Department of Political Science

Bachelor's degree in Politics, Philosophy and Economics

Chair of International Relations

Non-State Actors & Cyber-Warfare

Dr. Raffaele Marchetti | Supervisor

ISMAIL EL GATAA – N. 092012

ACADEMIC YEAR 2021/2022

Acknowledgments

This work is the last step of my journey as a bachelor's student at Luiss University. A journey filled with unforgettable experiences, made of growth both as a future professional as well as a human being. I will be forever grateful for this lifechanging opportunity.

I would like thank Professor Raffaele Marchetti, who kindly accepted to be the supervisor for this last task and whose course of International Relations caught my deepest interest and passion.

I would also like to express my gratitude to Professor Antonio Calcara, who kindly supported me through the conceptualization and development of this thesis.

Finally, I deeply thank my father, Abdelahad El Gataa, who believed in me when no one did, who always supported me chasing my dreams, in addition to thanking my mother, Raja Tir, who sacrificed so much to enable me attain a better life, while lifting me up during my darkest nights.

You made of me the biggest investment of your lives and I wish this achievement repays, even partly, all the efforts you have put into me.

Table of Contents

Introduction

This thesis offers an analysis of the growing use of non-state actors in cyberwarfare. With the Covid pandemic, which pushed societies towards an increased use of digital services and with the policymakers' realization that an ecological transition necessitates of a digital transition, the importance of the digital domain in our lives has known a dramatic expansion in the last few years.

The first chapter introduces the early 21st century developments of a market for zero days vulnerabilities, therefore giving economic incentives to both hackers and companies. In term, this phenomenon was crucial in the growth of non-state actors in cyberspace. Moreover, the chapter makes important clarifications regarding terminology and understanding the basis of cyberspace, which is paramount in order to understand the arguments put forward.

The second chapter takes a deeper look at one of the most important incentives behind the proliferation of non-state actors in the digital world, the attribution problem, as it often guarantees plausible deniability to state and non-state actors. Moreover, it dives deeper into a historical analogy between the role of non-state actors in cyberspace and the role of privateers in the high seas during the mercantilist era. This analogy helps us understand the hybrid role that non-state actors play vis a vis state security and sovereignty. Finally, this chapter thoroughly explains the operational roles and actions taken by non-state actors in cyberwarfare.

The third chapter offers two case studies, the United States of America and the Russian Federation. These cases show us how the operational roles offered by non-state actors change based on the specificities of the state hosting them. An central argument advanced by the thesis is that domestic political and economic structure influences state-non-state actor relations, their roles and activities in cyber-warfare.

Finally, the concluding chapter reflects on the future steps that will, arguably, change the scope and potential of cyber-warfare, and the role that non-state actors have in them. New technologies are expanding the existing cyber space and enhancing it with new capabilities and new opportunities for non-state actors to thrive.

First Chapter

During the early 2000s, many individual hackers would post on blogs their findings of vulnerabilities, earning little more than bragging rights. However, one company named iDefense decided to differentiate itself from the others: they started giving rewards in exchange of information about zero days vulnerabilities. They would get the information from the supplier that discovered zero days, and then inform their clients of such vulnerabilities so they could fix them.[1] This business model became a massive success and revolutionized the role of non-state actors in cybersecurity.

Since the creation of this market for zero days, their use for the development of cyberweapons, and the discovery of the potential scope of this new domain, many states started developing their capacities to conduct offensive and defensive cyber operations, but to do so they had to know the origins of the vulnerabilities. For instance, after the success of iDefense, the US government started contacting them in order to get an exclusive access to these vulnerabilities, to defend themselves and being capable of attacking others.

Nevertheless, that was not enough to protect the security of the state. Nowadays, the cyberweapons developed by the United States, which were arguably the most advanced, have spread around the world, and have become generalized even in less developed countries, such as North Korea. For instance, in 2017, a hacker group named the "Shadow Brockers" unleashed the American NSA's Tailored Access Operations (TAO) hacking tools, therefore providing it for the entire world to use. This leaked weapon can exploit weaknesses in a number of network hardware platforms and other devices.

Moreover, the importance of the digital world stems not only from the increased economic efficiency and global opportunities brought by the digital revolution, but it is extremely important for security purposes and for the ecological transition to net zero by 2050.

[1] Yaman Roumani, Patching zero-day vulnerabilities: an empirical analysis, Journal of Cybersecurity, Volume 7, Issue 1, 2021.

It is undeniable to state that the future economic relations will be increasingly centered around the digital and ICT domains. Hence, giving crucial importance to big data providers, cloud services, hyperscalers has become a priority to both the state and, of course, to the industry itself: what is today called in policy debates the "dual transition". Big tech companies are increasingly trying to protect themselves from cyberattacks stemming from both state and non-state actors. Thus, a policy discussion has emerged regarding the degree to which businesses may defend themselves against state-sponsored attacks and the appropriateness of private players engaging in retaliatory hacking.[2]

Based on the intention and capacity of the attacking state, as well as the defensive capabilities of the enterprise, a private company could be capable of protecting itself from a state-directed attack. A corporation with a high level of cybersecurity maturity may be able to deter an attacker by making itself a difficult target if it is a generic target. However, when a committed, well-financed state directly targets private companies, their defensive capabilities are lacking.

On the other side, the discussion of hacking back frequently omits to describe the potential goals of such an action for a private firm. Is it to make the assailant pay a price? Is it to aid in identifying the actor(s) responsible for the attack? Is it to investigate the attack's motives? It is unknown to what extent private actors would consider offensive or retaliatory measures against an attacker to be in their interests, given the ambiguity behind the consequences of such an act. The US government however (officially) discourages corporate hacking back by asserting that it is prohibited by the Computer Fraud and Abuse Act and by emphasizing the risk of escalation.[3]

Despite the ongoing debate, we can still infer that non-state actors play an unprecedented role in cyberwarfare. Now the question seems clear: what are the roles and the actions taken by them in this domain? And how do non state actors: terrorist groups, hacker individuals/groups, private/public firms and rogue actors, affect the power relations and payoffs in cybered warfare?

[2] Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures," Stanford Journal of International Law 103 (2014).
[3] Tiffany Curtiss, *"Computer Fraud and Abuse Act enforcement: cruel, unusual, and due for reform"*, Washington Law Review (Vol.91, Issue 4).

During the last thirty years, the internet evolved from being perceived as an innovative and inoffensive technology that promised to achieve the peaceful end of creating bridges between distant territories, increasing communication, and connecting humanity, to becoming a question of national security and, we hear, the new frontier for geopolitical conflict. Cyberspace and its different ramifications have opened new avenues of conflict, added several levels of complexity to existing power balances, and become increasingly influential in the strategic calculus of several major powers in the international system.

With the development of internet, and the widespread adoption of cybernetworks and computers in all parts of human activity, it was clear that what brought great economic advantages, would have become the center of a new landscape for conflict: cyberwarfare. Following the classic Clauswitzian argument, war is "nothing but a continuation of political intercourse, with a mixture of other means," and "an act of violence intended to compel our opponent to fulfill our will." And as of today, cybernetworks became so integral to everyday tasks that any action compromising critical infrastructure would not only harm the targets but may cause the failure of mechanisms crucial for the maintenance of everyday life.

Although being created to satisfy military communication purposes, the internet was developed and enhanced by private actors. For instance, the first cyber-emergency response was caused by the Morris worm, which was developed by a graduate student, not a military (quote?). However, with commercialization and widespread use of internet in the 1990s, some militaries' interest rose up, seeing it as a platform capable of far-reaching power projections. Indeed, cyber warfare has overarching potentialities, as it is a new dimension of conflict capable of leapfrogging borders and teleporting the chaos of war to civilians thousands of miles beyond the front. In term, it will have major effects on the physical, economic and societal security of nations.

In fact, since when non state actors developed offensive cyber capabilities, hackers are the masters of this new space, which made them find allies in governments and investors. Alexander Klimburg, director of the Global Commission on the stability of cyberspace stated, *"to create an integral national capability in cyber power, the non-state sector must be induced to cooperate with government".* All of those causes lead to a specific outcome: non-state actors play more than ever a crucial role in this new battlefield.

More than ever before, it has become clear that the threat stemming from hacking goes beyond vandalism, criminal activities, or even espionage, hence including the sort of physical-world disruption that was once possible to accomplish only with military attacks and terroristic sabotage.

The research questions of this thesis are: what is the role of non-state actors in cyberwarfare? Why do non-state actors play a critical role in cyberspace? What is the relationship between the State and non-state actors in this domain?

These questions are crucial as we are living in a time of deepened digitalization, an inflection point in history during which more and more crucial infrastructure is connected to a space which is dominated by non-state actors, while the state is incapable of offering full protection to the agents present in it. Moreover, with regards to domain of International Relations, this topic is of heightened importance, as the proliferation of non-state actors combined with the cruciality of cyber infrastructure has a direct impact on the competition between super-powers. Due to issues related to the attribution of cyber-attacks, which will be analyzed further in the next chapter, and the unclear stance of international law, this phenomenon is capable of creating instability in the power relations between them. If, for instance, Russian cyber-militias move independently from the Russian state, attacking crucial infrastructure of another state, will inevitably cause great tensions between the two, as the victim will not be capable of fully asserting the complicity and responsibility of the Russian Federation in the attack.

Therefore, studying the policy pursued by states in terms of relations with cyber non-state actors is of the utmost relevance. In this thesis we will look at how the United States of America and the Russian Federation manage and use non-state agents in the domain of cyberwarfare. The findings are interesting, as they show that these two states are arguably opposites in this policy choice. The Russian policy is characterized by a loose control over cyber proxies or militias, whereas the United States' policy is defined by the tight administration of what these actors can and cannot do. We will dive deeper later.

Conceptual clarifications

Cyberweapons, given their unclear legal stance and their inexpensive nature -taking into consideration economic but also political costs- and the potentially colossal damage they could

cause, are often perceived as instruments to pursue political goals, outside the realm of direct armed conflict.

Before starting our analysis however, due to the complexity of the topic we need to clarify two key concepts: what do we mean by cyberwarfare and its legal nature. In order to answer those questions, the chapter draws on the existing literature on cybersecurity studies.

First of all, we must recognize that there is no widely adopted definition of cyberwarfare and that terminology is still broadly defined, such as the differentiation between cyber war and cyber-warfare.[4] Therefore, we must start from the basics and specify what do we mean by cyberspace. Due to its depth, precision and usefulness it has in our analysis, we employ the definition provided by Dr. Daniel Kuehl, which defines cyberspace as a *global domain within the information environment whose distinctive and unique character. Is framed using electronics and electromagnetic spectrum, to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies*" (quote). We can also **complement this definition with the one provided by** the Committee on National Security Systems on cyberattacks: *"an attack via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disability, destroying, or maliciously controlling a computing environment or infrastructure, or destroying the integrity of the data or stealing controlled information"*.

We chose these definitions as they are specific enough to entail different types of activities entertained by public or private actors in the cyberspace, while keeping an open window to the possibility of widespread use of non-state actors in that domain. However, there is an added complexity to cyberwarfare: it is not effectively a domain of conflict, unlike the physical world (sea, land or air), but it is a substrate. This means that cyberspace is in fact a built environment, which is imagined, created, developed, sustained and extended by human intentions and actions. Therefore, it can be unbuilt, remodeled and perhaps even destroyed.

To illustrate this idea, take in consideration the role of cloud. The computers that make up cloud services are servers that create connections between different devices, far apart from each other. This continuous exchange of information, data and storage capability is what makes the basis of the cloud service. However, just like this space has been built and connected to the

[4] Robinson et al, "*Cyberwarfare, issues and challenges",* March 2015, page 12.

worldwide web, it can be unbuilt and de-connected, perhaps even destroyed. The same principle applies in general to cyberspace.

Regarding the international law behind cyber-attack, there has never been any international convention or agreement stipulating norms and/or provisions regulating them, making this debate much trickier. Indeed, it is not clear if a cyberattack should be considered generally as a prank, a crime, an act of terrorism, or act of war. However, some states have expressed that cyberattacks on their essential infrastructure by another nation state would be deemed an act of war, such as the United States of America. This fact supports the presence of non-state actors as state-caused cyber-attacks might be seen as an act of war, while if a hacker group is engaged it might be seen as terrorism or a ransomware rather than an act of war.

Hence, this is what encourages states to develop their relationships to non-state actors. In many cases it is the logic of profit and of the pursue of strategic political goals at the least possible cost that pushes for a cooperation between the state institutions and non-state actors in this domain. However, one of the most important issues in this sense is the *attribution problem.*

Classifying non-state actors in cyberwarfare

For the purposes of analyzing and developing in a clear manner the case studies we need to pin down a classification, definition, and examples of the relevant non-state actors operating in cyberspace. For reference, we need to remember that these definitions are ever changing and might not be fully representative in the next years, as we are living during an inflection point, in which the nature of internet and cyberspace is changing dramatically.

Cyberspace is a global domain, available for almost anyone with access to a computer with an internet connection, a smartphone or any other type of uplinked multimedia device. In this space, the individual represents an important hub of knowledge and technical skill. Today's technological developments give the possibility to any skilled-enough individual to act autonomously. **Individual hackers**, ICT experts and engineers may serve, formally or informally, as agents of a state. For instance, hackers working contracting for the Russian group VoidBalaur are a clear example of it5. Moreover, individual hackers may be used on a case to case basis. These contracting operations stem from single hacking operations to gathering

[5] Trend Micro Research, *Void balaur and the rise of the cybermercenary industry,* 2021.

information. Indeed, bug hunters are increasingly used in order to find software vulnerabilities, selling their services to big corporations such as Netragard which may resell the findings to any willing buyers.[6] For instance, Stuxnet was based on the exploitation of several vulnerabilities, most likely bought from bug hunters in the digital black market.

The capacity of a **single individual** to produce and use cyberweapons, and the loose command and control structure of many hacker groups, give to the individual an essential role. More and more automated attack tools are available, which push down the knowledge needed to cyberattack or find vulnerabilities in software. Cyberwarfare is so pervasive, that even common citizens may passively participate in conflicts. For instance, zombified computers are devices that have been compromised by hackers, thanks to the voluntary or involuntary contribution of a common worker. Therefore, they provide their devices to being remotely used by hackers for their purposes.[7]

Criminal organizations have flourished in cyberspace, by applying the same command and control structure and hierarchy of crime syndicates, partly thanks to the lack of regulation in this new domain. The digital manifestation of these organizations, based exclusively (or quasi) on financial interests gives the state the chance of using them to pursue political goals.[8] Russian Business Network for instance is a criminal organization that is likely to have taken part in the cyber attacks leading to the Russian invasion of Georgia.[9] These groups may include **cyber mercenaries**, which are groups composed of highly skilled individuals capable of sophisticated cyber operations. Their motivation is usually exclusively economic and their services may be sold to both public or private actors.[10]

Hacktivists are ideologically driven groups, that have the goal of influencing, furthering or shaping the political agenda of the polity. Indeed, the existence of these organizations is made possible by the digitalization of the public debate, which transferred the exchanging of political ideas to the world of digital platforms. For instance, the famous groups Anonymous, as its operations are grounded on cyber countercultures, such as the operation.[11]

---

[6] Rob Lemos, *"How to use bug bounties with penetration testing to bolster your app security",* 2017.
[7] Raymon Gozzi, ETC: A Review of General Semantics, Vol. 57, No. 3 (Fall 2000), pp. 349-352, 2000.

[8] David P Stewart, *International and Transnational Criminal Law, 505, 2010.*
[9] H. Schell, *Hackers and Hacking: a reference handbook*, 223-224, 2013.
[10] N. Bussolati, *The rise of non-state actors in cyberwarfare,* 102-126, 2015
[11] Ibid

Patriotic hackers are not particularly different from hacktivist groups, the difference stems from the fact that the former are exclusively driven by a patriotic devotion to defend the interests of their country. Vladimir Putin stated that patriotic hackers were beneficial to the Russian Federation, as they were defending the interests of the nation, however, we will focus more on Russia in the next chapters.[12]

Hackers are people with deep knowledge and thorough understanding of computer technology, and how computer hardware, software and networking interact. They may be motivated by a multitude of incentives, such as curiosity, economic gain, political agendas, attraction to technical challenge, or pure boredom. However, contemporary categorizing of hackers by intent and motivation is usually done by "hat color".[13]

Black-hat hackers are the malevolent types of hackers originally dubbed "crackers". They are people who exploit computer systems and networks for their own benefit. They may also release malware that destroys files, holds computers hostage, or steals passwords, credit card numbers, and other personal information. Hacking can operate like big business, the scale of which makes it easy to distribute malicious software. Organizations boast partners, resellers, vendors, and associates, and they buy and sell licenses for malware to other criminal organizations for use in new regions or markets. Some black hat organizations even have call centers, which they use to make outbound calls, pretending to work for a well-known technology organization such as Microsoft. In this scam, the hacker tries to convince potential victims to allow remote access to their computers or download software.[14]

White-hat hackers, or "ethical hackers", are hackers who have high moral standards, relative to common societal norms. They specialize in penetration testing and validation methodologies in order to ensure the security of an organization's information systems, and are commonly employed by government agencies or by companies specializing in information security consulting. [15]

---

[12] Ibid
[13] Johan Sigholm, "*Non state actors in cyberspace operations"*, Swedish National Defence College, 15.
[14] Kaspersky, Black Hat, White Hat and Gray Hat Hackers.
[15] Johan Sigholm, "*Non state actors in cyberspace operations"*, Swedish National Defence College, 16.

Gray-hat hackers are hackers who conform to white-hat standards most of the time, but who may also wear a metaphoric black hat occasionally. For example, if their interests are targeted by an attack, they might opt to take the matter into their own hands. For instance, the famous hacker organization Anonymous can be viewed as a gray hat hacker organization. As it puts itself as an organization fighting for "world justice", despite protecting its own interests when they are threatened or put at risk by other actors.

Furthermore, as all cyberattacks are made possible by a "zero day", which is an open vulnerability in a software that has not yet been identified or fixed by the software developer, a small but significant amount of zero days are purposely communicated to the potential attacker by an insider actor. These actors are generally divided in two categories: **Cyber Insiders** and **Cyber espionage agents**.

The *former* are characterized by their legitimate access to computer and network resources, including information residing in associated systems, and their disloyalty to their employer, hiring party or political branch, and are willing to betray them for monetary benefits or other reasons.[16] The cyber insider may plant logical bombs or open backdoors in programs they help develop, or steal sensitive data by use of small, portable and easily concealed storage devices. As we can infer, this threat is unlike other vulnerability-based attacks, as any illicit actions instigated by a cyber insider will thus not be perceived as anomalous by intrusion detection systems, logging or expert systems, making them highly difficult to mitigate.

On the other hand, **cyber espionage agents** have the goal of infiltrating organizations or/and intercepting intercept information that passes through, or resides in, computer networks or computer systems of special interest, by using cracking and infiltration techniques, software and hardware tools for surveillance, or other means. Cyber spies might be part of intelligence organizations, such as a secret police service, or hired by governments or non-state actors in order to attain some goals set in contracts.

Moving towards more complex non-state actors present in the realm of cyberwarfare, the first ones to be taken in consideration are **Cyber-militias**. They may be defined as a group of volunteers, often civilians with special skills and pushed by political motives, who are willing

[16] *Ibid*.

and able to use cyberattacks, do not get any monetary rewards for their services, nor are they bound by any contractual obligation. We must note that the involvement of civilians in recent cyber-conflicts has created a sizeable gray area between hacktivists, political hackers and legitimate combatants backed by nation-states. The debate has been fierce concerning if these people are individual and independent actors, motivated by political or nationalistic goals, or participants in covert government-orchestrated campaigns with the purpose to further the strategic political or military objective of the instigating state.[17]

Finally**, Private firms,** which are increasingly providing automated hacking capabilities to governments and firms, which are exponentially more prevalent and efficient. and in the future with quantum computers the trend might just increase. The presence of hundreds of giants in cybersecurity and the bigger stakes in the domain made more and more states keen on either investing in cybertechnologies, thus creating a full industrial background, or hiring specialized non state actors as proxies of the state.

Cyberwarfare has become growingly present in all three levels of security: tactics, operations and strategy. Many incidents have confirmed that criminals, hackers, and government sanctioned specialists can wreak havoc on governments, military communication systems and corporation.[18] In the next chapter we will look at the roles and actions undertaken by the aforementioned actors, while analyzing two case studies for non-state actor's cyber-warfare policy.

Second chapter

[17] Applegate, S. D., "*Cybermilitias and Political Hackers: Use of Irregular Forces in cyberwarfare*," IEEE Security & Privacy, Volume 9, Issue 5, Sep.-Oct. 2011.

[18] Dombrowski, Demchak, Cyber war, cybered conflict and the maritime domain, Naval War College Review , Vol. 67, No. 2 (Spring 2014), pp. 70-96.

In this chapter we will analyze three pivotal points of this thesis: the attribution problem and the operational role of non-state actors in cyber-warfare, while offering a historical analogy between XVIIIth century privateers and today's cyber-proxies.

The attribution problem

In the physical world, when a nation state is attacked by air, land or sea, it is in most cases capable of understanding who or what is attacking it, making the process of decision making clear and straightforward. In the cyberspace, the process of attribution is much more complicated, making the decision-making process stemming from an attack much more confused as the state or entity attacked has difficulties understanding what is happening and who is responsible, making the process much more politicized: attribution is what states make of it.[19] This is crucial in understanding why the use of non-state actors in the cyberspace as proxies has known a dramatic increase:

Attribution is one of the most intractable problems, it is the process of defining what actor or agent did what, in what space, how and why. Only a technical redesign of the internet, consequently, could fully fix the problem but this would lead to other problems. Meanwhile, human lives and security of the state may depend on ascribing agency to an agent. Attribution is effectively about matching an offender to an offence, and is almost all the time too large and too complex for a single person to manage, while it might have enormous stakes at play.

Furthermore, as cyber threats have reached a high level of complexity and automation, executing and uncovering their architecture requires refined division of labor, thus making it a team work. Based on Dr. Buchanan's study, it is an art as much as a science, as there is no single methodology that works, and has no black or white solution. In practice, the attribution is a process in minimizing uncertainty on three levels: tactical, operational and strategical. The tactical goal is understanding the technical side of the attack, the how. Meanwhile, the Operational goal, is understanding the high-level architecture and the profile of the offender, the what. Finally, the strategic goal is to understand the attack's reasons and motivations, the why and the who.[20]

[19] T. Rid & B. Buchanan, *Attributing cyber attacks*, Journal of strategic studies, 2014, p.6.
[20] *Ibid.*

With regards to this last point, it is helpful to keep track of the trials, damages and failures of different attacks, as the amount of damage caused or threatened frequently is revealing of the resources invested by the attacker, which also defines the resources that will be put into place for attribution purposes. Finally, communicating the outcome of the attribution process must not be left as a low priority, as it can have deep effects on the behavior of the offenders.

Cyberwarfare enters into play at all three levels and connects them iteratively and systematically. At the strategic level, national policies must provide commanders with the goals of cybered conflict. At the tactical level, commanders must fight battles using not only kinetic means but also offensive and defensive cyber instruments. All three levels overlap during military operations, and in the case of cyberwarfare the rule doesn't bend. Attribution is one of the most intractable problems, specifically targeting analysis may reveal the attackers' intentions, assumptions and how much it values the target, based on how many resources were put into place.

However, today's challenge is between discerning if an attack is perpetrated by a state or a non state actor in a politically timely manner. Indeed, in case of attack to crucial infrastructure, political institutions are expected to respond in a timely manner, which entails knowing who is the target, which is not as easy as it seems. The use of non-state actors in cyberwarfare, due to the attribution problem give plausible deniability to nation states, created an arms race in cyberspace, and a massively exploding new cyber industrial complex. Nevertheless, some countries created doctrines in order to respond to this issue. For instance, France's attribution doctrine is based on the principle of "host's responsibility", meaning that if a non-state actor is causing damage to French infrastructure from a specific country, it is the country's institutional responsibility to prevent this attack from taking place and the state will be taken as accountable to the damages afflicted.[21]

Historical background of Non-State Actors, Cyberwarfare & Privateering

[21] *Élements publics de doctrine militaire de lutte informatique*, Ministére des Armées Français, 2019.

Throughout history, civilizations have been trying to expand their power, influence and wealth, often by waging war and conquering new territory. The competition led to innovation and development of new ways to wage war and assert control over a group of people or a landscape, from the use of gun powder to the invention of armored vehicles, all the way to modern unmanned drone strikes. As new domains are created and opened to conflict, as what happened after the invention of the aircraft, a race to dominate the aforementioned domain starts. Today, just like with the skies one hundred years ago, the emergence of cyberspace as a new domain has led to a growing competition between states and non-state actors.

Around 2006, the US and Israel launched Stuxnet against Iranian nuclear facilities, for the first time in history. Stuxnet led to physical damage to the facilities leading to the enrichment of uranium for nuclear purposes in Iran, and it helped delay by years the long-standing efforts of Iran in acquiring nuclear material. However, many incidents have confirmed that also criminals, random hackers, and government sanctioned specialists can wreak havoc on any kind of actor, such as military communication systems or corporations.

In 2015, at the North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence in Estonia, Adm. Mike Rogers stated "The seas around the world are, much like the cyber domain, not governed by one single nation". Indeed, two specific characteristics of cyberspace resemble maritime space, before the creation of global blue-water navies: the lack of international norms regulating the protection of commercial and private shipments, and the lack of capacity of the state to provide appropriate security to all the actors making use of international waters.

Just like in the sixteenth and seventeenth century, in the modern cyberspace, protection from threats has been treated as a quasi-exclusively private undertaking. In the era of mercantilism, maritime commercial companies operated by their own international policies, seeking protection from other companies or states, engaging in open warfare, piracy, and privateering. [22] Although being played in much smaller dimensions, the analogy between privateers and non-state actors in today's cyberspace is particularly pertinent. It sheds light on specific aspects of cyberwarfare, such as the blurred lines between state and non-state actors, the non-

[22] Egloff, Florian, Cybersecurity and the Age of Privateering, Georgetown University Press, 233.

differentiation between economic and military realms makes us understand the dynamics in a system which is characterized by a loose distribution of power.[23]

Privateering, being a lucrative undertaking, led to many of the ablest seamen choosing to serve as privateers rather than sailors of the navy. One of the biggest companies was the East Indies Company, effectively draining men away from the Royal navy during the eighteenth century. Today, large companies seek to attract some of the most skilled cybersecurity experts, creating a recruitment issue states faced during the mercantilist era. For instance, in June 2022, the European Union has approved new sweeping reforms of the digital space, the Digital Services Act and the Digital Markets Act. The latter, having the goal of targeting hyperscalers and gate-keepers in the digital market, is the first legislative file setting comprehensive standards for regulation of the digital space.[24] Nevertheless, the European Commission, the executive body of the European Union responsible for the monitoring and the implementation of the acts, is struggling to find the necessary skilled workers to fully execute its plans for the digital market.[25] Three hundred years ago, the Royal Navy addressed the competition for skilled labor by forcing sailors to join the navy and issuing limited privateering licenses.

Benefits of using Non-State Actors in Cyber-Warfare

Based on our previous historical analysis, we must answer one question: what are the benefits that state see in using non state actors in cyberwarfare today?

After research, we can conclude that using these actors has many different advantages. The first one is the capacity to **counterstrike.** Employing non-state actors to conduct cyberattacks might arouse suspicion in the eyes of the international community, but the absence of any concrete proof will shield the attacker from any political fallout. The risk of a counterattack is therefore minimal. The absence of attribution prevented Estonia or the NATO from retaliating in 2007 even though overwhelming evidence pointed to Russia as the source of the Distributed Denial of Service (DDoS) assaults on Estonia. The killing may have been carried out by a

[23] *Ibid.*
[24] Thierry Breton, Press Release, European Commissioner for the Internal Market, 5 July 2022.
[25] Thierry Breton, ITRE Committee exchange of views, 28 June 2022.

patriotic cyber militia at the direction of the Russian government, although Russia categorically denied any involvement.

Cost Factor. A well-organized cyber wing would be expensive to create as part of the armed forces or the government because it would require funding and uniformed people. The same operation can be completed for little to no money by enlisting appropriately motivated and technically skilled non-state actors. Small governments today have the ability to harm the vital infrastructure of much bigger and more powerful countries by funding such cybermilitias.

Sponsor Cyberwar. Unearthly alliances between non-state actors and state apparatus are possible when the former receives advanced capabilities from the latter in the form of cash or actual infiltration tools, which they can then transfer to another state or its non-state actors that desire to develop cyberwar capability. As of right now, there are no international conventions or regulations that prohibit such behavior. Therefore, funding a cyberwar by transferring such technologies through non-state actors is entirely lawful, or at the very least morally above board.

Freedom to Attack from Anywhere. Non-state actors are not required to be based in the nation that sponsors them. There are no limits in cyberspace. As a result, an attack with an attacker residing in a third nation can still be carried out with the same accuracy and impact. Due to the difficulty of attribution in these situations, attacking another country is now made considerably simpler. This is particularly a benefit of international Hacker-for-Hire (HfH).

International laws of War do not Apply. There is no Geneva convention on the use of cyber weapons, or international cyber humanitarian law. No laws of war apply to these cyber non-state actors, even if an undeniable connection between a non-state proxy and a nation-state is proven. This is due to the fact that such non-state actors cannot be regarded as fighters under the law. Additionally, certain cyberattacks may not result in any physical harm, in which case the laws of armed conflict do not apply. Therefore, despite the attacks having the same destructive effects as physical attacks, such non-state actors in cyberspace may avoid being punished for war crimes.[26]

[26] Colonel Sanjeev Relia, "*Cyber Non-State Actors: the Cyber Taliban*", USI Journal, 2015.

The Roles of Non-State Actors in Cyber-Warfare

Unlike the development of conventional weaponry, Cyber weapons are cheap to develop and easy to hide, their use could have no consequences from the international law perspective and the rules of engagement are still blurry. This is very different from conventional weapons, which usually require substantial investment and manufacturing capabilities. Governments around the world are therefore not only working with large companies when it comes to cybersecurity but often also with small boutique firms. This means that the number of non-state actors present in the world is innumerable, and it is not possible for us to include *all* the potential roles or actions that they could pursue.

However, for the sake of the analysis, we can focus on three crucial roles played by non-state actors in cyberwarfare: support, supply, direct participation(proxy). These roles can overlap and based on the economic and political system of the country that hosts them, the scope of their actions could significantly change.

Support

Non-state actors contribute to an offensive cyber operation that a state executes or initiate their own cyber offensives. However, in order to understand their role in supporting state attacks fully, we need first to understand the modularity of offensive cyber operations is worth highlighting because it presents new challenges for attributing the responsibility of a malicious action to a specific actor.

Developing a state backed cyber-attack is complicated, and its modularity is divided in four phases: Planning and Preparation, Cyber Intrusion, Persistent Access and Management, and Execution of Payload to achieve objective. Non state actors can support the state in any of these phases.
During the planning and preparation, they can support in the development of a weaponized code, or in the reconnaissance of the target. For instance, Endgame Inc. is a US based company that supports government agencies such as the NSA in the exploitation of cyber threats. Moreover, Endgame provides the US government support with the reconnaissance of targets through intelligence gathering.[27]

[27] Andy Greenberg, *Inside Endgame: A Second Act For The Blackwater Of Hacking,* Forbes Article, 2014.

After the first phase of planning and preparation, comes the cyber intrusion. This phase has the goal of penetrating a cybersecurity network in order to implant the cyberweapon inside the system. It is divided in two tasks: the delivery of the weaponized code, which is the cyberweapon, and the exploitation of the vulnerability, which has the goal of gaining unauthorized access to the target's system.[28]

During the third phase, the agents will have the goal of installing the malware, therefore creating a beachhead in the target's system, and later establishing command and control, thus remotely controlling the implanted cyberweapon. This phase, named persistent access and management, has often the goal of keeping the weapon ready to inject its payload, without being caught by the target's cybersecurity.

Lastly, the execution of the payload and the achievement of the objective come. During this phase, the agents shall establish command create the effect desired, may it be to destroy a certain hardware or software, deny a certain service (DoS), deceive another agent or organization with false information, or collect data from it.

Non-State actors such as hackers or cyber-militias go through all these tasks and phases in order to execute their payload. Others, such as companies, may support nation state's agencies in one specific task or phase, or even the whole modulation of the attack. One such case is the in May 2016, US Cyber Command awarded a contract of USD 460 million to six private security companies that included assisting with offensive cyber operations.[29]

Supply

To non-state actors, the advantage (and incentive) of investing in cyberweapons is that most of them have lower barriers of entry. Nevertheless, not all the non-state actors make use of simpler cyberweapons. In terms of supply of these weapons, corporations have a significant advantage

[28] Lockheed Martin, "Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense".

[29] Aliya Sternstein, "Here Are the Companies That Won a Spot on $460m Cyber Command Deal," Nextgov, May 23, 2016.

on any other actor as of today. Governments, on the other side, have increased the use of private cyber-contractors and suppliers of defensive and offensive cyber-weapons. Moreover, Governments use contractors not only for external security, rather also for internal security.[30]

One of the most interesting cases, relevant for our analysis, is the software "Pegasus", developed and sold by the Herzliya based Israeli company NSO. Pegasus, a subscription-based service offered to government agencies by a company, is a "zero click" spyware, meaning that it can access any iPhone or Android device without the user of said device clicking a link or opening a file. The scope of this innovative cyber-weapon is still, after 11 years from its first use in 2011, with big consequences, as NSO's products seemed to solve one of the biggest problems facing law-enforcement and intelligence agencies in the 21st century: that criminals and terrorists had better technology for encrypting their communications than investigators had to decrypt them.[31]

The software gave access to every email, every photo, every text thread, every personal contact of the targeted device. On top of it, it could also see the phone's location and even take control of its camera and microphone, instantly transforming phones into surveillance tools. This spyware was used to help Mexican authorities capture Joaquín Guzmán Loera, the drug lord known as El Chapo. Meanwhile, European investigators have quietly used Pegasus to thwart terrorist plots, fight organized crime and, in one case, take down a global child-abuse ring, identifying dozens of suspects in more than 40 countries.[32]

Nevertheless, we must note that the NSO's developed cyberweapon was used by a series of governments around the world in order to crack down on rebels, target dissidents, journalists and control more stuff. One of the best documented abuses is the use of this specific spyware in the murder of Washington Post journalist Jamal Khashoggi, directly ordered by Saudi Arabian crown prince Mohammad Bin Salman.[33] The software was used to penetrate the communication of the journalist's wife and family, track their movement and activities. Jamal Khashoggi was finally killed by Saudi operatives and dismembered in Istanbul in 2018.His

[30] Tim Maurer, "*Cyber Mercenaries The State, Hackers, and Power*", 79.
[31] R. Bergman & M. Mazzetti, "*The Battle for the World's Most Powerful Cyberweapon*", New York Times article, 28 Jan 2022.
[32] *Ibid*.
[33] Office of the Director of National Intelligence, "*Assessing the Saudi Government's role in the killing of Jamal Khashoggi",* declassified on 25 February 2021, official report.

case demonstrates that the use of hacking tools does not necessarily stop with data theft and violation of privacy but can have physical consequences.

Furthermore, we must note the importance of these companies in the realm of cyberwarfare, as they are not only the main supplier of defense and attack capabilities to state agencies, but they are also a tool of diplomatic leverage. Indeed, selling weapons for diplomatic ends has for long been a tool of statecraft. However, we note that the role of companies in international diplomacy has become stronger in the world of cybersecurity. For instance, when the U.S. Commerce Department added the aforementioned Israeli firm to the "entity list", which "restricts the export, reexport, and in-country transfer of items subject to the EAR to persons (individuals, organizations, companies) reasonably believed to be involved, have been involved, or pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States"[34]; the Israeli government saw it as a direct attack to their own state security as that decision would have weakened a non-state actor, NSO, that is playing a crucial role in Israel's diplomacy in the middle east and the world.

Direct Participation

Cyber proxies either conduct or directly contribute to an offensive cyber operation. Proxies have been used in the past, particularly in the gray zone of quasi-war. The benefits of using such actors, that may be made by cyber militias, hacker groups, cyber terrorists acting as Private Military Contracts (hackers-for-hire) does not stop at plausible deniability. Indeed, using proxies to project coercive power through cyberspace is particularly attractive because the technology enables new coercive effects below the threshold of use of force. To illustrate this, we can use the example of the Sands Hotel and Casino attacks. Iranian Hackers penetrated the systems of both buildings and organizations, bringing them to a halt. The cost to Iranian Hackers was very little, however, it costed the target a whopping 40 million USD$.

Otherwise, it is possible for a state to benefit from the indirect services of a cyber-militia or hacker group in some cases of geopolitical conflict. In this domain, the growing cyber

[34] U.S. Department of Commerce, Press Release.

capabilities of non-state actors still exceed the capacity of the majority of developing states. This is mostly the case in Eastern Europe, where highly skilled labor is found, but which is not absorbed by neither the state nor the private sector. The solution engineered to resolve this issue is similar to the use of privateers in the mercantilist era: the sanctioning and the indirect use of patriotic hackers.

For instance, the Ukrainian Cyber Forces, a cyber-militia proclamated in defense of Ukraine against Russian aggressions, illustrates the presence of significant cyber capabilities in private hands, the activity of proxies during a hot conflict, and the incentives the state as mentioned above. Their activities include Distributed Denial of Service (DDoS) attacks, web defacements and the leaking of classified Russian government files. This is an example of a non-state uncontrolled actor which is supported only politically by the state. These types of actors often have their own internal organization, communication services, bureaucracy and ranks.

However, sometimes, non-state actors are directly used by the state in order to attain certain political, economic or social goals. One significant case is the use of the WannaCry attack, perpetrated by the North Korean backed cyber militia Lazarus in 2017, which forced the British National Health Service to work with pen and paper, potentially causing human life losses and damages.

The Actions of Non-State Actors in Cyber-Warfare

Now that we have looked upon the roles taken by these actors, we will focus on the geopolitical or military driven actions taken by non-state actors in cyberwarfare: **espionage, interference and coercion.** We already considered the attack operations when analyzing their role during direct participation in an operation.

Espionage

Cyber espionage is a form of cyber attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.[35] Since

[35] VMware, "What is Cyber Espionage?", article.

companies started encrypting the electronic communications between electronic devices, the role of the non-state actors has skyrocketed in importance in cyber espionage.

Given the biggest advantage of cyber espionage, namely the capacity of gathering information without sending agents to far away territories, increasing costs, endangering crucial information carried by them and even their own lives: everything can be stolen by well-paid experts sitting on a computer, physically safe. For this reason, and to ensure plausible deniability, today states increasingly rely on cyber militias for espionage purposes.

Non-state actors, just like secret service agencies offer cyber espionage disguised in many different types of cyber espionage tools. As they are ever changing and always developing, we will only focus on the most used ones. First there are DDoS attacks, which are mainly used to disrupt the victim nation-state's communication systems. DDoS attacks are preferred because an attacker can implement them with very limited resources against a larger, more powerful victim. Malware, such as viruses, worms, and Trojan horses, are also popular tools for disrupting normal computer operations, secretly collecting data, or destroying it entirely. Other kinds of attacks include "Logic Bombs", which are malware designed to lie dormant until a specific time or until triggered by a certain event, and IP Spoofing, where an attacker manages to disguise itself in order to gain access to private information or secure networks.[36] One last tool are the "Zero click" malwares, which we have analyzed above with the Pegasus case.

However, a very recent trend has emerged, cyber espionage through cloud computing. In May 2022, researchers from Unit 42 of Palo Alto Networks has found out that the Russian hacker group "Cloaked Ursa", or also known as "Cozy Bear" has shared infected files using Dropbox and Google Drive, two of the most used cloud services in the world. This technique is an innovation of the zero day penetration model, instead of using an infected email, this time the infected files penetrate the system only by using the cloud service or in some cases, without any interaction with a human being on the targeted device. This is the first documented time that a hacker group uses cloud services in order to steal sensible data from diplomatic organizations.[37]

[36] Dana Rubenstein, "*Nation state cyber espionage and its impacts",* 4.
[37] M. Rossi, A.V. Sica, "*Cyberspionaggio attraverso il cloud",* CyberSecurity360, 2 August 2022.

Interference

Meddling in foreign political affairs is part of politics since when humans started . All the succession wars in Europe from the end of the middle ages to the 19th Century are a clear example of how much states care about the environment around them and the [38] Indeed, the tools used to interfere however have changed throughout the ages. Today, foreign cyber interference in elections is a hot topic that is still debated and discussed throughout the "democratic world".

Basing ourselves on research published by the Australian Strategic Policy Institute, we can infer that the ctivity can be divided into two attack vectors. First, these actors target electronic and online voting infrastructure and attacked it with a variety of cyber operations, including denial of service (DoS) attacks and phishing attempts. Meanwhile, they make use of internet information operations to take advantage of candidates, legislators, media, and voters' online presence.

Indeed, the internet has gained incredible importance in political beliefs, electoral campaign and voting infrastructure. In the last decade, the use of social media in particular has given the capacity to states using cyber militias or internet bots of expanding certain political messages across borders. This is the case with the Russian meddling in European and American elections. Although not only being delivered exclusively by cyber interference, the delivery of fake news, attacks on electoral infrastructure, the extensive of use of bots and the support to certain candidates are not uncommon tools used by the Russian federation to influence other countries' elections, and all of these tools are delivered by cyber non-state actors.

Coercion

Non-State actors such as cyber militias, hacker groups, are often used in coercive actions against other actors, may them be states, companies or other militias. Coercion in this case means obliging another agent to pursue policies or a set of actions by the use of force or threat.

[38] Fergus Hanson, Sarah O'Connor, Mali Walker, Luke Courtois*, "Hacking democracies: cataloguing cyber-enabled attacks on elections",* ASPI

One of the most famous cases of a cyber militia, supported by a state (in this case), to have applied coercive power on another is the case of the Sony Pictures attack in 2014.

On the 24th of September 2014, an employee of Sony Pictures Entertainment received an email that was purported to be from Nathan Gonsalez. The email account of Gonsalez was bluehotrain@hotmail.com. An email contained a link that, when clicked, purported to launch a video clip promoting another "company." The words "video" and "Adobe Flash" were in the file name, probably to fool a worker into thinking this was a media clip that would play in the Flash program that was popular at the time. Strangely, the email's signature didn't include Nathan Gonsalez's name but rather the name of an executive from a different company. The North Koreans employed this code to gain a far stronger foothold inside the Sony network. The malicious code could copy data from the targeted computers' memory, map the network's file directories, launch the malicious code onto the Sony network, and then wait patiently for additional instructions.[39]

On November 24, two months after the success of the phishing operation, the North Korean militia, Lazarus (also known as "Guardians of Peace"), leaked personal information about Sony Pictures employees and their families, emails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, plans for future Sony films, scripts for certain films, and other information. After this, the North Korean cyber militia used malwares to erase Sony pictures infrastructure, damaging it.[40]

Why was this course of actions taken? Sony Pictures was working on the development and release of the then upcoming movie: "The Interview". Said film included comic scenes regarding the North Korean leadership, an act that was seen as a direct mockery and attack of the "Supreme Leader" of the North Koreans, therefore pushing the Lazarus group to coerce Sony Pictures Entertainment. Indeed, after the cyber-attack and threats of terrorist attacks in cinemas displaying the movie, Sony Pictures opted to cancel the film's formal premiere and mainstream release.

[39] Ben Buchanan, "*The Hacker and the State*", 109.
[40] G. Siboni & D.Siman-Tov, "*Cyber Extortion: North Korea versus the United States*".

Third Chapter: Case Studies

From all the examples we have analyzed, there is one factor that is ever changing: that is the relation between the non-state actor and the state. From the different cases, we can infer that the structure of the state itself influences the centralization of the decision making in cyber policy, which in term affects the roles and actions that the non-state actor will pursue. In term, what makes one state develop a certain policy structure differently from another is the set of beliefs, ideologies, interests, and choices which are based on the economic and political structure of the country. In this sense, we will now analyze two very different state policy systems as our case studies: the United States of America and the Russian Federation.

Case study: United States of America

The United States of America is the hegemon of our international political system. It has the largest defense expenditure in the world, and one of the most effective cyber capabilities. In terms of external interference, the stance of the US towards cyber violation is particularly harsh. In 2017 Jim Mattis, classified memo "united states should declare its willingness to take extraordinary steps, including the use of nuclear weapons, in response to a foreign cyber-attack against critical infrastructure."

Moreover, we must note that in the case of countries as technologically developed as the United States of America, there is a non-ignorable disproportionally: the US is at the same time extremely technologically developed, arguably having the strongest cyber-capabilities in the world. However, while it keeps that strength, it is extensively reliant on those technologies, therefore making it extremely vulnerable to an efficient and large-scale cyber-attack. In order to counter this imbalance, the United States is making an extensive use of non-state actors and contractors in the cyber domain, but the question is: how does the US use non state actors, what is their strategy, policy and organization?

To start, we note that private military companies (PMCs) increasingly appeared in the US military starting from the 1990s.[41] At first many of these companies provided aggressive tip-of-the-spear services, but after a series of scandals the industry as a whole tilted towards defense. However, The US government tightened the noose after realizing that principal-agent issues had unintended negative effects. As a result, businesses began cooperating much more closely with their home nations or with other nations in the nation's alliance network.[42]

There continue to be problems because employees of private military and security firms in Iraq were excluded from the US Military Code while still enjoying immunity from local prosecution. The push for privatization, a general rethinking of the role and scope of the state, increased economic incentives for outsourcing, and the shift in business focus from military to security services all contributed to the remarkable growth of the private market for security services.[43]

The collaborative relationships between public and private entities continues to define the market for cyber capabilities today. Depending on how big they are and who their clients are, private cybersecurity businesses can be divided into two main groups. According to Shorrock, a cybersecurity contractor expert, the largest companies fall into this first category because they are "focused on a single market and earning most of their revenue from that market, with up to 90% of their revenue coming from contracts with the Pentagon, the CIA, and the national collection agencies."[44] The second type of companies includes those with a broader, more varied clientele outside of governmental organizations. Private cybersecurity contractors started to appear when the private security sector grew, and this development has been fueled by two factors.

First, traditional pure-play military contractors have begun to integrate cybersecurity in their range of operations. For instance, one of the most relevant case of a contractor actor playing a

---

[41] Juan Carlos Zarate, "The Emergence of a New Dog of War: Private International Security Companies, International Law, and the New World Disorder," Stanford Journal of International Law, 34.

[42] Sarah Percy, "*Mercenaries: The History of a Norm in International Relations*", 232-235.

[43] Tim Maurer, "*Cyber Mercenaries The State, Hackers, and Power*", 72.

[44] Shorrock , *"Spies for Hire"*, 264.

role in supplying the United States with zero day vulnerabilities to the US government is the firm iDefense, which started to give financial rewards to anyone finding these vulnerabilities, before selling these same to the government agencies.[45]

Second, smaller boutique businesses and start-ups appeared and were either acquired by bigger businesses or developed into reputable contractors. These smaller businesses need special consideration because there is far less information available about them, which reduces transparency and oversight.[46]

However, the United States is not alone in this pattern of privatization, bringing contentious principal-agent developments: Israel, France, and the UK also rely extensively on private contractors. In its case, the agency responsible for Cyber Security is the "US Cyber Command", created in 2010 when the Pentagon declared the cyber space a new operational domain. Its contemporary economic model, which was developed based on the values of the "Washington Consensus", made the state reliant on the private market in terms of cyber security, alongside other European NATO countries.

In the United States, the trend of privatization dates back to the Reagan administration, which was enhanced with the development of "new public management", bringing more and more government functions under the realm of private companies. [47]

To begin with, it is important to emphasize that the US Cyber Command is still a fairly new organization. The US Cyber Command's 2016 budget contains 963 civilian and military government employees, together with 409 contract workers, up from the Joint Task Force's initial 150 employees. In other words, there are 30% contractors and 70% government workers. The head of the US Cyber Command also serves as the NSA director, making it a hybrid entity.[48]

---

[45] Tim Maurer, "*Cyber Mercenaries The State, Hackers, and Power*", 74.

[46] *Ibid*.

[47] Allison Stanger, One Nation Under Contract: The Outsourcing of American Power and the Future of Foreign Policy (New Haven, CT: Yale University Press, 2009).

[48] Lachow, "The Private Sector Role in Offensive Cyber Operations".

The US Cyber Command's still-nascent structure is also reflected in the contract itself. One of its goals was to "simplify USCYBERCOM's purchase of cyber mission support capabilities and services, information technology services, and cyber professional services... within a consolidated framework," according to the contract itself.[49] This indicates that the US Cyber Command is a highly centralized organization that heavily relies on non-state actors as vendors and service providers. It is simple to apply principal-agent theory to the government's use of contractors for cyber operations. The contractual criteria of US Cyber Command provide a comprehensive description of the selection and screening procedure. All individuals executing the work must be US residents and have "Top Secret personnel security clearances with SCI access eligibility", while businesses must be US-owned or, if foreign-owned, "hold a positive National Interest Determination".[50]

many businesses offer customer service and product updates that necessitate a continuing relationship and give insight into the use of the products, despite the assertions of some businesses that they have no control over how their products are used once they are sold and shared with the client. Therefore, private cybersecurity contractors are really just an extension of the current practice of outsourcing activities to the private sector and defense contractors. This has the effect of implying that even in external foreign affairs, the USA controls which countries will be supplied. Additionally, it is questionable how strong oversight can be formed and maintained when the government is generally lacking in personnel with the knowledge required to carry out their monitoring duty. An issue faced by other international actors, like the European Commission, as we have seen before.

In conclusion, we have found that the US' cyber non-state actors' policy is particularly state centered and the role of non-state actors is limited to the supply of capabilities or logistical support. Indeed, defense contractors, who serve as the United States' proxies, are kept relatively close by the country, allowing for close control over their actions and monitoring of their choice of targets and tactical approaches.

What does all of this signify for US cyber security management? The majority of the cyber companies work as contractors under state supervision. A variety of techniques are used to

[49] U.S. Cyber Command website.

[50] Tim Maurer, "*Cyber Mercenaries The State, Hackers, and Power*".

monitor contractors. They frequently collaborate physically with their federal colleagues. Actually, the US Cyber Command's request for proposals states that "contractors designated as critical to successfully completing mission essential functions, or as emergency personal, may be required to travel with government counterparts to work for extended periods of time from a remote contingency location during a continuity of operations event".[51] These kinds of partnerships are among the closest beneficiary-proxy ties and have the most intense state control as a result of such clauses.

Case study: Russian Federation

To understand the policy of the Russian Federation, we should firstly understand the concept of "Sanctioning". Sanctioning occurs when a state consciously but indir- ectly benefits from a malicious activity targeting a third party, an activity which the state could stop but chooses not to. Sanctioning describes environments where the state indirectly creates a fertile ground for such malicious activity to occur in the first place.[52]

From a historical standpoint, former Soviet Union countries stand out for having a large population of people with highly developed technical abilities and for having some of the greatest math, engineering, and computer science departments in the world. However, after the collapse of the Soviet Union thousands of experts in math, ICT and engineering could not be absorbed by the private or public market, therefore creating a phenomenon of highly skilled hackers turning to the black market or cybercrime in order to gain an income.[53]

This trend kept on developing through the beginning of the twenty-first century, until when, according to the think tank Carnegie Endowment for International Peace, Russian Cyber Economy's size reached a whopping 2.3 billion Euros in 2014. However, we must note that the overwhelming majority of these acts are specifically targeted to organizations and people in the European Union and the United States. This, combined with Russian lack of cooperation

[51] Request For Proposal (RFP), USCYBERCOM request, September 2015.
[52] Tim Maurer, "*Cyber Mercenaries The State, Hackers, and Power*", 94.

[53] Boris N. Mironov, "The Development of Literacy in Russia and the USSR from the Tenth to the Twentieth Centuries," History of Education Quarterly, 31

with foreign law enforcement agencies, are the main reasons why Russia arrests an increasingly lower number of cyber criminals, which is in itself a form of sanctioning.

From an official point of view, Russian policy continues to give hackers a lot of freedom to operate outside of Russia and in the country's public interest. This is shown by a quote stated by the Russian President Vladimir Putin, made in June 2017, when the he was questioned by the media about Russia's role in interfering in the 2016 U.S. election:

"Hackers are free spirited people, like artists. If they are in a good mood in the morning, they wake up and paint. It is the same for hackers. They wake up today, they read that something is happening in inter-state relations, and if they are patriotically minded – they start making their contributions which are right, from their point of view – to the fight against those who say bad things about Russia. Is that possible? Theoretically, it is possible."[54]

This form of romanticization of patriotic hackers and cyber militias showcases the high level of political cover for hackers becoming active in Russian interests and demonstrates their strategic use as a means to establish plausible deniability while attacking certain objectives.

The use of the policy of sanctioning by the Russian state started with the DDoS attacks on Estonia in 2007. after the Estonian government decided to move the Bronze Soldier, a Soviet-era World War II mem- orial, sparking vocal protest by the Russian government and among many Estonians of Russian origin. These physical protests were accompanied by a virtual riot in form of a DDoS attack that brought down websites of the Estonian government and businesses.

With its policy of demonizing the Estonian government, calling its policies a "pursuit of Neo-Nazism", [55] the Russian government turned the narrative in a climate, within which patriotic hackers may have been at work. The Russian official bodies outlined an interest of the Russian state against the removal of the monument. By doing so, the government supported a narrative

[54] Andrew Higgins, *"Maybe Private Russian Hackers Meddled in Election, Putin Says,"* New York Times, 1. June 2017.

[55] Federation Council of the Federal Assembly of the Russian Federation, "*Address of the Federation Council of the Federal Assembly of the Russian Federation (No. 15-SF)*" 24, January 2007.

with a clearly identifiable opponent (the Estonian government), victims (the Russian people), and a call for political action.[56] Nevertheless, there is no *conclusive* evidence of the Kremlin's direct involvement with the cyber-attack on the Baltic nation. What the Russian policies show, and what we are arguing in this thesis, is not a direct involvement, is the fact that the Russian government did little to nothing to stop the hackers provoking malicious activity in Estonian software network and databases.

The year after the Estonian cyber-attacks, a short war between Russia and Georgia took place, during which observers noted a blitz orchestration, characterized by the rapid mobilization of non-state actors to project coercive (cyber) power, in the form of a DDoS attack.[57] One of the most notorious examples of a Russian backed cyber-militia is the Russian Business Network, a criminal organization which administers various illegal cyber-activities, has according to some contributed to the cyber-attacks conducted in 2008 during the Russian-Georgia war.

However, arguably the biggest, most important case of cyber sanctioning and support to cyber militias is the cyberwar perpetrated during the (still ongoing at the time of writing) invasion of Ukraine. Cyber Berkut, which arose after President Yanukovych left the country and Berkut, the Ukrainian special police force, was disbanded, is the most notable actor on the pro-Russian side of the conflict. The operations of pro-Russian hacktivist groups like Cyber Riot Novorossiya and Green Dragon, as well as Cyber Berkut, match those of pro-Ukrainian hacktivist groups in that they undertake DDoS attacks against Ukrainian government networks. The Russian invasion of Ukraine serves as an example of the existence of sizable cyber capabilities in private hands, the actions of proxies during a volatile conflict, and the incentives for the participating states to employ these private capabilities.

In conclusion, from the cases analyzed before, we can infer that the Russian government has a looser use of non-state actors in cyber warfare. The Russian government is increasingly providing covert support to various hacker organizations, even threatening them with legal action and offering them payments to cooperate, especially when it comes to attacking the United States and its allies. However, the backing of the state is typically just passive; frequently, the only connection between the state and the proxy is that the state voluntarily

[56] Egloff, "*Cybersecurity and Non-State Actors*", University of Oxford, 162.
[57] *Ibid.*

chooses to ignore the proxy's activities in spite of having the power to take action. However, due to the low level of sources and absence of documents confirming many of the suggestions on Russian policy, further research will be required on the Russian non-state actors' cyber policy.

Future Developments and Conclusion

The world of Information and Communication Technology (ICT) is continuously changing and developing new technologies that do not only shape the market, but can have deep repercussions on the geopolitical, economic and social branches. This is the case with the cases of Quantum computers, Artificial Intelligence and the Metaverse, all newly developing domains that will be increasingly relevant in the future. In this short chapter, we will try to summarize the potential impacts of these technologies on cyber warfare and the potential role that will be played by non-state actors in them.

Quantum Computers and Artificial Intelligence

Historically, intelligence agencies and secret services focused on gathering information in transit. It was simpler to get more information while it is going from one place to another rather than getting it from the source, and as the digital era developed, this trend continued. However, as manufacturers caught up with this vulnerability and started encrypting with complex mathematical operations the information as soon as it left the devices.

The very basis of hacking stems from the issue created by the secrecy and difficulty of penetration attributed to computers developed since the start of the 21st century. Nevertheless, even if encryption does not fail, humans do. Because all the software and hardware is created by humans, and humans are not infallible, these devices have holes, called zero days.

However, with the creation and development of quantum computers the course of history is set to know dramatic change. Both quantum computing and artificial intelligence have shown to have a significant impact on the development of warfare as we know it. Artificial intelligence can collect excessively large amounts of data through algorithms that operate artificial intelligence systems. The rules or patterns in the data used to create the algorithms can help

artificial intelligence learn new skills. Although it has incredibly sophisticated capabilities, it is more than plausible that artificial intelligence may be utilized against us, leaving us vulnerable. To do multiple calculations at once, quantum computing can use quantum mechanical engineering, and the fastest/most effective computer ever created is a quantum computer. In theory, quantum computing poses a risk because a single quantum computer would be more powerful than all of the supercomputers in the world today.[58]

In the case of Artificial Intelligence (AI), it has many dangers associated with it, including cyberattacks on existing AI systems themselves, and the implementation of AI in conventional military warfare. Indeed, as more of our choices, on the battlefield and on the civilian life, will be handed over to this set of "intelligent" algorithms, hacking this system could cause an unthinkable amount of human and economic damage to a country or to an army. Current AI systems have begun to see data breaches from unknown sources due to insecure centralized servers that hold valuable information. This creates an easy target for even the simplest of hackers to obtain information within these databases in bulk. Cyberattacks on AI databases could cause severe destruction for individuals, businesses, and our government.[59]

With regards to quantum computers, they might revolutionize cybersecurity and warfare as a concept. First of all, we must note that quantum computers are different from a classic computer in many ways, but the biggest difference is the bits on which they operate. quantum computers operate on quantum bits (qubits). Qubits are like bits in that they can be zeros and ones, but, unlike classical bits, they can be in both at the same time. Qubits work simultaneously, giving an advantage over classical computers because they can reach solutions much faster.[60]

The capability of quantum computers to break any encryption found in few seconds is arguably the biggest threat to cybersecurity that we might face in the near future. However, this is completely hypothetical of the worst-case scenario. Today, all current quantum computers do not have the processing capabilities to carry out such a massive threat.[61] Despite this, the potential power promised by these devices is pushing many political institutions, including the European Union, to develop the first large scale working quantum computer.

---

[58] K. Kline, M. Salvo, D. Johnson, "How artificial intelligence and quantum computing are evolving cyber warfare", the Institute of World Politics.
[59] *Ibid*.
[60] *Ibid*.
[61] D. E. Denning, "*Is Quantum Computing a Cyber Threat?*", American Scientist.

Nevertheless, we must note that the debate around the impact that quantum computers will have on cybersecurity is still ongoing. Critics of the theory that Quantum computers will revolutionize the world of cybersecurity point at the fact that despite this new technology changing cryptography, robust cryptosystems can be undermined by poor organizational coordination, and careful security policy can compensate for technical vulnerabilities. Which means that even if quantum computers will be extremely powerful, there will not be a revolution in cybersecurity.

One thing is for sure : in these new domains, non-state actors will be crucial as they have the skills, the technological and industrial capacity to keep such undertakings under control. Still, given the importance and potential of these technologies, we can predict that further collaboration between the state and non-state actors will be sought, but how, and with what structure those collaborations will come into place should be further researched in the future.

Metaverse

If there is a part of cyberspace in which there is no presence of the state at all, that is the metaverse. It is a space completely conceptualized, thought and created by a non-state actor. The metaverse is defined as a digital world that combines virtual and augmented reality. Individuals will navigate this online world, which can be identical to the real world or based on imagination, or some combination of both, by using digital avatars.
Although the technology is particularly new and in development, thus blocking us from making a deep analysis of it, we know that it could have a relevant impact on cyberwarfare and the role of non-state actors in it.

Unlike current virtual reality, which is mostly used for gaming, this new virtual world can be used for anything, from work, leisure, concerts and cinema trips, or simply socialising with friends on the other side of the world.

Looking to the future, we can expect an absolute universe of possibilities for the metaverse, both good and bad. One vulnerability is that data captured through this domain’s devices, or any of the wearable devices that will certainly be introduced in the future, can be very sensitive in nature. Data that ends up in the wrong hands can easily be used as a tool for social engineering schemes or as a form of blackmail. Additionally, when people and businesses have

lives outside of the actual world and within the metaverse, it can be more difficult to safeguard intellectual property.[62]

As we have seen in the past, new technology is often developed and introduced to the market long before cybersecurity concerns are addressed. This means that we can expect the Metaverse to become the new landscape of cyber conflict, where non-state actors will find again much more space than ever before.

Conclusion

This thesis has shown that different states have different ways of interacting with the non-state actors in the cyberspace. There are states that have stricter control such as the case of the United States of America, which relies on cyber-contractors mainly for logistical support and supply of payloads. Whereas, some other states' institutions display a looser control of cyber non-state actors, such as the Russian Federation which, as we have analyzed, incentivizes cyber militias, patriotic hackers to attack opponents of the Russian foreign policy. In addition, this freedom to act given to cyber-proxies is emphasized by the Russian state tendency to not cooperate with law enforcement agencies, never cracking down on cybercrime caused by Russian non-state actors, outside of its borders.

Furthermore, we have shown that there is a strong analogy between the use of non-state actors in cyberspace and the privateers in the mercantilist era. While analyzing the diverse roles and actions that said actors push further in this growing domain.

Cyber-warfare is a domain that is becoming increasingly important, and the capability for catastrophic cyberwarfare exists now more than ever. As digitalization grows and new technologies develop, our reliance on them does too, therefore increasing the risks. In this domain non-state actors, proxies, private military contractors and hackers flourish, pushed by the privatization of conflicts and the libertarian nature of the internet. Moreover, using traditional weapons and armies has deep legal and political consequences, but using cyber-

[62] Nahla Davies, "*Cybersecurity & the Metaverse: Pioneering safely into a new digital world*", Global Sign by GMO.

proxies or militias gives a “way-out” from getting the responsibilities that come from perpetuating an attack.

Finally, it is not clear how the relationship between non-state actors, states and cyber-warfare will develop in the new cyber spaces of the Web 3.0, such as the ones developed with the Metaverse or quantum computers. In particular, how non-state actors will develop in a new stateless domain that brings cyber integration to a deeper. Indeed, this should be further researched in the future.

Bibliography

Buchanan, Ben *"The Hacker and the State, Cyber-attacks and the new normal in geopolitics."*

Robinson et al, *"Cyberwarfare, issues and challenges"*, March 2015

Rid, Thomas & Buchanan, Ben *"Attributing Cyber Attacks",* Journal of Strategic studies, 2014.

Ministére des Armées Français, *"Élements publics de doctrine militaire de lutte informatique"*, 2019.

Trend Micro Research, *"Void balaur and the rise of the cybermercenary industry"*, 2021

Lemos, Rob, *"How to use bug bounties with penetration testing to bolster your app security*", 2017
Gozzi, Raymon, *"ETC: A Review of General Semantics"*, Vol. 57, No. 3 (Fall 2000)

Stewart, David P., *"International and Transnational Criminal Law",* 2019.

H. Schell, *Hackers and Hacking: a reference handbook*, 2013.

Bussolati, Nicolò, *"The rise of non-state actors in cyberwarfare",* 2015.

Sigholm, Johan*, "Non state actors in cyberspace operations",* Swedish National Defence College.

Kaspersky*, Black Hat, White Hat and Gray Hat Hackers*

Applegate, S. D., *"Cybermilitias and Political Hackers: Use of Irregular Forces in cyberwarfare,"* IEEE Security & Privacy, Volume 9, Issue 5

Dombrowski, Demchak, *Cyber war, cybered conflict and the maritime domain*, Naval War College Review , Vol. 67, No. 2 (Spring 2014)

Egloff, Florian, *Cybersecurity and the Age of Privateering*, Georgetown University Press

Breton, Thierry*, Press Release*, European Commissioner for the Internal Market

Roumani, Yaman *Patching zero-day vulnerabilities: an empirical analysis*, Journal of Cybersecurity

Rosenzweig, Paul *"International Law and Private Actor Active Cyber Defensive Measures,"* Stanford Journal of International Law 103 (2014).

Curtiss, Tiffany *"Computer Fraud and Abuse Act enforcement: cruel, unusual, and due for reform"*, Washington Law Review (Vol.91, Issue 4).

Colonel Sanjeev Relia, *"Cyber Non-State Actors: the Cyber Taliban*", USI Journal, 2015

Greenberg, Andy Inside *Endgame: A Second Act For The Blackwater Of Hacking*, Forbes Article, 2014

Lockheed Martin, *"Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense".*

Sternstein, Aliya *"Here Are the Companies That Won a Spot on $460m Cyber Command Deal,"* Nextgov, May 23, 2016.

R. Bergman & M. Mazzetti, *"The Battle for the World's Most Powerful Cyberweapon"*, New York Times article, 28 Jan 2022.

Office of the Director of National Intelligence, "*Assessing the Saudi Government's role in the killing of Jamal Khashoggi"*, declassified on 25 February 2021, official report

U.S. Department of Commerce, *Press Release.*

VMware, *"What is Cyber Espionage?",* article

Dana Rubenstein, "Nation state cyber espionage and its impacts",

M. Rossi, A.V. Sica, *"Cyberspionaggio attraverso il cloud"*, CyberSecurity360, 2 August 2022.

Fergus Hanson, Sarah O'Connor, Mali Walker, Luke Courtois, *"Hacking democracies: cataloguing cyber-enabled attacks on elections"*, ASPI

G. Siboni & D.Siman-Tov, *"Cyber Extortion: North Korea versus the United States".*

Zarate, Juan Carlos "*The Emergence of a New Dog of War: Private International Security Companies, International Law, and the New World Disorder,"* Stanford Journal of International Law

Percy, Sarah *"Mercenaries: The History of a Norm in International Relations"*

Shorrock , *"Spies for Hire"*

Lachow*, "The Private Sector Role in Offensive Cyber Operations".*

Stanger, Allison *"One Nation Under Contract: The Outsourcing of American Power and the Future of Foreign Policy*" (New Haven, CT: Yale University Press, 2009).

Request For Proposal (RFP), USCYBERCOM request, September 2015

Mironov, Boris N. "The Development of Literacy in Russia and the USSR from the Tenth to the Twentieth Centuries," History of Education Quarterly

Higgins, Andrew *"Maybe Private Russian Hackers Meddled in Election, Putin Says,"* New York Times, 1. June 2017.

Federation Council of the Federal Assembly of the Russian Federation, *"Address of the Federation Council of the Federal Assembly of the Russian Federation*, 24 January 2007.

K. Kline, M. Salvo, D. Johnson, *"How artificial intelligence and quantum computing are evolving cyber warfare"*, the Institute of World Politics

D. E. Denning, *"Is Quantum Computing a Cyber Threat?",* American Scientist.

Davies, Nahla *"Cybersecurity & the Metaverse: Pioneering safely into a new digital world"*, Global Sign by GMO.

Riassunto

Questo elaborato offre un'analisi del crescente utilizzo degli attori non statali nella guerra informatica. A causa della pandemia di Covid, che ha spinto le società verso un maggiore utilizzo dei servizi digitali, e con la consapevolezza da parte della classe politica che una transizione ecologica richiede una transizione digitale, l'importanza del settore digitale nelle nostre vite ha conosciuto una drammatica espansione.

Il primo capitolo introduce gli sviluppi, all'inizio del XXI secolo, di un mercato per le vulnerabilità informatiche, fornendo incentivi economici sia agli hacker che alle aziende. In definitiva, questo fenomeno è stato cruciale per la crescita degli attori non statali nel cyberspazio. Inoltre, il capitolo fornisce importanti chiarimenti sulla terminologia e sulla comprensione delle basi del cyberspazio, che sono fondamentali per comprendere le argomentazioni presentate in questa tesi.

Il secondo capitolo approfondisce uno degli incentivi più importanti alla base della proliferazione degli attori non statali nel mondo digitale, il problema dell'attribuzione, che spesso garantisce la negabilità plausibile agli attori statali e non statali. Inoltre, approfondisce un'analogia storica tra il ruolo degli attori non statali nel cyberspazio e quello dei corsari in alto mare durante l'era mercantilistica. Questa analogia ci aiuta a comprendere il ruolo ibrido che gli attori non statali svolgono nei confronti della sicurezza e della sovranità dello Stato. Infine, questo capitolo spiega in modo approfondito i ruoli operativi e le azioni intraprese dagli attori non statali nella guerra cibernetica.

Il terzo capitolo offre due casi di studio, gli Stati Uniti d'America e la Federazione Russa. Questi due ci mostrano come i ruoli operativi offerti dagli attori non statali cambino in base alle caratteristiche dello Stato che li ospita. Un argomento centrale della tesi, infatti, è che la struttura politica ed economica nazionale influenza le relazioni tra Stati e attori non statali, i loro ruoli e le loro attività nella guerra cibernetica.

Infine, la conclusione offre riflessioni e dibattiti sul futuro che, potenzialmente, cambieranno la portata e il potenziale della guerra cibernetica e il ruolo che gli attori non statali hanno in essa. Le nuove tecnologie stanno espandendo e approfondendo lo spazio cibernetico, arricchendolo di nuove capacità e opportunità per gli attori non statali.