the Georgian-Russian cyber incident in 2008[138]. The existence of powerful groups of volunteers could be an important asset for a state to take advantage of as a tool against the attribution of cyber attacks[139], yet there is a challenge of implementation of these groups into the national security perspective. Estonia is a country which, since its independence, has included non-state ICT actors in its cyber security framework, given the adoption of an early ICT-friendly culture. Due to this culture, Estonia is a highly cyber dependent country with a consequence of vulnerability, a fact that was proven during the 2007 cyber attacks. The Estonian CERT coordinated the role of industry actors along with volunteers, and as a result the country successfully managed to overcome these incidents. Since then, the role of volunteers has been promoted and gained official recognition with its presence in Estonia's national cyber security framework[140].

Another way to increase cyberpower is to take advantage of cybercriminals. This method has been allegedly used numerous times by the government of Russia, yet there is no hard evidence to prove these allegations. The theory that connects Russia with cybercrime in

[136] CPNI, *Counter Terrorism Strategy*.

[137] "OSINT is derived from data and information that is available to the general public. It's not limited to what can be found using Google, although the so-called "surface web" is an important component…Most of the tools and techniques used to conduct open source intelligence initiatives are designed to help security professionals (or threat actors) focus their efforts on specific areas of interest.", What is Open Source Intelligence and How Is It Used?, *Recorded Future*, 2019.

[138] Krebs B., Security Fix- Report: Russian Hacker Forums Fueled Georgia Cyber Attacks, *The Washington Post*, October 16, 2008.

[139] Klimburg A., Mobilising Cyber Power, *Survival*, vol. 53, no. 1, pp.41-60, 2011.

[140] Czosseck C. et al., Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security, *International Journal of Cyber Warfare and Terrorism*, vol. 1, no. 1, pp. 24-34, 2011.

its territory is based on the cyber incidents of Estonia in 2007 and Georgia in 2008, when the government had the control over cybercriminals and botnets who conducted the attacks, and consequently there was a merger of them with the Russian interests, through targeting Estonia via DDoS attacks[141]. Use of cybercrime elements by Russia can be seen in the Georgia incident as well, where there was even a coordination of cyber attacks and conventional military operations. Given the fact that Estonian law enforcement agencies requested cooperation with Russian agencies, in order to identify the perpetrator(s), and the latter did not responded, along with the successful continuation of RBN[142] even after its supposedly takedown, we can argue that Russia is unwilling to confront cybercrime and tolerates cybercriminals to a certain point.

State and Proxies

Proxies have been observed since ancient Greece, when Thucydides wrote about them, as well as mercenaries, during the Peloponnesian War. It is essential to examine this relationship in cyberspace and spot the advantages that can occur for the parties involved. Before moving to the advantages and risks of this relationship, I would like to clarify the reason for choosing the term “proxy” to describe the relationship between states and non-state actors in the cyber domain.

Why proxies over alliances and mercenaries in cyberspace?

At this point I will review three distinct, but related forms of relationships that exist in conventional domains: alliances, mercenaries, and proxies. Is it possible to be used in a relationship between a state and a non-state actor in cyberspace? Why is proxy ultimately the form of relationship that is being established and what are the differences among this one and the others?

To begin with, alliances are considered accords between two or more states, and they are formally expressed through official agreements that include each party’s obligations, as well as the mutually agreed conditions of operation, in order to mitigate the risk of exploitation of a party against another one. An alliance may have some attributes that could be effective in a relationship between a state and a non-state actor in cyberspace, such as the exchange of resources among the parties, however there are significant challenges. The nature

[141] Ottis R., Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, *Proceedings of the 7th European Conference on Information Warfare, CCDCOE*, pp. 163, 2008.
[142] Schrank P., A walk on the dark side, *The Economist*, August 30, 2007.

of participants involves -by definition- only state actors, and the formality of such relationships does not fit to the necessities of the cyber realm. To be more specific, in cyberspace actors desire to operate informally, obscuring C2 operations, maintaining plausible deniability, and thus making attribution difficult.

Regarding mercenaries or PMCs/PMFs[143], they account for an option for states as soldiers-for-hire, when such endeavor is favorable for the state (lack of capability, political and economic cost). Mercenaries' motivation is primarily financial profit and their presence in conflict is quite active. They represent the privatization of war and their characteristics can be described in Article 47(2) of Additional Protocol I of the Geneva Conventions:

> "*special recruitment, direct participation in hostilities, desire for private gain as primary motivation, neither a national of a party to the conflict nor a resident of territory controlled by a party, not a member of the armed forces of a party to the control, and not sent by another State on official duty as a member of its armed forces.*[144]"

There are some similarities between the mercenary relationship and the one conducted in cyberspace between states and non-state actors, nevertheless there are non-state actors who work with states, not only for profit driven motives, but also for political purposes. Considering these relationships as "cyber mercenary relationships" we exclude several individuals and/or groups. such as patriotic hackers, who are evenly important to states[145] (e.g. China). Additionally, there are significant cyber actors who are residents of territory controlled by a state involved in a conflict, and thus cannot be considered as mercenaries by definition. Last but not least, mercenaries -like alliances- usually operate through formal contracts.

Regarding a proxy relationship, it is in fact an agreement between a state and a non-state actor with mutual interests. This relationship is characterized by the exchange of resources and manpower. For instance, it is common for the state to provide financial resources, arms, training, and other forms of assistance to the non-state actor, while the latter remains loyal and facilitates the state's goals and priorities. From its nature, a proxy relationship is characterized by informality and secrecy, and thus this accounts for the most adequate model to define the existing relationships between states and non-state actors in

[143] Singer P. Corporate Warriors: The Rise of the Privatized Military Industry and Its Ramifications for International Security, *International Security*, vol. 26, no. 3, 2001, pp. 186-220.

[144] Schmitt M., ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press: Cambridge, 2013, pp. 104.

[145] Hang R., Freedom for Authoritarianism: Patriotic Hackers and Chinese Nationalism, *The Yale Review of International Studies*, 2014.

cyberspace. In fact, the attribute of informality and the advantage of plausible deniability that non-state actors offer to the equation, are the most crucial elements to ultimately result in the term “proxy” as the appropriate definition of such relationships.

Mutual Benefits

States can rely on proxies with special capabilities in order to increase their cyberpower, due to numerous advantages that occur, compared to a possible strategy of acting alone.

A first advantage is that a lot of non-state actors have greater experience in cyber issues than states per se, and thus non-state actors can provide quality of knowledge and expertise.

Secondly, through the use of proxies, states can avoid accusations and maintain plausible deniability. A state may also desire to avoid revealing its cyber capabilities to adversaries, and thus using cyber proxies can proceed without exposing them. As cyberspace accounts for a challenging environment regarding attribution, using proxies as a front adds another layer of security in the process of successful attribution.

Thirdly, a state can choose to use a proxy as a method to test the response of its victim and the international community in general, while denying responsibility and avoiding attribution. For instance, the incident of the Conficker botnet[146] can be the case of this approach, which was a combination of advanced malware and botnet technology infecting millions of computers over the time. Many attempts were made by law enforcement agencies and industry actors to take it down, although with no successful outcome at all. The interesting part of this botnet was that its purpose was not malicious (e.g. stealing information, etc.), while some believe that it was created solely to be tested by the take down attempts, and to examine the response and the effectiveness of the international community.

Fourthly, by using cyber proxies, states do not engage in direct conflict and -consequently- the operations do not have any casualties, nor are they that expensive. States tend to be careful as far as the intensity of an operation is concerned, due to still evolving norms of appropriateness in the cyber realm. Focusing in democratic societies, there are also electoral consequences from a possible association of a state with a cyber operation, a fact that leads as well to the use of cyber proxies.

Last but not least, cyber proxies may be used by states in order to be monitored and do not act against the governmental agencies.

[146] Conficker Working Group, *Conficker Working Group: Lessons Learned Document*, 2011.

On the other hand, cyber proxies acquire a lot of benefits as well, in some cases even more than the state gains from them. The first and vital advantage is the financial support that they receive from the state directly. A second one, a more indirect aspect of financial support, is the tolerance that they enjoy from the state, regarding their illicit activities in the cyber realm. Besides the financial aid, a state can provide sensitive equipment which is either too expensive for proxies to acquire it, or it is the state's monopoly. Such equipment could be significant for proxies, as it could allow them to expand their exploit capabilities and ultimately implement it to their operations in order to be more efficient. Along with equipment, a possible benefit of this relationship for proxies could be the revocation of Internet restrictions, providing thus full access and a remarkable advantage against other competitive actors. Also, proxies enjoy physical and legal security in the state's territory, where -as I mentioned before- there is tolerance regarding their illegal activities, and the state may target and sanction their competitors, or even share vital information with them, in order to advance their operational security.

It is important to clarify that in this section I focus on scenario (II) (see Table 1.2., pp. 22) where a state is determined as beneficiary and a non-state actor as a proxy. As I examine this specific beneficiary-proxy relationship, a crucial question arises: are states responsible for the actions of their proxies?

From a legal perspective, states are indeed responsible for their proxies' actions when the latter act under their instructions or control[147]. This measure has been established in order to assure that states cannot use private groups or individuals to avoid responsibility for their actions. However, there is practically a higher level of difficulty in attributing a cyber action than one in the traditional domains, and thus to blame the proxy in the first place. Usually the attribution process, when possible, overcomes the timeframe necessary for measures to be taken. Besides the attribution problem, there is also another challenge which relies on the existing high legal thresholds, where the level of support and involvement of states has to be so apparent and clear in order to be connected directly with the actions of a proxy, that technically there is a normative safe zone for them[148].

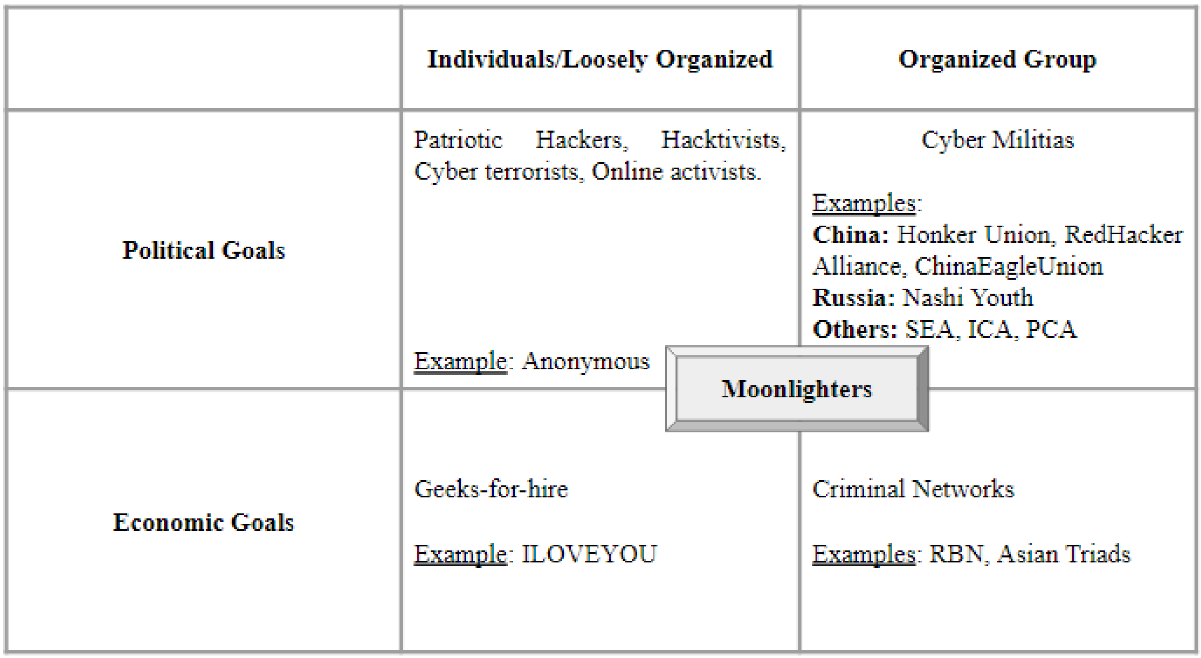
[147] Koh H., International Law in Cyberspace, *Harvard International Law Journal*, vol. 54, 2012, pp. 6

[148] Schmitt M. and Vihul L., Proxy Wars in Cyber Space: The Evolving International Law of Attribution, *Fletcher Security Review*, vol. 1, no. 2, 2014, pp. 71.

Categorization: Politically vs Financially Motivated Proxies

In Table 2.1. (pp.22) I have already provided information concerning the non-state actors in cyberspace, including their identities as well as their motives and targets. In this subsection I will focus on the detailed categorization of the major cyber proxies between political and economic goals, and thus I will use the information as a guideline to discover which one is more adequate in terms of reliability and risk mitigation for states.

To begin with, I will further distinguish politically motivated cyber proxies according to their organizational level (Loosely organized or Organized group), and financially or politically motivated cyber proxies respectively.



	Individuals/Loosely Organized	**Organized Group**
Political Goals	Patriotic Hackers, Hacktivists, Cyber terrorists, Online activists. Example: Anonymous	Cyber Militias Examples: **China:** Honker Union, RedHacker Alliance, ChinaEagleUnion **Russia:** Nashi Youth **Others:** SEA, ICA, PCA
Economic Goals	Geeks-for-hire Example: ILOVEYOU	Criminal Networks Examples: RBN, Asian Triads

Moonlighters

Table 3.2., Politically vs Financially Motivated Cyber Proxies[149]

Carrying political motives with loose organization or even individually organized can be considered the patriotic hackers, hacktivists, cyber terrorists, or online activists in general. Due to lack of resources and proper training, they have limited technical capabilities and their operations are restricted to site defacements, URL redirects, DoS attacks, virtual sabotage, and limited software development among others[150]. A great example of such proxies is the interventions of Anonymous as a response in several incidents, such as the Israeli policy

[149] Borghard E. and Lonergan S., Can States Calculate the Risks of Using Cyber Proxies?, *Foreign Policy Research Institute*, 2016, pp. 14.
[150] Samuel A., *Hacktivism and the Future of Political Participation*, Harvard University 2004, pp. 7

toward the Palestians in 2013[151], which was unsuccessful, and recently the Russia's invasion in Ukraine in 2022[152].

Cyber proxies with political motives but also with better organization and equipment, are the so-called cyber militias, such as the SEA, which has succeeded hacking operations in the past, such as the URL redirection of The Washington Post's website in 2015[153].

Concerning economically motivated cyber proxies, they are usually better resourced than the politically motivated ones, and the organized ones are the primary option for states to cooperate with. There is always the possibility of recruiting individuals for malware distribution or other operations, such as Gizman, who created the ILOVEYOU virus in 2000, however organized criminal networks are considered a more reliable option. This kind of networks count thousands of active groups cooperating through illicit activities, and their interest -especially the last decade- seems to be focused on cyberspace. As expected, these groups mostly operate in Eastern Europe and Asia, as the local regimes are not capable or motivated to confront them. Their sophisticated capabilities are a significant advantage which result in successful outcomes.

Moreover, there is a fifth unique category, the moonlighters. In fact, moonlighters are individuals who may operate in different forms of organization (e.g. operating both individually and as part of a group) or be motivated by both politically and economically goals. For instance, a moonlighter may operate as a geek-for-hire or patriotic hacker (individual, economic motive and political motive accordingly), while at the same time belongs to a criminal syndicate. This attribute proves the fluidity and the subjectivity of the distinct categories of cyber proxies, yet their existence facilitates the process of a more comprehensive examination of their nature.

Criteria for Choosing Cyber Proxies

When it comes to choosing a cyber proxy, a state should examine two factors: its motivation, and goals. As I have mentioned before, states are motivated to cooperate with cyber proxies when they desire to avoid any kind of involvement in an operation, due to possible physical or political costs, or when they lack technical capabilities that sophisticated proxies can provide.

To be more detailed, avoiding attribution is a major endeavor for states. It is commonly

[151] Anonymous hacker attack on Israeli websites 'causes little real damage', *The Guardian*, February 27, 2013.
[152] Milmo D., Anonymous: the hacker collective that has declared cyberwar on Russia, *The Guardian*, 2022.
[153] Fung B., The Syrian Electronic Army Just Hacked the Washington Post, Again, *The Washington Post*, May 14, 2015.

believed that attribution is impossible or really difficult to occur, although in fact the challenging part of the procedure is the political aspect, not the technical one. For instance, the U.S. identified DPRK as the perpetrator of the cyber attack against Sony in 2015, a fact that proves the existence of the technical capability. What defines attribution as challenging is identifying the level of C2 of a state over its proxy, and thus the level of the state's involvement in the operation. Reaching to a successful and accurate outcome, it is required high quality intelligence regarding the relationship on each specific operation (whether the state provides instructions, direction, or directly controlling the proxy)[154].

The technical capabilities and economic expenditures needed to conduct a cyber operation are quite demanding, as they require a great amount of investments, skill sets, tools, as well as infrastructure. This accounts for another motive for states to recruit cyber proxies for the needs of relative operations. DPRK for example, is not able to conduct cyber offensive operations on its own, due to the lack of capabilities, yet is willing to cooperate with cyber proxies and -for this reason- it has concluded several sophisticated cyber attacks in the past, besides the fact that it maintains a low level of IT infrastructure[155].

States also have their own agenda, their own goals and priorities. A broader categorization of goals is distinguishing them in two options: responding to an external, or an internal threat.

An internal threat may be introduced by a non-state group which is dangerous for the regime's stability. The government, hence, cooperates with them, in order to monitor and provide a target to keep them occupied. China usually organizes hacker competitions, not only to discover and recruit promising talents, but also to monitor and discourage individuals to get involved in anti-state activities[156].

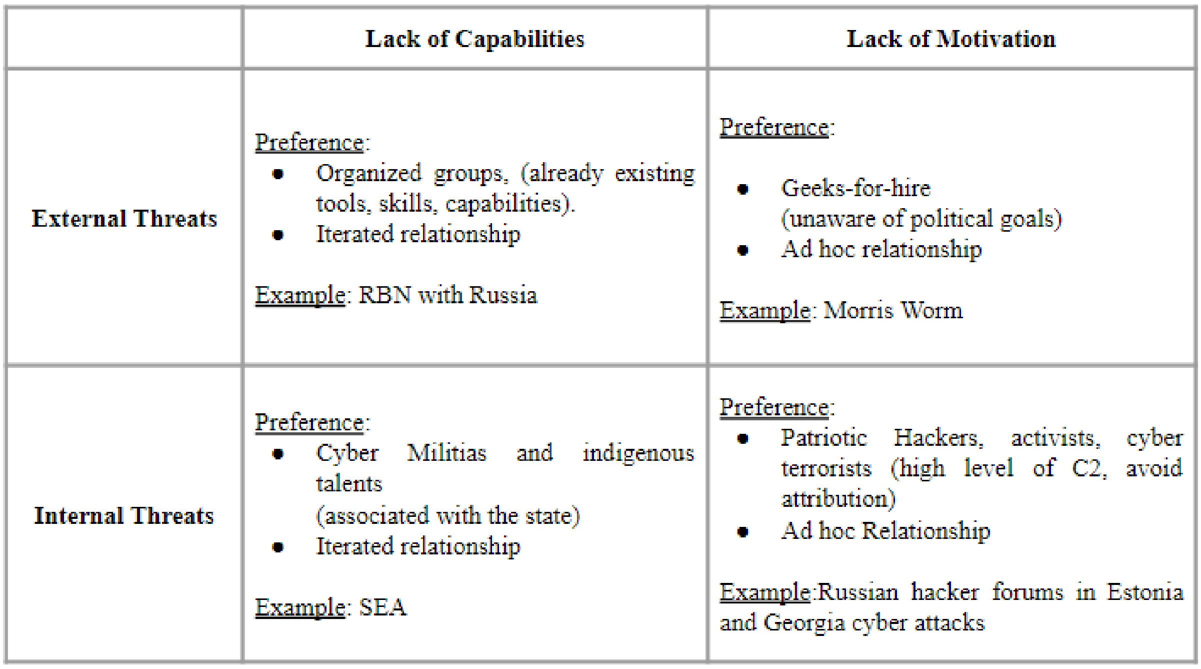
Considering both goals and motivation, a state will seek to choose a cyber proxy that maximizes the effectiveness, while at the same time is relatively manageable. Maintaining a strong C2 between the state and the cyber proxy is possible to reduce a state's capabilities to avoid attribution, although it is vital when the state deals with actors who are potential internal threats to the regime. As far as the states that lack cyber capabilities are concerned, it is more rational to establish long term relationships with specific groups, as thus they can reduce transaction costs. Nevertheless, this kind of relationship creates a pattern that can be identified, and hence plausible deniability is being undermined. On the other hand, relying on

[154] Schmitt M. and Vihul L., *supra note* 171, pp. 62.

[155] Krepinevich, Cyber Warfare: A 'Nuclear Option'?, *Center for Strategic and Budgetary Assessments*, 2012, pp. 36.

[156] Klimburg A., *supra note* 163, pp. 46.

ad hoc or ephemeral relationships enhances plausible deniability, but they can be more unstable and risky, due to lack of trust and short-term nature[157].



	Lack of Capabilities	**Lack of Motivation**
External Threats	Preference: • Organized groups, (already existing tools, skills, capabilities). • Iterated relationship Example: RBN with Russia	Preference: • Geeks-for-hire (unaware of political goals) • Ad hoc relationship Example: Morris Worm
Internal Threats	Preference: • Cyber Militias and indigenous talents (associated with the state) • Iterated relationship Example: SEA	Preference: • Patriotic Hackers, activists, cyber terrorists (high level of C2, avoid attribution) • Ad hoc Relationship Example:Russian hacker forums in Estonia and Georgia cyber attacks

Table 3.3., Optimal choice of Cyber Proxies[158]

Promethean Dilemma and Dilemma of Inadvertent Crisis Escalation

Examining the combination of the aforementioned criteria in order to establish beneficiary-proxy relationships, two kinds of dilemmas emerge: the Promethean dilemma and the dilemma of inadvertent crisis escalation. Both of them occur due to the fact that states provide tools, resources, and technical capabilities to cyber proxies, although there is the risk of a cyber proxy to overcome its mandate and become uncontrollable. Without those benefits, cyber proxies would be ineffective, yet providing them such tools imposes risks of mishandling them. Hence, it is crucial for states to execute a balanced calculation by taking all the benefits and risks of each circumstance into account, and seek to equip proxies as necessary as possible, but not to a level that it will become a threat.

Engaging with politically motivated proxies, states should expect a higher level of risk in both dilemmas. The Promethean dilemma occurs when the provided equipment and capabilities to proxies turn against the state, and it is more possible to appear in ad hoc relationships, besides the motivation, as there is no sufficient incentive for cooperation, due to lack of trust and the short-term nature of such a relationship. On the other hand, the dilemma

[157] Axelrod R., *The Evolution of Cooperation*, Basic Books: Cambridge, 2006. pp. 6.
[158]Borghard E. and Lonergan S, *supra note* 172, pp. 20.

of inadvertent crisis escalation emerges when the proxies may use the provided -from the state- tools to cause an unintended escalation with an adversary. This kind of risk is more likely to take place when the state cooperates with politically motivated cyber proxies, and more specifically with patriotic hackers, as it is more common to lack C2 over these actors, and simultaneously they can easily get carried away by their zealous motives and exceed the given mandate. Economically motivated proxies are usually less dangerous concerning risk escalation, due to their financial incentive.

To sum up, when it comes to politically motivated groups, the more organized a proxy is, the more likely it is to confront the consequences of the dilemmas. However, an organized economically motivated group is more reliable to mitigate the risk, especially when there is an iterated relationship between state and proxy. In most of the cases, the safest choice, as far as the risk mitigation is concerned, is an organized criminal group, which meets both the criteria of financially-driven nature, and it is also well organized, more capable and efficient, as it is constantly adapting to the dynamics of cyberspace. Another option for states should be the individuals with economic goals (geeks-for-hire). They may not have similar capabilities with the organized criminal groups, yet they are easier to be managed and controlled by the state From their perspective, economically motivated actors, either organized or individuals, can gain more benefits from their cooperation with a state than the politically motivated ones, and that is why the element of reciprocity and the expected profits are sufficient for both parties to commit in their cooperation. It is worth noting that politically motivated proxies could be efficient for the state if the latter's goal is to target internal, domestic threats. In this way, the dilemma of inadvertent crisis escalation will be excluded, while at the same time these groups can be more effective and provide vital information regarding domestic hacker networks.

Of course, in many cases states may not be able to choose the optimal option, due to other factors that influence their decision. For example, it is possible to lack technical capabilities in a level that ultimately limits their decision, and ultimately be forced to compromise with any cyber proxy available. If states end up with politically motivated cyber proxies, an essential strategy to follow would be the proliferation of low level capabilities, in order to be managed more easily and effectively.

Categorization: Distinguished types of relationship

Why is it important to examine and understand the different types of beneficiary-proxy relationships? The most significant reason is because of the implications that emerge for international stability. Proxies can escalate tensions and facilitate a conflict to occur, for example, through accident or miscalculation. Cyber proxies account for a technological addition to the international relations equation, and as such, they maintain an uncertainty regarding their behavior, a fact that leads to unpredictability. The risk related to proxies can be described through the so-called 'principal-agent problem', where the relationship is too loose and the principal's control is so weak, that raises a high possibility of a situation where the agent becomes unobedient and carries out operations beyond the principal's intention.

Examining the intensity of control that a state maintains over its proxies is essential due to national security implications, which result in danger for international peace and security. For instance, in 2014 Nasdaq[159] was hacked and its software was stolen by independent individuals with profit-driven motives[160]. Nevertheless, the initial concern of NSA was a potential involvement of the Russian government, and thus it is quite obvious that in times under tension or crisis, a hasty decision could lead to unfortunate outcomes. It could be argued that all states rely somehow on hackers in order to project cyberpower, however the difference emerges when it comes to the quantity and quality of control exercised over these proxies. Following Maurer's typology, there are three types of relationship between beneficiary and proxies: delegation, orchestration, and sanctioning.

Delegation is the type of relationship where a state delegates authority to proxy, in order to act on its behalf. This type can be seen as a "principal-agent" situation, as the agent obeys and complies with the principal's orders. However, in the real world this relationship is more complex, due to the fact that there are interests on behalf of the agent that should be considered, which can be distinct from the principal's, and transform the agent into an unpredictable actor. Attempts to confront undesirable behavior take place through monitoring and competition among the non-state groups, as the example of the U.S. which operates through proliferation of contracts, in order to increase competition among private companies. In addition, the U.S. government seeks to achieve direct communication with its proxies to ensure that they will comply with the government's goals. The CYBERCOM researches the background and behavior of its potential proxies before offering contracts, and keeps monitoring their actions during their cooperation. This approach is arguably the best way for beneficiaries to handle their proxies.

[159] "*Nasdaq is a global electronic marketplace for buying and selling securities*",

[160] Riley M., How Russian Hackers Stole the Nasdaq, *Bloomberg*, July 21, 2014.

Orchestration is the type of relationship where the beneficiary and the proxy are more distant and loose. The state uses its proxy as a means of achieving its goals[161], and the cooperation between the two parties emerges from similar goals and ideologies. In this specific occasion, the state tolerates proxy's behavior, provides its support and it is unable to prevent non-state actors from engaging in malicious activities. As a result, the beneficiary encourages and protects its proxy by following a more detached approach of control. The Iranian government has expressed its interest in this type of relationship, as the IRGC cooperated with politically motivated proxies, providing them with sufficient assistance, such as resources and training, to continue conducting operations that were beneficial for the government[162].

Sanctioning is the type of relationship where states remain idle to the malicious operation of their proxies. In contrast with delegation and orchestration, sanctioning does not include active assistance to proxies, and it is considered the most distant type of relationship. At some occasions, keeping distance with the proxy may have more benefits for the state itself, as sanctioning is a more internationally palatable way of engagement. Russia is a country that uses this type of relationship with its proxies, overlooking several malicious cyber activities conducted by hacking groups targeting extraterritorial objectives, such as the DDoS attack in Estonia and Russia's involvement in Ukraine and Georgia. This pattern indicates a sanctioning behavior on behalf of the Russian government[163].

Reviewing a country's approach to its cyber proxies occurs that liberal democracies tend to pursue a more tight control, while non-democratic ones choose a more loose relationship. This outcome possibly emerges from the fact that the political systems of the former countries operate with the principle of accountability through parliaments and elections. Of course, there are covert operations in which a more distant approach is being implemented, however these are the exceptions in the general rule of the modern conception of the state and its use of force.

Another worth mentioning attribute is the behavior of some countries, which they target not only foreign governments and/or companies, but dissidents as well, either foreign or local ones. These are the cases of China and Iran, among others, which perceive information

[161] Abbott K. et al., Orchestration: Global Governance Through Intermediaries, *SSRN Electronic Journal*, 2013, pp. 1-33.

[162] Maurer T., *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, 2018, pp/. 84-86

[163] Ibid, pp. 102.

as a threat to their stability, and thus they prioritize information security in both monitoring and manipulation of information, and establishing robust systems against intrusions.

In order to achieve a higher level of control upon proxies in their territory, states are encouraged to follow the U.S. model of delegation, as this specific form of engagement can result in a more effective communication between the parties and reduce the likelihood of proxy's disassociation from government's goals, and consequently a broader potential international instability. Of course, delegation requires active measures of participation, discussion, monitoring, as well as management of cyber capabilities, rather than prohibition and dictatorship[164].

But what measures must be implemented to control other states' proxy relationships? For a country, dealing with its own proxies is much more simple than trying to influence and manage a beneficiary-proxy relationship out of its sovereignty area. However, Maurer's DIME(LE) model attempts to overcome this challenge by creating leverages, incentives and disincentives to involved parties. DIME(LE) stands for Diplomacy, Information, Military, Economy, and Law Enforcement.

Through diplomacy, a country can be encouraged to alter its relationship with its proxy and adopt a more tight approach of control. China, for example, is a country that was criticized by numerous governments in public statements, regarding the issue of economic cyber espionage. Among the leaders who pressured the Chinese government so far was Angela Merkel, Hillary Clinton, and President Obama[165].

Information can be used as a tool in order to achieve a naming-and-shaming strategy and give a clear message to beneficiaries and their actors that a cyber operation is indeed possible to be attributed. In this context, the U.S. government unsealed a number of indictments against Iraninan citizens, sponsored by their country, accused for several DDoS attacks, as well as Russian and Canadian citizens regarding the Yahoo hack in 2016[166].

[164] Ibid, pp. 150.

[165] Merkel's China Visit Marred by Hacking Allegations, *Der Spiegel*, August 27, 2007.
Lander M., Clinton Urges Global Response to Internet Attacks, *New York Times*, January 21, 2010.
Gorman S., US Eyes Pushback on China Hacking, *Wall Street Journal*, 2013.

[166] US Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts, *U.S. Department of Justice*, 2017.

CONCLUSION

A clear definition of cyberpower is absent, given its immaturity as a concept in international relations. This term faces numerous difficulties that consequently hold back successful cyberpower estimation, leading to misinterpretation and misinformation regarding the level of domestic or adversary's cyber capabilities. The dominant phenomenon in the cybersphere is the diffusion of power that results in the developing role of non-state actors, as the Internet is an open, minimalist and neutral system with no central authority. Several great powers emphasize on different aspects of cyberpower, proving thus the distinct priorities and doctrines that they maintain in cyberspace. The significance of acquiring cyber capabilities can be seen in both offensive and defensive advantages that emerge, such as the ability to strike with less risk, at less cost, with anonymity, with no loss of personnel, and the need for protection of domestic critical infrastructure systems. Cyberpower for states can be enhanced through the development of their own cyber capabilities, through their cooperation with and reliance from private sector cyber security companies and/or volunteers, and through taking advantage of existing cybercrime and hacktivism in a way that is favorable to them.

States can rely on cyber proxies with special capabilities in order to increase their cyberpower. Some proxies have sophisticated cyber capabilities which provide quality of knowledge and expertise, while at the same time states can avoid attribution, costly and risky kinetic operations. However, cyber proxies benefit from their relationship with states, through direct financial gains, equipment, and tolerance regarding their illicit activities (if the proxy is a criminal group). There is also a distinction between financially and politically driven cyber proxies, and organized groups and individuals/loosely organized groups. States should rationally examine both their motivation and goals, in order to maximize the effectiveness of a cyber proxy without losing control. During this process, two dilemmas emerge: the Promethean dilemma and the dilemma of inadvertent crisis escalation, due to the fact that states provide tools, resources, and technical capabilities to cyber proxies, although there is the risk of a cyber proxy to overcome its mandate and become uncontrollable. When it comes to politically motivated groups, the more organized a proxy is, the more likely it is to confront the consequences of the dilemmas. From their perspective, economically motivated actors can gain more benefits from their cooperation with a state, because the element of reciprocity and the expected profits are sufficient for both parties to commit in their cooperation. Nevertheless, politically motivated cyber proxies could be efficient in targeting internal, domestic threats.

The risk related to proxies can be described through the ‘principal-agent problem’, where the relationship is too loose and the principal’s control is so weak, that raises a high possibility of disobedience on behalf of the agent. It could be argued that all states rely somehow on hackers in order to project cyberpower, however the difference emerges when it comes to the quantity and quality of control exercised over these proxies. Following Maurer’s typology, there are three types of relationship between beneficiary and proxies: delegation, orchestration, and sanctioning. Liberal democracies like the U.S. tend to follow a more tight control, while non-democratic ones choose a more loose relationship. In order to achieve a higher level of control upon proxies in their territory, states are encouraged to follow the model of delegation, as it can result in a more effective communication between the parties and reduce the likelihood of proxy’s disassociation from government’s goals. Last but not least, as far as influencing a beneficiary-proxy relationship outside of the area of sovereignty, Maurer’s DIME(LE) model attempts to create leverages, incentives and disincentives to involved parties.

BIBLIOGRAPHY

Academic Articles

- Abbott, K. W., Genschel, P., Snidal, D., & Zangl, B. (2013, August). Orchestration: Global Governance through Intermediaries. *SSRN Electronic Journal*, pp. 1-33. DOI: 10.2139/ssrn.2125452
- Alford, L. D. (2001, April). Cyber Warfare: A New Doctrine and Taxonomy. *Journal of Defense Software Engineering*, pp. 27-30. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.641.8312&rep=rep1&type=pdf
- Amorosi, D. (2011, November). Chinese State of Denial. *Infosecurity*, *Vol.8*(No.6), pp. 4-7. DOI:10.1016/S1754-4548(11)70076-6
- Armstrong, H. L., & Forde, P. J. (2003). Internet Anonymity Practices in Computer Crime. *Information Management and Computer Security*, *Vol.11*(No.5), pp. 209-215. https://doi.org/10.1108/09685220310500117
- Austin, G. (2016, September 19). *Mapping and Evaluating China's Cyber Power*. Lau China Institute, King's College London. https://ww1.prweb.com/prfiles/2016/09/19/13694501/Policy-Papers-Issue-2-Greg-Austin-Chinas-Cyber-Power.pdf
- Bartos, C. (2016, June). Cyber Weapons Are Not Created Equal. *Proceeding*, *Vol.142*(No.6). https://www.usni.org/magazines/proceedings/2016/june/cyber-weapons-are-not-created-equal
- Breen, M., & Geltzer, J. (2011). Asymmetric Strategies as Strategies of the Strong. *The US Army War College Quarterly: Parameters,*, *Vol.41*(No.1). https://press.armywarcollege.edu/parameters/vol41/iss1/3/
- Buchanan, B. (2016). *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press. DOI:10.1093/acprof:oso/9780190665012.001.0001
- Cavelty, D. (2018, January 25). Europe's Cyber Power. *European Politics and Society*, *Vol.19*(No.3), pp. 304-320. DOI: 10.1080/23745118.2018.1430718
- Cheung, T. M. (2018, December 12). The rise of China as a cybersecurity industrial power: balancing national security, geopolitical and development priorities. *Journal of Cyber Policy*, *Vol.3*(No.3), pp. 306-326. DOI: 10.1080/23738871.2018.1556720
- Cragin, R. (2015, March 25). Semi-Proxy Wars and U.S. Counterterrorism Strategy. *Studies in Conflict & Terrorism*, *Vol.38*(No.5), pp. 311-327. DOI: 10.1080/1057610X.2015.1018024
- Czosseck, C., Ottis, R., & Taliharm, A. M. (2011, July). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *Vol.1*(No.1), pp. 24-34. DOI: 10.4018/ijcwt.2011010103
- Dahl, R. A. (1957). The concept of power. *Behavioral Science*, *Vol.2*(No.3), pp. 201-215. DOI: 10.1002/bs.3830020303
- Denning, D. E. (1998). *Information Warfare and Security* (1st ed.). Addison Wesley Professional. DOI:10.1201/1079/43255.27.9.20000301/30321.7
- Denning, D. E. (2011). Cyber Conflict as an Emergent Social Phenomenon. In T. J. Holt (Ed.), *Corporate Hacking and Technology-driven Crime: Social Dynamics and Implications* (pp. 170-186). IGI Global. http://hdl.handle.net/10945/37158

- Duner, B. (1981, December 01). Proxy Intervention in Civil Wars. *Journal of Peace Research, SAGE Publications*, *Vol.18*, pp. 353-361. DOI: 10.1177/002234338101800404
- Farwell, J., & Rohozinski, R. (2011, January 28). Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy*, *Vol.53*(No.1), pp. 23-40. DOI: 10.1080/00396338.2011.555586
- Friesen, T. L. (2009). Resolving tomorrow's conflicts today: How new developments within the U.N. Security Council can be used to combat cyberwarfare. In *Naval Law Review* (Vol. 58 ed., pp. 89-98). U.S. Navy Judge Advocate General's Corps. https://www.jag.navy.mil/documents/navylawreview/NLRVolume58.pdf
- Goel, S. (2020, January). Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race. *Partnership for Peace Consortium of Defense Academies and Security Studies Institutes*, *Vol.19*(No.1), pp. 87-95. DOI:10.11610/Connections.19.1.08
- Golling, M., & Stelte, B. (2011, July 18). *Requirements for a future EWS- Cyber Defence in the internet of the future*. 2011 3rd International Conference on Cyber Conflict.
- Gorman, S. (2013, April 22). US Eyes Pushback On China Hacking - WSJ. *Wall Street Journal*. https://www.wsj.com/articles/SB10001424127887324345804578424741315433114
- Hare, F. (2012). *The Significance of Attribution to Cyberspace Coercion: A Political Perspective*. 4th International Conference on Cyber Conflict. http://195.222.11.251/uploads/2012/01/2_5_Hare_TheSignificanceOfAttribution.pdf
- Harter, M. E. (2006). Ten Propositions Regarding Space Power:The Dawn of a Space Force. *Air and Space Power Journal*, *Vol.20*(No.2), pp. 64-78. https://apps.dtic.mil/sti/pdfs/ADP023961.pdf
- Hassan, A., Funmi, D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *APRN Journal of Science and Technology*, *Vol.2*(No.7), pp. 626-631. http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf
- Hyatt, J., Laugesen, P., Rampino, M., Ricchi, R., & Schwarz, J. (1995, May). Space Power 2010. *Air Command and Staff College*, *Research Report no.95-05*. https://spp.fas.org/eprint/95-010e.pdf
- Jellenc, E. (2012). *Explaining Politico-Strategic Cyber Security: The Feasibility of Applying Arms Race Theory*. 11th European Conference on Information Warfare and Security. https://www.researchgate.net/publication/283674637_Explaining_politico-strategic_cyber_security_The_feasibility_of_applying_arms_race_theory
- Karatzogianni, A. (2010, November). Blame it on the Russians: Tracking the Portrayal of Russians During Cyber Conflict Incidents. *Digital Icons: Studies in Russian, Eurasian and Central European New Media*, (No.4), pp. 127-150. https://www.researchgate.net/publication/259850767_Blame_it_on_the_Russians_Tracking_the_Portrayal_of_Russians_During_Cyber_Conflict_Incidents
- Klare, M. (1989, Summer/Fall). Subterranean Alliances: America's Global Proxy Network. *Journal of International Affairs*, *Vol.43*(No.1), pp. 97-118. https://www.jstor.org/stable/24357169
- Klimburg, A. (2011, February). Mobilising Cyber Power. *Survival*, *Vol.53*(No.1), pp. 41-60. DOI: 10.1080/00396338.2011.555595
- Koh, H. (2012, December). International Law in Cyberspace. *Harvard International Law Journal*, *Vol. 54*, pp. 1-12. https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf

- Krepinevich, A. F. (2012, August 24). Cyber Warfare: A “Nuclear Option”? *Center for Strategic and Budgetary Assessments*, pp. 1-189. https://csbaonline.org/research/publications/cyber-warfare-a-nuclear-option
- Krzysztof, S. (2014, September). European Union-Cyber Power in the Making. *Asia-Pacific Journal of EU Studies*, *Vol.12*(No.1), pp. 1-22. https://www.researchgate.net/publication/317717658_European_Union_-_cyber_power_in_the_making/stats#fullTextFileContent
- Maurer, T. (2016, October 19). 'Proxies' and Cyberspace. *Journal of Conflict & Security Law*, *Vol.21*(No.3), pp. 383-403. DOI: 10.1093/jcsl/krw015
- Maurer, T. (2018, July 05). Cyber Proxies and Their Implications for Liberal Democracies. *The Washington Quarterly*, *Vol.41*(No.2), pp.171-188. DOI: 10.1080/0163660X.2018.1485332
- Miladi, N. (2016, February). Social Media and Social Change. *Domes: digest of Middle East Studies*, *Vol.25*(No.1), pp. 36-51. DOI:10.1111/dome.12082
- Naim, M. (2012, May/June). Mafia States: Organized Crime Takes Office. *Foreign Affairs*, *Vol.91*(No.3), pp. 100-111. https://www.jstor.org/stable/23217970
- Newton, B. (2015, August). The Flawed Strategic Discourse on Cyber Power. *The Army War College Review*, *Vol.1*(No.3), pp. 26-37. https://publications.armywarcollege.edu/pubs/2380.pdf
- Pelican, L. (2012). Peacetime Cyber-Espionage: A Dangerous But Necessary Game. *CommLaw Conspectus: Journal of Communications Law and Technology Policy*, *Vol. 20*, pp. 363-471. https://www.semanticscholar.org/paper/Peacetime-Cyber-Espionage%3A-A-Dangerous-But-Game-Pelican/7e9ffcb8629fdc614c6cebe4a2678fe066ac7307
- Prunckun, H. (2018). *Cyber Weaponry: Issues and Implications of Digital Arms*. Springer. https://doi.org/10.1007/978-3-319-74107-9
- Putman, C., Abhishta, A., & Nieuwenhuis, D. (2018, April 28). Business Model of a Botnet. *Proceedings of 2018, 26th Euromicro International conference on Parallel, Distributed, and Network-Based Processing (PDP)*, pp. 1-6. DOI: 10.1109/PDP2018.2018.00077
- Rid, T. (2011, October 05). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *Vol.35*(No.1), pp. 5-32. DOI: 10.1080/01402390.2011.608939
- Robinson, M., Jones, K., & Janicke, H. (2015, March). Cyber Warfare: Issues and Challenges. *Computers & Security*, *Vol. 49*, pp. 70-94. DOI: 10.1016/j.cose.2014.11.007
- Rowe, N. (2010). *International Journal of Cyber Ethics*, *Vol.1*(No.1), pp. 20-31. DOI:10.4018/jte.2010081002
- Schmitt, M., & Vihul, L. (2014, February 01). Proxy Wars in Cyberspace. The Evolving International Law of Attribution. *Fletcher Security Review*, *Vol.1*(No.2), pp. 55-73. https://ccdcoe.org/uploads/2018/10/c28a64_2fdf4e7945e9455cb8f8548c9d328ebe.pdf
- Shamsi, J. A., Zeadally, S., Sheikh, F., & Flowers, A. (2016). Attribution in cyberspace: techniques and legal implication. *Security and Communication, Special Issue Paper*. DOI: 10.1002/sec.1485
- Sharma, A., Gandhi, R. A., Mahoney, W., Susan, W., & Zhu, Q. (2010, August). *Building a social dimensional threat model from current and historic events of cyber attacks*. IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust.
- Sigholm, J. (2013, December). Non-State Actors in Cyberspace Operations. *Journal of Military Studies*, *Vol. 4*(No. 1), pp. 1-37. https://doi.org/10.1515/jms-2016-0184

- Silomon, J. (2018, Summer). Software as a Weapon: Factors Contributing to the Development and Proliferation. *Journal of Information Warfare*, *Vol.17*(No.3), pp. 106-123. https://www.jinfowar.com/journal/volume-17-issue-3/software-weapon-factors-contributing-development-proliferation
- Singer, P. (2001, December). Corporate Warriors: The Rise of the Privatized Military Industry and Its Ramifications for International Security. *International Security*, *Vol.26*(No.3), pp. 186-220. https://www.jstor.org/stable/3092094
- Sliwinsky, K. (2014, September 22). Moving beyond the European Union's Weakness As a Cyber-Security Agent. *Contemporary Security Policy*, *Vol.35*(No.3), pp. 468-486. DOI: 10.1080/13523260.2014.959261
- Starr, S. (2009). Towards an Evolving Theory of Cyberpower. *Cryptology and Information Security Series*, *Vol.3*, pp. 18-52. DOI: 10.3233/978-1-60750-060-5-18
- Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., & Vigna, G. (2009, November). Your botnet is my botnet: analysis of a botnet takeover. *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 635-647. https://sites.cs.ucsb.edu/~chris/research/doc/ccs09_botnet.pdf

Books

- Axelrod, R. M. (2006). *The Evolution of Cooperation* (Revised ed.). Basic Books. ISBN-13: 978-0465005642
- Carr, J. (2011). *Inside Cyber Warfare* (2nd ed. ed.). O'Reilly Media Inc.
  The Compact Edition of the Oxford English Dictionary: Complete Text Reproduced Micrographically, Vol. II P-Z. (1971). Oxford University Press: New York. ISBN: 019861117X 9780198611172
- Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010, November). *On Cyber Warfare* [A Chatham House Report]. Chatham House.
- Douchet, G. (1953). *The Command of the Air*. Air University Press: Alabama. https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0160_DOUHET_THE_COMMAND_OF_THE_AIR.PDF
- Hughes, G. (2014). *My Enemy's Enemy: Proxy Warfare in International Politics*. Sussex Academic Press. ISBN: 978-1845196271
- Jaitner, M. L. (2015). Russian Information Warfare: Lessons From Ukraine. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (pp.88-89). NATO CCD COE. https://ccdcoe.org/uploads/2018/10/Ch10_CyberWarinPerspective_Jaitner.pdf
- Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In *Cyberpower and National Security* (1st ed. ed., pp. 24-42). Protomac Books and Center for Technology and National Security Policy.
- Lachow, L. (2009). Cyber Terrorism: Menace or Myth? In F. Kramer, S. Starr, & L. Wentz (Eds.), *Cyberpower and National Security*. National Defense University Press. ISBN-13 : 978-1597974233
- Libicki, M. C. (1995). *What is Information Warfare?* ACT and National Defense University. https://apps.dtic.mil/sti/pdfs/ADA367662.pdf
- Mahan, A. T. (1987). *The influence of sea power upon history, 1660-1783*. Dover Publications. ISBN-13: 978-0486255095

- Maurer, T. (2018). *Cyber Mercenaries: The State, Hackers, and Power* (1st ed.). Cambridge University Press. ISBN-13: 978-1107127609
- Mearsheimer, J. J. (2016). Structural realism. In T. Dunne, M. Kurki, & S. Smith (Eds.), *International Relations Theories: Discipline and Diversity* (4th ed.). Oxford University Press. ISBN: 9780198707561
- Morgenthau, H. J. (1978). *Politics Among Nations: The Struggle for Power and Peace* (5th Edition ed.). Knopf. ISBN-13: 978-0394500850
- Mumford, A. (2013). *Proxy Warfare* (1st ed.). Polity. ISBN: 978-0745651194
- Nye, J. (2010, May). *Cyberpower*. Harvard Kennedy School: Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf
- Nye, J. S. (2011). *The Future of Power*. Public Affairs. ISBN-13 : 978-1610390699
- Pakharenko, G. (2015). Cyber Operations at Maiden: A First-Hand Account. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (pp.59-66). NATO CCD COE. https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/
- Rattray, G. (2009). An environmental approach to understanding cyberpower. In F. Kramer, S. Starr, & L. Wentz (Eds.), *Cyberpower and National Security* (pp. 253-274). National Defense University Press. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-10.pdf?ver=2017-06-16-115053-850
- Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. DOI: 10.1017/CBO9781139169288
- Spykman, N. J. (1944). *The geography of the peace*. Archon Books. ISBN-13: 978-0208006547
- Thomas, T. (2009). Nation-state cyber strategies: examples from China and Russia. In *Cyberpower and National Security*. Protomac Books, Inc. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-20.pdf?ver=2017-06-16-115054-850
- Thucydides. (1974). *History of the Peloponnesian war* (M. I. Finley, Ed.; R. Warner, Trans.). Penguin Publishing Group. ISBN: 9780140440393
- Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations*. CCDCOE Publications. https://ccdcoe.org/library/publications/international-cyber-incidents-legal-considerations/
- Weedom, J. (2015). Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (pp.67-77). NATO CCD COE. https://ccdcoe.org/uploads/2018/10/Ch08_CyberWarinPerspective_Weedon.pdf
- Westenhoff, C. (2002). *Military Air Power: The CADRE Digest of Air Power Opinions and Thoughts*. University Press of the Pacific. ISBN-13 : 978-1410201454
- Yichang, L. (1993). *On High-Tech War*. Military Sciences Publishing House: Beijing.
- Ziolkowski, K. (2013, December). *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*. NATO CCD COE. https://ccdcoe.org/library/publications/peacetime-regime-for-state-activities-in-cyberspace/

Other

- Anonymous hacker attack on Israeli websites 'causes little real damage'. (2013, April 8). *The Guardian*. https://www.theguardian.com/technology/2013/apr/08/anonymous-hacker-attack-israeli-websites
- Anonymous TV. (2022, March 10). *Release: Roskomnadzor*. Twitter.com. https://twitter.com/YourAnonTV/status/1501942349550653443?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1501942349550653443%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.jpost.com%2Fbreaking-news%2Farticle-700940
- Arimatsu, L. (2012). *A treaty for governing cyber-weapons: Potential benefits and practical limitations*. 4th International Conference on Cyber Conflict. https://ccdcoe.org/uploads/2012/01/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf
- Arms Control Association. (2020, August). *Nuclear Weapons: Who has what at a Glance*. https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat
- Barnett, J. (2019). *Formbook Information Stealer*. Infoblox. https://www.infoblox.com/wp-content/uploads/threat-intelligence-report-formbook-information-stealer.pdf
- Beale, J. (2022, February 26). Ukraine: Is Russia's invasion going as expected? *BBC*. https://www.bbc.com/news/world-europe-60539113
- Bodeau, D. J., Fabius, J., & Graubart, R. D. (2010, August). *How Do You Assess Your Organization's Cyber Threat Level?* The MITRE Corporation. https://www.mitre.org/publications/technical-papers/how-do-you-assess-your-organizations-cyber-threat-level
- Borghard, E., & Lonergan, S. (2016, July 1). *Can States Calculate the Risks of Using Cyber Proxies?* Foreign Policy Research Institute. https://www.fpri.org/article/2016/07/can-states-calculate-risks-using-cyber-proxies/
- Chanlett-Avery, E., Rosen, L. W., Rollins, J. W., & Theohary, C. A. (2017). *North Korean Cyber Capabilities: In Brief*. Congressional Research Service.
- Choucri, N., & Reardon, R. (2012, April 01). *The Role of Cyberspace in International Relations: A View of the Literature*. Paper Prepared for the 2012 ISA Annual Convention. https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf
- Christou, G. (2017, Spring/Summer). The EU’s Approach to Cyber-Security. *University of Essex Online Paper Series*, pp. 1-13. http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf
- Clayton, M. (2014, June 17). Ukraine election narrowly avoided 'wanton destruction' from hackers. *Christian Science Monitor*. https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers
- Committee on National Security Systems (CNSS) 4009. (2015, April 06). *Glossary*. Strategic Environmental Research and Development Program. https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary
- Conficker Working Group. (2011, January). *Conficker Working Group: Lessons Learned Document*.

http://docs.media.bitpipe.com/io_10x/io_102267/item_465972/whitepaper_76813745321.pdf

- Council of Europe. (2001, November 23). *Convention on Cybercrime (ETS No. 185)*. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
- CrowdStrike. (2015). *2015 Global Threat Report*. https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf
- *Cyber-Attack Against Ukrainian Critical Infrastructure | CISA*. (2016, February 25). US-CERT. https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01
- Department of Defence. (2011, July). *Department of Defense Strategy for Operating in Cyberspace*. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf
- *Doctrine of Information Security of the Russian Federation*. (2000). MFA Russia. https://www.mid.ru/en/main_en
- Espionage Report: Merkel's China Visit Marred by Hacking Allegations. (2007, August 27). *Spiegel*. https://www.spiegel.de/international/world/espionage-report-merkel-s-china-visit-marred-by-hacking-allegations-a-502169.html
- Ferdinando, L. (2018, May 4). CYBERCOM to elevate to combatant command | Article | The United States Army. *U.S. Army*. https://www.army.mil/article/204771/cybercom_to_elevate_to_combatant_command
- Frances, K. (2022, March 5). Putin says Western sanctions are akin to declaration of war. *Reuters*. https://www.reuters.com/world/europe/putin-says-western-sanctions-are-akin-declaration-war-2022-03-05/
- Fruhlinger, J. (2020, January 09). *What is a false flag? How state-based hackers cover their tracks*. CSO. https://www.csoonline.com/article/3512027/what-is-a-false-flag-how-state-based-hackers-cover-their-tracks.html
- Fung, B. (2015, May 14). The Syrian Electronic Army just hacked the Washington Post (again). *The Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2015/05/14/the-syrian-electronic-army-just-hacked-the-washington-post-again/
- Fung, B. (2021, August 16). Colonial Pipeline says ransomware attack also led to personal information being stolen. *CNN*. https://edition.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html
- Gatlan, S. (2022, March 5). Russia shares a list of 17,000 IPs allegedly DDoSing Russian orgs. *Bleeping Computer*. https://www.bleepingcomputer.com/news/security/russia-shares-list-of-17-000-ips-allegedly-ddosing-russian-orgs/?&web_view=true
- Gatlan, S. (2022, March 11). Russian defense firm Rostec shuts down website after DDoS attack. *Bleeping Computer*. https://www.bleepingcomputer.com/news/security/russian-defense-firm-rostec-shuts-down-website-after-ddos-attack/
- Giles, K. (2015, July 31). *Putin's troll factories*. Chatham House. https://www.chathamhouse.org/publications/the-world-today/2015-08/putins-troll-factories

- Hang, R. (2014, October). Freedom for Authoritarianism: Patriotic Hackers and Chinese Nationalism. *The Yale Review of International Studies*. http://yris.yira.org/essays/1447
- Harrington, D. (2021, October 25). *Zero-Day Vulnerability Explained*. Varonis. https://www.varonis.com/blog/zero-day-vulnerability/
- Heath, B., Timmons, H., & Cooney, P. (2021, February 14). SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president. *Reuters*. https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R
- The hidden history of cyber-crime forums. (2017, September 6). *BBC*. https://www.bbc.com/news/technology-40671091
- Hvistendahl, M. (2010, March 3). China's Hacker Army. *Foreign Policy*. https://foreignpolicy.com/2010/03/03/chinas-hacker-army/
- Keller, B. (1989, June 5). 500 on 2 Trains Reported Killed By Soviet Gas Pipeline Explosion (Published 1989). *The New York Times*. https://www.nytimes.com/1989/06/05/world/500-on-2-trains-reported-killed-by-soviet-gas-pipeline-explosion.html
- Kelly, H. (2012, August 03). 83 million Facebook accounts are fakes and dupes. *CNN Business*. https://edition.cnn.com/2012/08/02/tech/social-media/facebook-fake-accounts/index.html
- Krebs, B. (2008, October 16). Security Fix - Report: Russian Hacker Forums Fueled Georgia Cyber Attacks. *The Washington Post*. http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html
- Landler, M. (2010, January 21). Clinton Urges Global Response to Internet Attacks. *The New York Times*. https://www.nytimes.com/2010/01/22/world/asia/22diplo.html
- Langer, R. (2016). Cyber Power - An Emerging Factor in National and International Security - CIRSD. *Center for International Relations and Sustainable Development*. https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-international-security
- Love, D. (2013, May 22). 10 Reasons To Worry About The Syrian Electronic Army. *Business Insider*. https://www.businessinsider.com/syrian-electronic-army-2013-5?op=1#ixzz2h728aL8P
- Makrushin, D. (2017, March 23). The cost of launching a DDoS attack. *Securelist*. https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/
- Markoff, J. (2009, May 30). Contractors Vie for Plum Work, Hacking for US. *The New York Times*. https://www.nytimes.com/2009/05/31/us/31cyber.html
- Markoff, J., & Shanker, T. (2009, August 1). Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk (Published 2009). *The New York Times*. https://www.nytimes.com/2009/08/02/us/politics/02cyber.html
- Masters, S. (2014, March 5). Ukraine crisis: Telephone networks are first casualty of conflict. *The Independent*. https://www.independent.co.uk/news/world/europe/ukraine-crisis-telephone-networks-are-first-casualty-of-conflict-9171771.html
- Maurer, T. (2016, March 3). *Internet Freedom and Export Controls :Briefing before the Commission on Security and Cooperation in Europe*. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Tim_Maurer_final_briefing_-_03.03.20162.pdf

- Microsoft Security Tech Center. (2017, November 11). *Microsoft Security Bulletins*. microsoft.com. https://docs.microsoft.com/en-us/security-updates/securitybulletins/securitybulletins
- Musotto, R., O'Shea, B., & Haskell-Dowland, P. (2021, July 7). Holding the world to ransom: The top 5 most dangerous criminal organizations online right now. *GCN*. https://gcn.com/cybersecurity/2021/07/holding-the-world-to-ransom-the-top-5-most-dangerous-criminal-organizations-online-right-now/315611/
- Newman, L. H. (2021, December 8). A Year After the SolarWinds Hack, Supply Chain Threats Still Loom. *WIRED*. https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/
- Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*. Proceedings of the 7th European Conference on Information Warfare. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
- Perlroth, N. (2014, December 2). Reinventing the Internet to Make It Safer. *Bits, The New York Times*. https://bits.blogs.nytimes.com/2014/12/02/reinventing-the-internet-to-make-it-safer/?mtrref=www.google.com&as&mtrref=bits.blogs.nytimes.com&gwh=4BF8EC8B11C193BCDB3DF66D48E15211&gwt=pay&assetType=PAYWALL
- Riley, M. (2014, July 21). How Russian Hackers Stole the Nasdaq. *Bloomberg*. https://www.bloomberg.com/news/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq
- Roberts, P. (2012, September 25). UK's top ecrime investigator describes a life fighting cybercrime. *Naked Security*. https://nakedsecurity.sophos.com/2012/09/25/interview-bob-burls/
- Rosen, K. R. (2022, February 15). 'Kill Your Commanding Officer': On the Front Lines of Putin's Digital War With Ukraine. *Politico*. https://www.politico.com/news/magazine/2022/02/15/10-days-inside-putins-invisible-war-with-ukraine-00008529
- Samuel, A. (2004, March 4). *Hacktivism and the Future of Political Participation A thesis presented by Alexandra Whitney Samuel to the Department of Governm*. Harvard University. https://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf
- Sanger, D. E., Schmidt, M. S., & Perlroth, N. (2014, December 19). Obama Vows a Response to Cyberattack on Sony (Published 2014). *The New York Times*. https://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html
- Schrank, P. (2007, August 30). A walk on the dark side. *The Economist*. https://www.economist.com/unknown/2007/08/30/a-walk-on-the-dark-side
- Shevchenko, V. (2014, December 20). Ukraine conflict: Hackers take sides in virtual war. *BBC*. https://www.bbc.com/news/world-europe-30453069
- Sommer, P., & Brown, I. (2011). *Reducing Systemic Cybersecurity Risk*. OECD/IFP Project. https://www.oecd.org/governance/risk/46889922.pdf
- The State Council of the People's Republic of China. (2016, December 27). *State Council releases five-year plan on informatization*. http://english.www.gov.cn/policies/latest_releases/2016/12/27/content_281475526646686.htm
- Stevens, W., & Westcott, A. (1920). *A History of Sea Power*. Doran Company: New York. https://www.gutenberg.org/files/24797/24797-h/24797-h.htm

- Tidy, J. (2020, September 18). Police launch homicide inquiry after German hospital hack. *BBC News*. https://www.bbc.com/news/technology-54204356
- Tiezzi, S. (2014, February 28). Xi Jinping Leads China's New Internet Security Group. *The Diplomat*. https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/
- United Nations Publication, E.10.IV.6. (2010). *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*. UNODC. https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf
- United States, White House, & Obama B. (2011, May 1). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
- *U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts*. (2017, March 15). U.S. Department of Justice. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions
- U.S. Department of Justice. (2016, March 24). *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector*. https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged
- Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., & Schwarzenbach, A. (2020, September 4). *National Cyber Power Index 2020*. Belfer Center, Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf
- *What Is Open Source Intelligence and How Is it Used?* (2019, February 19). Recorded Future. https://www.recordedfuture.com/open-source-intelligence-definition/
- Zetter, K. (2014, November 03). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *Wired*. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/