OUTSOURCING OF STATE CYBER GOALS TO NON-STATE ACTORS

PROJECT GROUP

AUTHORS

Geoffrey Hubbard Valenzuela
Marcel Schneuer
Tomas Bueno dos Santos Momčilović
Zafer Dogukan Cincil
Isaac Bravo Lara

CONTENTS

PREFACE

Welcome to Outsourcing of State Cyber Goals to Non-State Ac-tors, a project developed in the context of the Master's course Introduction to Politics, Technology & Sustainability (TUM).

We were inspired to research this topic when we realised that a large number of cyberattacks against public and private targets are carried out by non-state groups but supported by governments. This led us to the following research question: ***Why do states resort to independent (including criminal) groups in order to achieve their goals in cyberspace?***

This document consolidates the different analyses conducted, based on a total of 349 sources and interviews with 6 experts in the field. We hope that this will allow the reader to gain a deeper ac-ademic understanding regarding the dynamics between states and non-state actors in cyberspace, and their main implications.

For more information, we encourage you to explore the web-site of this project, where you will find extracts from the in-terviews, along with dynamic visualisations, which provide a better experience and understanding of the topic.

Thank you very much.

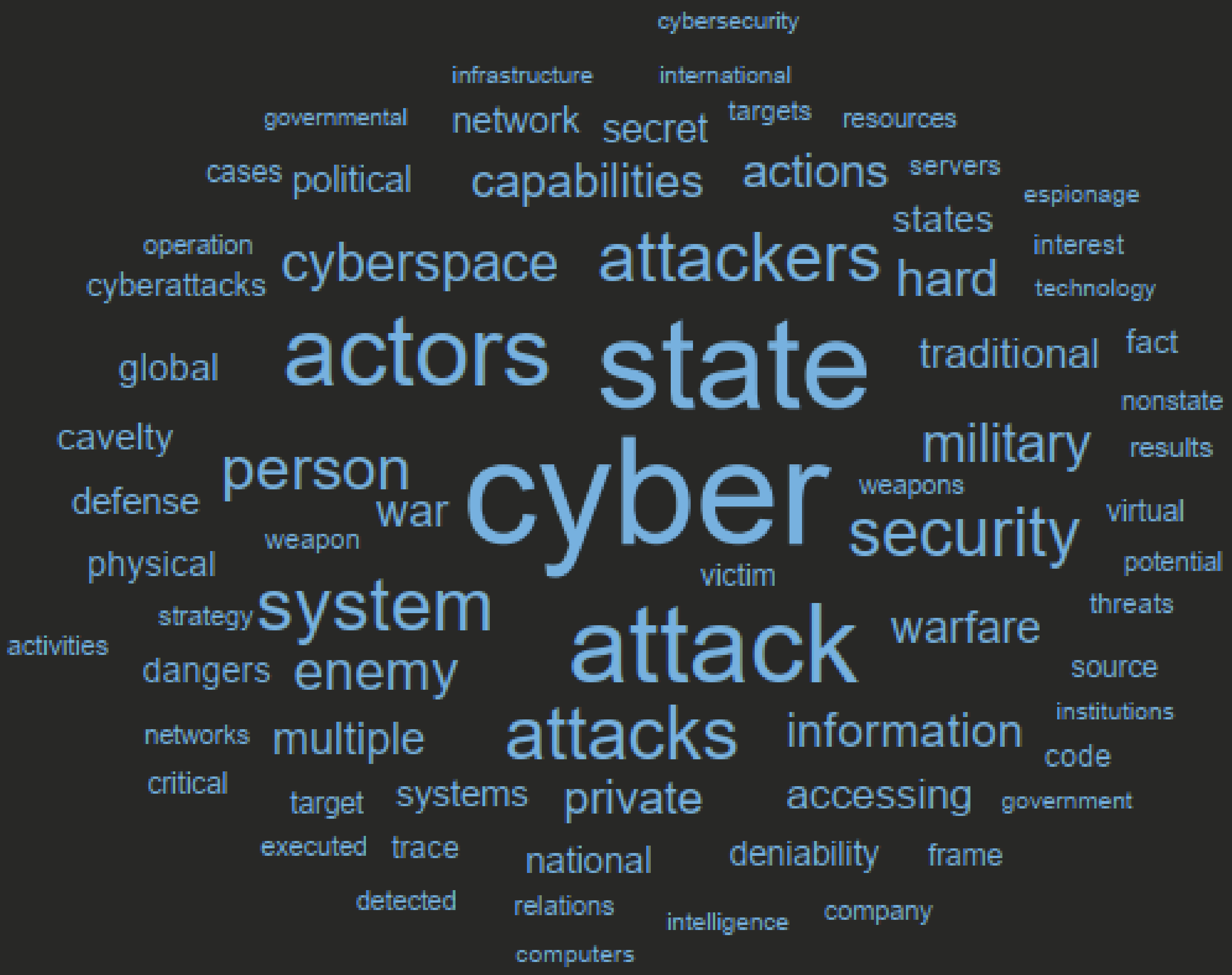
Outsourcing of State Cyber Goals to Non-State Actors Project Team.

CHAPTER 1

INTRODUCTION

Wordcloud of Key Concepts

Chapter 1: Introduction



Data source: Chapter 1: Introduction

INTRODUCTION

CHAPTER 1

DEFINITION OF CYBERSPACE

Cyberspace can be defined as the “fusion of all communication networks, databases, and sources of information into a vast... blanket of electronic interchange.” (Dunn Cavelty 2015, 401) Put more simply, it is the electronic networks medium in which computers communicate. It is important to remember that cyberspace is not only a virtual network; it is also inextricably made up of physical elements, such as computers, cables, satellites, and servers. The World Wide Web is one of the most important applications of cyberspace, but it is still only one of many parts that is part of it. There is no regulatory body for the whole cyberspace, it can be imagined like several decentralized systems that agreed on communicating with each other (Schulze 2018).

CYBER ATTACKS AND VULNERABILITIES

From a state security perspective, cyberattacks are a completely new way of warfare. Neither proximity nor military budget is a reliable indicator for the capabilities of a state. Attackers can either work on their own, are part of a state operation, or something in between. An attack can be carried out without the victim knowing and the single imminent defence is normally to shut down the whole network which can have further implications. The source of an attack is hard to trace and deliberately obscured, even espionage gets harder because operation centers can be an office building or don’t exist at all because of decentral command structures. In short: cyberattacks are hard to predict, hard to defend against, and hard to trace in the aftermath.

While for a long time, the military spending pretty much decided the position in international relations, those new kinds of attacks are more based on very few very knowledgeable people with access to high-speed internet and some technical resources which are still way less costly than for example a fighter jet. Additionally, once a security vulnerability in, for example, a software which is used in multiple governmental institutions is found, an attacker can target multiple systems at the same time without physical presence. Attacks that are based on overpowering a system are easily scalable through taking over external unsecured devices and, based on the attack, have exponential growth.

ATTRIBUTON PROBLEM

Because the finding of the source of an attack is aggravated, the attackers gain the possibility of plausible deniability. While there are normally some indicators where the attackers are based, they regularly try to hide behind a network of intermediate servers and purposely add false information in their code and actions to blur their traces. The time of activities or the naming of variables is for example circumstantial evidence in finding attackers. The problem is that attackers know this as well. In most cases, real progress in investigating the root of the attack is only made by intelligence services that use other methods besides analyzing the code. However, even if state actors concluded who was behind the attack and sanction those attackers, they will still dispute those actions and use this “injustice” as an argument for putting themselves in the victim role or for countermeasures.

While such covert actions by state actors are nothing new (assassinations, secret service, etc.), the effectiveness of deniability increased because of physical contact being unnecessary for most of these attacks. For the same reason, attacks are also more likely to stay undetected and can therefore be executed over a longer time.

This results in a big problem for cybersecurity research: Only attacks that were found can be analyzed but the news show over and over that attackers can stay in a system for multiple years without being detected and are sometimes found only by accident. Therefore, we need to expect that for every found attack there are many more that are still happening and may never be detected.

Being found on the other side, is also a strategy in itself. Appearing in a critical system can be seen as a warning signal: "We can get here if we want to and we want you to see us". This can be used to intimidate the enemy and spread distrust in the state about the own defense capabilities (Cormac and Aldrich 2018).

VICTIMS

It is important to highlight that different agendas result in different targets for cyber attacks. While the attack on 'soft goals' like airports and general infrastructure can have a big effect on the trust of the public in their government (and the fear of another state), an attack against governmental institutions are normally made to access secret information and to collect intelligence against an (potential) enemy. Like normal "war", there is not one single goal to destroy the enemy physically but many different ones (Iasiello 2015).

Less mentioned are attacks on private individuals in the context of state security. Attacking and accessing the system of the right person can be used to gain information either about the person or about their role in a company or government. If attackers find something which can be used to blackmail the person they have the leverage to bring this person to work in their interest. If they may find out that the person uses the same USB stick both on their private and their company device, they have a perfect entry point without the need to penetrate the system from outside.

The focus of defense policies is still critical infrastructure though, which is basically "all systems and assets whose incapacity or destruction would have a debilitating impact on the national security and the economic and social well-being of a nation." (Dunn Cavelty 2015, 439). An attack can lead to whole cities (for example if multiple hospitals are without their IT system) or even the whole country (it is an open secret that the weapon developments of North Korea are manipulated by foreign state actors which lead to many failed rocket starts) being impacted.

FRAMING CYBER THREATS

Plausible deniability and weakened capabilities to determine the cyber strength of enemies can lead to a very open field for political actors to frame "imminent" dangers for their own interest. The line between cyberterrorism and cybercrime is very thin and is most of the time only a question of definition (Bendrath, Eriksson, and Giacomello 2007). There can be made a difference between hacktivism, cybercrime, cyber espionage, cyber sabotage, cyber terror, and cyber warfare. Nevertheless, the lines between those definitions are vague and depend on the person using them (Dunn Cavelty 2008).

This uncertainty results in an open playing field for political actors to make cyber threats what they want. Because no one knows what can and will happen in the next few years, it is also a fruitful ground for Securitization, therefore the trend of political actors to frame events as exceptional dangers and therefore also ask for extraordinary measures to fight those dangers like interference with fundamental rights. An example is the Patriot Act after 9/11 (Bendrath, Eriksson, and Giacomello 2007; Gorr and Schünemann 2013).

CYBERSECURITY IN INTERNATIONAL RELATIONS

In the realm of national security, just over a decade ago, cyberattacks were "missing entirely" from global threat assessment reports prepared for the US Congress; today, cyber risks dominate national security concerns (Sanger 2018, xii). There is an observable dispersion of offensive cyber capabilities: states do not hold a monopoly of this class of weapons; in fact, they largely depend on the private sector to develop such capacities. (Seligman 2018, 51) This fact is set in the wider phenomenon of the empowerment of non-state actors. Despite the advantages that private actors hold in cyber technology, states remain the dominant global actors. (Kello 2017, 161) One reason for this is that they can flexibly and effectively harness other sectors for their objectives.

Lucas Kello in his book The Virtual Weapon argues that cyber politics exhibits two primary conditions: the traditional state's system, and the "chaotic 'global' milieu" of non-traditional actors, (Kello 2017, 12) and he attempts to explain "how these two universes converge and collide". (Kello 2017, 12) When we see cases of governments collaborating with criminal organizations to further their policy goals, this is an example of a convergence of these two realms. An important consequence of the rise of cyber technologies is a heightened state of global anarchy, comparable to the seas in the age of privateering. (Egloff 2015)

CYBERWARFARE AND REALITY

The main advantage of cyber warfare is that it uses an asymmetric strategy. The higher the technology of a potential enemy is advanced, the higher is the risk that there are security flaws in the system because of its complexity. Contrary to the traditional military field, a nation-state is more likely to be a good target the better equipped he is (Iasiello 2015). While cyber weapons have many features that make modern warfare more dangerous and less assessable, there is a low chance that there will be a war in its full form with cyberspace as its only battlefield. Realistically, it will be one of many battlefields next to traditional military attacks and information propaganda to achieve a broader goal (Iasiello 2015).

This also means that it is highly unlikely that state actors who concentrate a large part of their resources on cyber capabilities would try to start a war with a state stronger in traditional military tactics. Because even if they succeed in sabotaging for example the electric grid, a counterattack via drone strike or a missile would inflict longer lasting and more fatal damage on them. Fittingly, most of the observed cyber activities executed against state targets have come during times of diplomatic tension and conducted largely by non-state actors operating as state proxies. They are therefore more of a tool to keep the enemy on its toes but not to go in full war mode (Iasiello 2015).

PROJECT GROUP

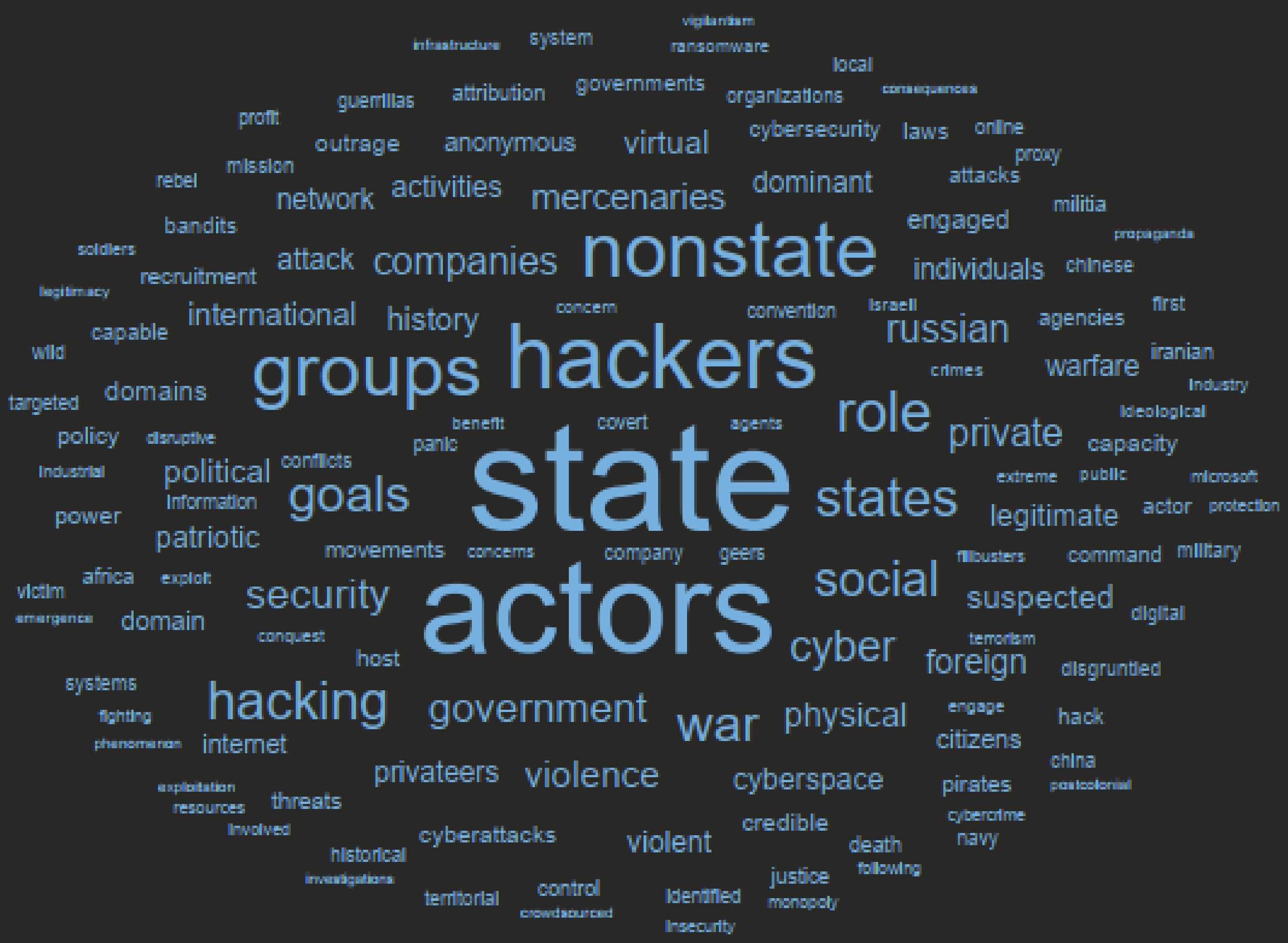
Outsourcing of State Cyber Goals to Non-State Actors

CHAPTER 2

PRIVATE ACTORS

Wordcloud of Key Concepts

Chapter 2: Private Actors



Data source: Chapter 2

CONTENTS

INTRODUCTION

CHAPTER 2

Among other elements, the overwhelming role of non-state actors makes the cyber domain distinctive from all the other domains of operations: land, sea, air, and space (on the discussion of cyberspace as a separate domain, see, for example: Allen & Gilbert, 2009; Bunker & Heal, 2014; McGuffin & Mitchell, 2014; Leventopoulos & Benias, 2017). Historically, however, the nexus between the state and non-state actors has been an ever-present concept; their cooperation and the conversation on legitimacy, are not new. In fact, on land and the high seas - as the primary domains of historical warfare and politics - violent non-state actors have played a significant role (Thomson, 1994), extending the power of the state until several geopolitical agreements made their role officially unwanted.

The subsequent illegitimacy of certain non-state actors made it harder to trace the connection between the state and non-state. These covert actors serve as proxies to a state's goals without implicating the state in their activities. If well hidden, any proof of the connection is plausibly deniable , and states have used that uncertainty to sponsor activities and achieve policy goals before. This issue of tracing relationships is even larger in cyberspace, where it is already difficult to find out who is behind an attack at all (Clayton, 2005).

Yet as in the physical world, many non-state actors undertake activities of their own accord, aligning themselves - inadvertently or on purpose – with the goals of a state. Taking the existence of militia, vigilantism and crowdsourced naming-and-shaming as examples, individuals sometimes organize in groups to fulfill what they see as a space to further the dominant patriotic or ideological agenda (Hare, 2017), or a metaphorical and virtual vacuum of state capacity and in some cases, blatant state failure (Moncada, 2017; Cheong & Gong, 2010; Seraccino-Inglott, 2017). Because of the daily cases in the cyberspace involving many such actors, it is never easy to ascertain whom the state may sponsor, and whom it does not.

Still, many legitimate actors have provided an overall supportive role. Either by helping bolster the security of various states and their citizens, or by engaging in activities that promote the common values, these individuals, groups and organizations have contributed to making the Internet free and open to all. Although more recent trends predict an increasingly fragmented Internet, their contribution needs to be recognized.

	Allocation		**Ownership**	
Decision-making authority	**Authoritative**	**Market**	**State**	**Nonstate**
State	Loan troops to ally	Lease troops to ally	Modern standing army	Privateers
Nonstate	International brigades	Soldier of fortune	Filibusters	Pirates

Source: p. 8, Thomson, 1994.

Purely looking at the cyberspace, who are the hackers and what are they motivated by? One typology proposed in 2001 provides a general overview (Barber, 2001). According to groups, they are either script-using amateurs ("script kiddies"), capable hackers, and profit-motivated crackers. According to motives, their interests range from curiosity, vandalism and hacktivism, to industrial espionage, extortion and fraud, and information warfare – but also security-building 'white hats' (further defined below; p. 3, Barber, 2001). Nonetheless, the typology does not represent the full spectrum of activities that has emerged in the 20 years since the concepts were coined.

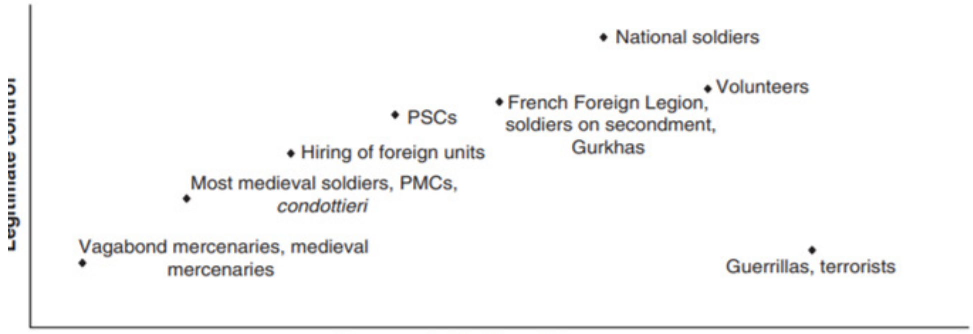
To look at the evolution of non-state actors from the conventional domains of land and sea to the information/cyber domain, we use the common motives as examples to compare upon. Juxtaposing the historical and modern concepts of violence and the virtual of today, we hope to illustrate the variables at play with non-state actors whose alignment with a state actor's goals is motivated by: profit and personal gain; patriotism and ideology; exploitation, revenge, rebellion and resistance; moral outrage and perceived insecurity; and other sets of parameters.

and the virtual of today, we hope to illustrate the variables at play with non-state actors whose alignment with a state actor's goals is motivated by: profit and personal gain; patriotism and ideology; exploitation, revenge, rebellion and resistance; moral outrage and perceived insecurity; and other sets of parameters.

PROFIT AND PERSONAL GAIN

Profit and personal gain were some of the ubiquitous motives throughout history. Across civilizations from Aztecs (Townsend, 2019) to the Celts (p. 56, Chadwick, 1970), violent non-state actors gained resources and reputation by engaging in both own and foreign warfare. However, what differentiated state actors such as soldiers with salaries from non-state mercenaries and profiteers?

Political scientist Sarah Percy (2007) proposes to look at the level of legitimate control and the attachment to a cause, rather than the foreignness or the monetary reward. By putting the focus on the concept of legitimacy in (jus in bello) and behind (jus ad bellum) combat, it is possible to compare different groups and understand the boundary between state and non-state.



Source: Percy (2007)

VIOLENT: Mercenaries, Privateers, Private Military and Security Companies

While difficult to properly delineate in law and theory (Percy, 2007), mercenaries can be defined as actors, groups or entire companies which are paid to wage war on behalf of a sovereign state (For a deeper legal definition, see: International Convention Against the Recruitment, Use, Financing and Training of Mercenaries, December 4, 1989). From the ancient civilizations (see, for example: Trundle, 2004), through the middle and later ages (see, for example: Percy, 2007; Thomson, 1994; Ingrao, 1987) and up until the 19th century (see, for example: Dempsey, 2002), mercenaries were part and parcel of interstate conflicts (Avant, 2000).

From de left to right: Xenophon, Marble bust, n.d., National Gallery Berlin, Artist unknown; Condottieri, ca. 1472, Leonardo Da Vinci; Hessian troops in British pay in the US war of independence, 1799, Conrad Gessner; Photo Portrait of Edward S. (Tex) O'Reilly, 1918, Photographer unknown. Appeared in O'Reilly, E. (1918). Roving and Fighting: Adventures Under Four Flags. New York City, NY: The Century Co.

As fighting between states ebbed and flowed, and mercenaries and privateers became too uncontrollable (Percy, 2007), costly (see, for example: Chapter XII, Machiavelli, 1521) or an impediment to geopolitical goals, the willingness to use mercenaries at land and sea subsided. States signed a number of treaties which led to antimercenarist laws (p. 83 & 86, Thomson, 1994). Thus, the idea of a profit-seeking soldier slowly went out of favor.

At sea, pirates were useful to a state when they attacked vessels of another state. With a Letter of Marque – an English document formalizing the legitimacy of a naval non-state aggressor as working on behalf of the state (p. 22, Thomson, 1994) – pirates, merchants and naval officers were covertly or overtly officiated as privateers.

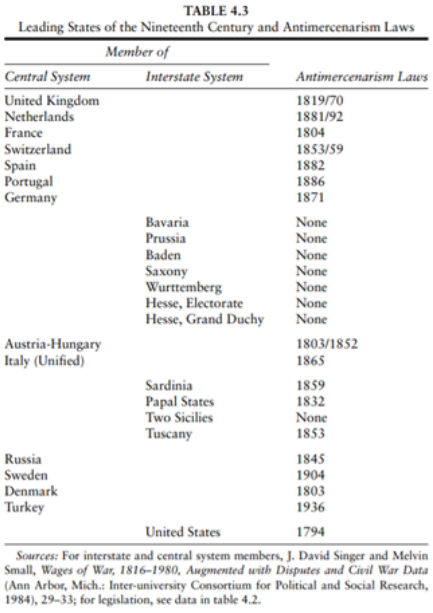


TABLE 4.3
Leading States of the Nineteenth Century and Antimercenarism Laws

Member of		
Central System	*Interstate System*	*Antimercenarism Laws*
United Kingdom		1819/70
Netherlands		1881/92
France		1804
Switzerland		1853/59
Spain		1882
Portugal		1886
Germany		1871
	Bavaria	None
	Prussia	None
	Baden	None
	Saxony	None
	Wurttemberg	None
	Hesse, Electorate	None
	Hesse, Grand Duchy	None
Austria-Hungary		1803/1852
Italy (Unified)		1865
	Sardinia	1859
	Papal States	1832
	Two Sicilies	None
	Tuscany	1853
Russia		1845
Sweden		1904
Denmark		1803
Turkey		1936
	United States	1794

Sources: For interstate and central system members, J. David Singer and Melvin Small, *Wages of War, 1816–1980, Augmented with Disputes and Civil War Data* (Ann Arbor, Mich.: Inter-university Consortium for Political and Social Research, 1984), 29–33; for legislation, see data in table 4.2.

Source: p. 83, Thomson, 1994

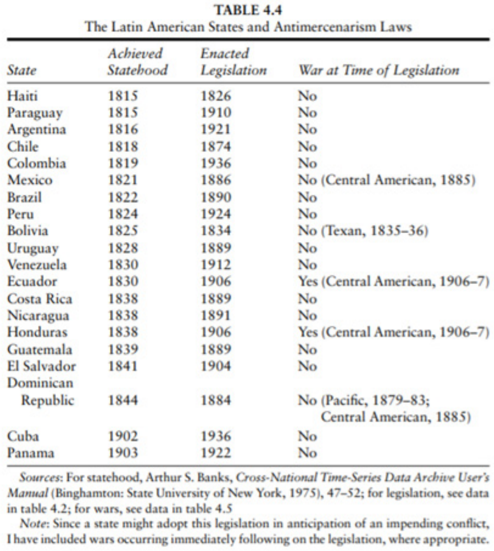


TABLE 4.4
The Latin American States and Antimercenarism Laws

State	*Achieved Statehood*	*Enacted Legislation*	*War at Time of Legislation*
Haiti	1815	1826	No
Paraguay	1815	1910	No
Argentina	1816	1921	No
Chile	1818	1874	No
Colombia	1819	1936	No
Mexico	1821	1886	No (Central American, 1885)
Brazil	1822	1890	No
Peru	1824	1924	No
Bolivia	1825	1834	No (Texan, 1835–36)
Uruguay	1828	1889	No
Venezuela	1830	1912	No
Ecuador	1830	1906	Yes (Central American, 1906–7)
Costa Rica	1838	1889	No
Nicaragua	1838	1891	No
Honduras	1838	1906	Yes (Central American, 1906–7)
Guatemala	1839	1889	No
El Salvador	1841	1904	No
Dominican Republic	1844	1884	No (Pacific, 1879–83; Central American, 1885)
Cuba	1902	1936	No
Panama	1903	1922	No

Sources: For statehood, Arthur S. Banks, *Cross-National Time-Series Data Archive User's Manual* (Binghamton: State University of New York, 1975), 47–52; for legislation, see data in table 4.2; for wars, see data in table 4.5

Note: Since a state might adopt this legislation in anticipation of an impending conflict, I have included wars occurring immediately following on the legislation, where appropriate.

Source: p. 83, Thomson, 1994

As such, pirates were allowed to pillage and destroy vessels of other nations, provided that they leave the merchants and navies of the host state undisturbed. As time moved on and peace treaties between the main sponsors, England, France and Spain, came about, states had to address the damaging role of raiders on the high seas. In a show of force, the golden age of piracy and privateering was swiftly brought to an end (Thomson, 1994).

In today's role, companies specializing in the protection of the shipping industry are known as privately-contracted armed security personnel (PCASPs; Titahena & Sumser-Lupson, 2013; Spearin, 2014). Other examples include floating armories that circumvent the strong arms control protocols of state maritime zones (Chapsos & Holtom, 2015), as well as government-mandated vessel protection detachments (VPDs; Zwanenburg, 2012; Farnelli, 2015).

Henry Morgan, 1684, Alexandre Exquemelin; and Sir Francis Drake, 1590, Marcus Gheeraerts the Younger

Legitimation and then subsequent delegitimation of the violent non-state actors motivated by profit led to an emergence of a different type of actor. Taking the roles of international private companies in the 20th century, colonial and post-colonial soldiers-for-hire organized in private military and security companies (PMSCs; Avant, 2007). Undertaking different roles in the spear model of warfare (see, for example: McFate, 2014; Singer, 2003; Kaldor, 2013), PMSCs provide services ranging from consultations and supply to protecting key assets and engaging in combat. Tip-of-the-spear cases involved companies fighting as proxies in the (post-)colonial conflicts against guerrillas, independence fighters and communist-backed militia of the 20th century Cold War (Voss, 2014), and other notable groups such as the Executive Outcomes and the "Wild Geese" of South Africa which organized coups across Africa (Singer, 2003).

Nonetheless, the post-colonial movement led to an international ban of mercenaries (UN Resolution 44/34), albeit a controversial and ineffective one (Milliard, 2003). Today, the foreign regiments such as the French Foreign Legion (Koller, 2013) or the British Brigade of Gurkhas (Rathaur, 2001; Chisholm, 2015) serve as auxiliaries. Many of the PMSCs fulfill a logistical or supply role (Bearpark & Schulz, 2007) in the wake of controversies of the conflicts in 2000s (McFate, 2014).

VIRTUAL: Hackers-for-hire, Cybersecurity Companies

Since the very beginnings of the Internet, capable individuals have found a market for their niche in the information-cyber domain (Maurer, 2018). The enduring vernacular coined in the 90's (Gattiker, 2004; Brown, 2015) divides computer hackers according to the motives they represent: black hats, who hack and exploit vulnerabilities for personal gain; white hats, who market their skills in security or protection; and grey hats, whose motives are a blur of the former two.

Services which black-hat hackers-for-hire can offer to states – also termed cyber mercenaries (Maurer, 2018) or cyber privateers (Egloff, 2018) – have been a credible concern for the past few decades (Zilber, 2018; Avramov, 2019; Egloff, 2017; Jones, 2017; Hare, 2017; Ricks, 2014; Apps, 2011). At times, states use these services inadvertently: one example in 2010s involves a hacker from the UK who helped a private company owner steal carbon credits and later resell them to unwitting companies and state agencies (Funk, 2015). However, most concerns center around deliberate use. The credible assumption underlying the Shadow Brokers, a network of hackers and leakers of unknown origin (Schneier, 2017) who operated in the years before the Snowden case, is that they sold the tools they extracted from the US National Security Agency (NSA) to various state and non-state actors, including those behind the WannaCry attack originating from North Korea (Shane, 2017; Goodin, 2019). Like floating armories, these networks provide hacking tools to paying customers. Using the analogy of the high seas, suspicions have arisen that governments are releasing proverbial letters of marque (Apps, 2011), and in the 2009 GhostNet attacks, the US state suspected the Chinese state of covertly sponsoring hackers in such a way to attack its infrastructure (USCC, 2009).

More conventional information leakage for money has a physical component, whether the actor is external or internal to the system. The salient example of external threats has been the 6th January 2021 riot on the US Capitol, where some of the homegrown actors allegedly attempted to sell the hardware found onsite to foreign governments (currently only Russian; BBC, 2021). For insider threats, the Shadow Broker exploit led to the prosecution of an NSA contractor, who was initially suspected to have leaked the tools (Schneier, 2017). These are credible vulnerabilities to existing systems (Steele & Wargo, 2007), and security plans for nuclear power plants and weapon production facilities already incorporate such internal risks from disgruntled or profit-seeking employees (Vlahakis & Partridge, 1989; Jenkins, 2008; Ahn et al, 2015; Masood, 2016). It would be devastating if capable internal employees or external non-state hackers managed to access nuclear secrets to sell to the highest bidder (Futter, 2016).

In terms of grayer hats, there has been a proliferation of PMSCs offering cyber services. In 2011, there have been at least five PMSCs which have marketed cyber-protection services to the US government (Palou-Loverdos & Armendariz, 2011), some of which garnered hundreds of millions of USD in government funding since 2015 (Maurer, 2018). Others offered information systems-related services to other governments as well (O'Brien, 2000). Contemporary worries are that current laws allow for the use of PMSCs in cybersecurity and cyberwarfare (Liu, 2015), where they are already partially involved (Maurer & Hoffman, 2019; Prem, 2018).

However, the concept of grayness also features black hats who have turned white hats too, whether they were recruited to do so, switched after being imprisoned, or have been offered monetary rewards. The concept of such 'ex-hackers' is salient in the US media especially (see, for example: Sauter, 2016). The US Pentagon has rewarded attempts to hack into its systems, regardless of the hacker's history (Chatfield & Reddick, 2017), and other agencies (most notably FBI) have hired individuals from the black hat world (Peterson, 2015). After being imprisoned, the carbon credit hacker moved onto helping the UK government and private firms improve their security (Funk, 2015).

Finally, white hat hackers represent the private auxiliaries to state capacity to make itself and others secure – they are the protection detachments of information "vessels." Discussed further in the text, they range from individuals and companies specializing in cybersecurity (Watkins, 2018) to "bug-chasing" bounty hunters (Akgul et al, 2020). The recent SolarWinds attack in the US, for example, was only reported on by the FireEye company (Sanger, Perlroth & Barnes, 2021), after the government-placed tripwires and alarm systems failed to detect the malware. Due to the more private nature of the markets in Western countries, software firms have been on the forefront of using AI technology to monitor IT networks for abnormal behavior (Taddeo & Floridi, 2018). Due to the nature of and connotations attached to their work, however, white hat hackers have at times faced difficulties in marketing their services with clear intentions (Watkins, 2018).

As in other domains, the uncontrollability of non-state actors has motivated international agreements to try and reign in the phenomenon. The 2001 Budapest Convention on Cybercrime by the Council of Europe (2001, no. 185) is the first international treaty that regulates crimes committed in cyberspace, by extent regulating the acceptability of states engaging in certain activities. The 2013 Tallinn Manual (Schmitt, 2013) complements the attempt by providing a non-binding instruction on the applicability of current international law on issues pertaining to cyber warfare, including mercenarism (p. 89, Schmitt, 2013) and conscription of non-state actors (p. 90, Schmitt, 2013). However, the low number of signatures on the former document, and the non-binding nature of the latter, make regulation of virtual non-state actors inconclusive.

PATRIOTISM AND IDEOLOGY

PRIVATE ACTORS

Since the dawn of civilizations, patriotism and nationalism have been the pervasive and universal element of state-making (Kohn, 1944). Using volunteers, conscripts, citizen and professional armies, national unity and war have defined the boundaries of modern nation-state (see, for example: Avant, 2000; Williams, 2005). According to the perspective provided by the political scientist Charles Tilly (1985), the state actors undertook predatory expansionist "entrepreneurship" when war-making (cf. Becke, 2019); building a state that was based on continuous conquest and extraction of resources, taxes and labor required a regular inflow of individuals who will fight for a cause.

The concept of mission command – the ability of individual soldiers, officers and other military elements of taking independent decentralized decisions aligned with the general strategic goal (i.e. mission command, auftragstaktik) – has existed in various military organizations throughout the world (see, for example: Nelsen, 1987; Storr, 2003; Shamir, 2011; Josefsson, et al, 2019). However, at times, only non-state actors could fulfill the roles that state actors could or would not, and the patriotic actors represented a niche of extending state capacity.

However, it is not easy to trace who are state actors at all. A common theme behind the difficult traceability in physical and cyber domains is the idea that state actors will pose as regular individuals to avoid being held accountable, because the existence of powerful non-state actors in these domains dilutes the higher capabilities of state actors. In history, ununiformed police agents disrupted protests and broke strikes, and soldiers engaged in a variety of covert operations. In the modern domains, agents need to take even less physical precautions (albeit substituting them for more digital ones; p. 24, Sigholm, 2016). The asymmetric advantage of plausible deniability exists because state actors are identifiable by markings and thus legitimate targets in war under the Geneva Convention. In the cyber domain, there are no such markings other than geolocation or identification, and there is no threshold when the conflict becomes a war.

Benefits	Drawbacks
Gaining the initiative - element of surprise	No direct control of non-state actors
Plausible deniability	Risk of unintended collateral damage
Can choose target and attack vector	Targeting of own resources
Determinate scale and duration of attack	Escalation to conventional war
Exploit legal uncertainties	Labeling as sponsor of terrorism
Possibility of rapid attacking-by-proxy	Backlashes (blackmailing, etc.)

Source: Benefits and drawbacks of using non-state actors in cyberspace operations, p. 24, Sigholm, 2016

Kerr & Murphy (2017) posit that because of difficult international law, states engage in hidden hacking even when doing so for legitimate reasons. The network investigative techniques that seek to identify cybercrime on the Dark Web are cross-border, and thus face an international relations issue with less-cooperative states. Still, as international cooperation on transborder crime regulation increases, it is expected that the less justification will remain for using covert means to conduct legitimate operations.

However, state-making also eventually collides with other movements and ideologies. Across different nation-states, many groups engaged in irregular warfare against the dominant state, gathering the epithets of guerrillas, insurgents and terrorists (see, for example: Merari, 1993; Byman, 2008; Moghadam, Berger & Beliakova, 2014; Carter, 2016). Various ideologies from the late modernity until today fueled the uprisings (Goodwin, 2016); to what extent states benefit from terrorism in another state is debatable, although proxy violence based on same ideological precepts has been an element of the Cold War (e.g. Paszyn, 2000; Hoekstra, 2018). The role of these actors, although motivated by ideological or ethno-nationalist movements, is discussed separately.

VIOLENT: Filibusters, Paramilitaries, Guerrillas

Although the historical distinction between the state and the non-state has mostly been blurry, the Vikings (Raffield, 2019), crusaders (Alessio & Villegas-Aristizabal, 2020), colonialists (Adams, 1996) and conquistadors (Townsend, 2019) undertook nomadic "entrepreneurial" conquest with or without support of the dominant state, to appropriate new territories and acquire slaves. A novelty of the American history, filibusters were self-organizing actors who engaged in territorial expansion and organized coups under the idea of American exceptionalism (see: Manifest Destiny), often with support of private investors who sought to benefit from the Latin American land they targeted (Thomson, 1994).

William Walker, n.d., Author unknown

With the prohibition of slavery, the introduction of the Homesteading Act, the diversion of investors to infrastructural projects, and the strengthening of the concept of state sovereignty (p. 141, Thomson, 1994), the original filibusters and colonialists slowly disappeared. Privateers who were originally navy captains or merchants returned to their original functions. In modern history, however, foreign fighters or irregulars have taken to existing conflicts to create theocratic states (Honig & Yahel, 2017), participate in "liberation" (in ideological terms, at least; cf. second and third waves of terrorism, Rapoport, 2004; c.f. Richardson, 1976; Wickham-Crowley, 1987; Reeves & Wallace, 2015; Galeotti, 2018; Koch, 2019), independence suppression (Voss, 2014), or even organize coups for more sympathetic governments (e.g. Singer, 2003; Kreegipuu & Lauk, 2007; Hoekstra, 2018; Baesso Moura, 2020).

Finally, paramilitaries represent the (tacitly) state-sponsored actors which are not subject to state control, yet participate in conflicts or repression. From the so-called "death squads" to paramilitary formations (e.g. Sanford, 2003; Auley, Tonge & Shirlow, 2009; Oude Breuil & Rozema, 2009), various groups played a role in solidifying state control or supporting nationalist expansionism, respectively, without facing similar accountability.

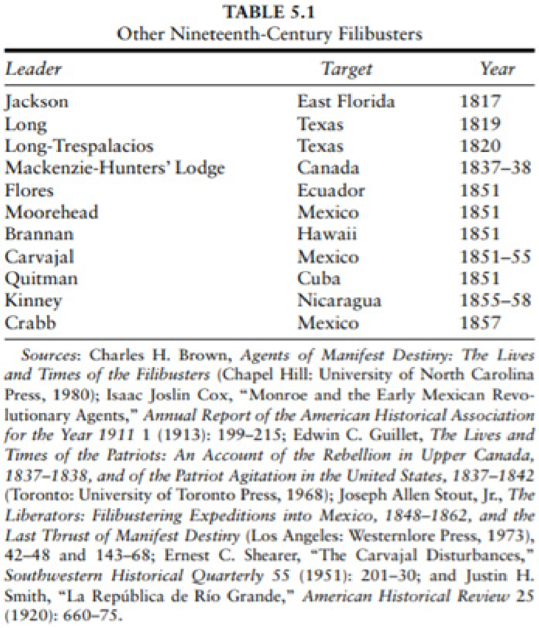


TABLE 5.1
Other Nineteenth-Century Filibusters

Leader	*Target*	*Year*
Jackson	East Florida	1817
Long	Texas	1819
Long-Trespalacios	Texas	1820
Mackenzie-Hunters' Lodge	Canada	1837–38
Flores	Ecuador	1851
Moorehead	Mexico	1851
Brannan	Hawaii	1851
Carvajal	Mexico	1851–55
Quitman	Cuba	1851
Kinney	Nicaragua	1855–58
Crabb	Mexico	1857

Sources: Charles H. Brown, *Agents of Manifest Destiny: The Lives and Times of the Filibusters* (Chapel Hill: University of North Carolina Press, 1980); Isaac Joslin Cox, "Monroe and the Early Mexican Revolutionary Agents," *Annual Report of the American Historical Association for the Year 1911* 1 (1913): 199–215; Edwin C. Guillet, *The Lives and Times of the Patriots: An Account of the Rebellion in Upper Canada, 1837–1838, and of the Patriot Agitation in the United States, 1837–1842* (Toronto: University of Toronto Press, 1968); Joseph Allen Stout, Jr., *The Liberators: Filibustering Expeditions into Mexico, 1848–1862, and the Last Thrust of Manifest Destiny* (Los Angeles: Westernlore Press, 1973), 42–48 and 143–68; Ernest C. Shearer, "The Carvajal Disturbances," *Southwestern Historical Quarterly* 55 (1951): 201–30; and Justin H. Smith, "La República de Río Grande," *American Historical Review* 25 (1920): 660–75.

Source: p. 83, Thomson, 1994

In terms of extreme violence, terrorism is a salient modern and global phenomenon. Political scientist David Rapoport (2004) posits that in its most extreme and ideological forms, political violence followed four historical waves: the anarchist wave (pre-1920s); the anticolonial wave (1920s – 1960s); the New Left wave (1960s – 1970s); and the religious wave (post-1979). In pursuit of the next elusive fifth wave, other political scientists ask whether the modern emergence of terrorist semi-statehood (Honig & Yahel, 2017) or right-wing terrorism (Auger, 2020) qualify.

VIRTUAL: Cyber Privateers, Patriotic Hackers, Cyber-terrorists?

Territorial appropriation, resource extraction or the conquest above others are unattainable goals for hackers, if not for purely physical reasons, then because their attainment would be unacceptable in the international relations of today. What motives remain for patriotic hackers?

The concept of mission command in the cyberspace allows one to take personal responsibility in attaining certain policy goal. In the words of the oft-cited military theorist Carl von Clausewitz (1832), “war is not an independent phenomenon, but the continuation of politics by different means;” cyberattacks are thus another avenue for both war and politics. In the conception of modern militaries, a cyber levee en masse (Croninn, 2006; p. 90, Schmitt, 2013) or mission command in cyberspace (Josefsson et al, 2019) open the space for a new Manifest Destiny (Leaven & Dodge, 2010) around which filibusters and paramilitaries can organize. Given the increasingly lower level of engagement needed, individuals and groups can be effective with the new technologies.

Political scientist Florian Egloff (2016) found the emergence of cyber privateers as the concept parallel to the colonialist mercantile companies (Egloff, 2018) and navy privateers (Egloff, 2017), supported in their missions without being state actors themselves. Patriotic hackers, a term iterated by the Russian President Vladimir Putin in 2017 (BBC, 2017) and investigated by academics (Hare, 2017; Lokot, 2017), contrasts that idea with the concept of a self-motivated individual whose actions cannot always be controlled. With little chance for attribution, mission command policy in policy in cyberspace is difficult to prove (see, for example: Galeotti, 2018).

The advent of this soft, hybrid war (Lucas, 2017) where virtual non-state actors regularly participate is the underpinning principle of the new idea of a "cyberwar". While the information/cyber domain is commonly referred to as the fifth domain of warfare (Bunker & Heal, 2014; McFate, 2014), the term has gained traction in recent decades (see, for example: Singer & Friedman, 2013; Lucas, 2014; Liu, 2015; Foxall, 2016) due to the ongoing nature of disruptive cyberattacks around the world. Most attacks remain without physical consequences; even in attributed large-scale exploits (e.g. DoJ, 2018; CISA, 2020; Stubbs, 2021), radical action is difficult to justify due to limited disruption. However, the examples of attributed Iranian hacks on the US dam (Carlin, 2016) and the Israeli airstrike on the suspected Hamas hacker headquarters (Hewman, 2019) show the potential future of the trend where "patriotic hackers" bring consequences and initiate a geopolitical response in the physical domains.

The following cases illustrate how patriotic hackers, cyber privateers or undercover state actors operated under fuzzy attribution throughout the world, organized around the large capable states which are deemed their hosts:

CASE 1

Because of their targets, methods and quantity, cyber-operations of Russian origin are some of the most salient in the world. During the 1994 war in Chechnya, hackers on both sides defaced government websites to spread propaganda (Geers, 2017). In the 2008 conflict with Georgia, the involvement of Russian "volunteer cyberwarriors" under the names Energetic Bear and Dragonfly was suspected in disrupting the infrastructure in South Ossetia and Abkhazia (The Economist, 2008; Morozov, 2008; Morozov, 2009). When the government of Estonia moved a Soviet World War 2 memorial farther from the center of the city of Tallinn, hackers from Russia targeted Estonian infrastructure for three weeks. In the 2015 conflict in Ukraine, a group under the names CyberBerkut hacked and shut down the websites and information security systems of the local government in Crimea (Boulet, 2015).

In the 2016 US election hacks, the cyberattacks which the US attributed to 12 Russian state intelligence officers (DoJ, 2018) was dismissed by Vladimir Putin as potentially the work of patriotic Russian hackers instead (BBC, 2017). Following the thread, the subsequent US attribution of the 2017 NotPetya hacks (US White House, 2018) and the ongoing SolarWinds exploit (compared with the Turla group, suspected to be FSB-sponsored, Stubbs, 2021; FBI, 2021) has led to little developments (US White House, 2021). Indeed, Microsoft identified the Russian-based Strontium group as hacking more than 200 political entities related to the 2020 US election (Burt, 2020). Aside from specific examples, the Russian government has been suspected of using and/or allowing non-state proxy groups such as troll farms (Luceri, Giordano & Ferrara, 2020) or organized crime groups (Sullivan, 2018).

CASE 2

In the years up until 2018, China has benefited from the cyber fervor from the communist youth (Pan, 2018). In 2001, hackers from China and the US engaged in patriotic hacking against each other, with the Californian electric power grid disabled by the group called Honker Union of China (Geers, 2017). In 2009, the Chinese government was suspected of releasing a bounty on infrastructural disruption in the US, in what later came to be termed the GhostNet attacks (USCC, 2009). Among other examples, the Chinese government is suspected of using non-state actors engaged in propagandization or trolling (Creemers, 2016; Bradshaw & Howard, 2017; Linvill & Warren, 2020). The Chinese-based Zirconium group was identified by Microsoft as attackers of high-profile politicians associated with the 2020 US election (Burt, 2020).

CASE 3

The examples of the US-originating cyber-engagement frequently center on covert. The 2009-2010 hack of the Iranian Natanz nuclear plant, using the Stuxnet malware developed by the Equation Group, is widely believed to be the work of the US and Israeli governments, although attribution was never claimed (Anderson, 2012; Josefsson et al, 2019). The Equation Group itself stands behind the 2016 Shadow Brokers leaks (Gallagher, 2016), and is alleged to be the non-state arm of the NSA itself (Goodin, 2017). It is also believed that the NSA and GCHQ conducted man-in-the-middle attacks by spoofing the Google website (Moyer, 2013). In 2020, an investigation uncovered a Swiss company that is believed to be a CIA front, that as a non-state actor sold compromised encryption equipment to foreign states (Miller, 2020).

CASE 4

Israeli actors are attributed to the Stuxnet Iranian Natanz hack (Anderson, 2012). Israeli hackers have also engaged in hacks, leaks and propaganda war with Palestinian hackers (Geers, 2017). Israel is also the first known state to launch an airstrike based on cybersecurity concerns (Hewman, 2013).

CASE 5

Iranian actors are implicated in several attacks. The Ajax Security Team, a hacking group behind the 2013 Operation Safron Rose, is believed to originate from Iran (FireEye Inc, 2013). The 2016 hacks involving the US banking sector attributed to actors from Iran, also included hackers gaining access to the control flow of a local dam (Carlin, 2016). In the days leading up to the US election in November 2020, Iranian hackers distributed online death threats to US election officials; the US FBI attributed the attack to several state actors (Federal Bureau of Investigations, 2020), which the Iranian spokesmen denied, claiming Iran to be the largest victim of cyberattacks instead (Hosenball, 2020). Iranian-based Phosphorus group was identified by Microsoft as attacking personal accounts of the US republican party (Burt, 2020).

CASE 6

North Korean hackers are implicated in the 2014 breach against Sony Pictures, the Bangladeshi bank heist, and the 2017 WannaCry ransomware attack with more than 2 million victims in hospitals, companies, universities and other organizations in the US (Bossert, 2017; CISA, 2020); the Hidden Cobra and Lazarus groups are suspected by the US to originate from North Korea (CISA, 2017).

Other cases include: Indian and Pakistani hackers conducting cyberattacks against each other in a show of rivalry (Baezner, 2018); Serbian hacking group "Black Hand" disabling NATO equipment using Ping bombardment strategy during the 1999 bombing of Serbia (Verton, 1999; Geers, 2017); Egyptian Cyber_Horus group attacked and defaced Ethiopian government websites in 2020 over the dispute on the Ethiopian dam construction (Zelalem, 2020).

Finally, hacks for guerrilla and insurgent causes have yet to gain traction, although in 2016, a member of the Hacking Team network stole €10K in Bitcoin and sent it to the communist group in Rojava (Porup, 2016). However, even as an already-salient concept, cyberterrorism is quite disputed (cf. Collin, 1997; Gordon & Ford, 2002; Foltz, 2004; Weimann, 2005; Jarvis & Macdonald, 2014). Because the cyberattacks have not led to direct physical consequences, a cyberterrorist is currently only a terrorist actor which engages in propagandization, radicalization, or death threats online. Still, the future of cyber-physical systems will potentially reveal an integration between the physical and the digital (Collin, 1997).

EXPLOITATION, REBELLION, REVENGE AND RESISTANCE MOTIVES

PRIVATE ACTORS

Inherent to many societies are those who remain on the margins by finding themselves in a foreign, hostile or otherwise unaccepting territory, or operate on the margins and reject the dominant system. In ways defined by the sociologist Robert K. Merton (1938), these so-called "deviants" have five possibilities of adjustment to societal goals and methods:

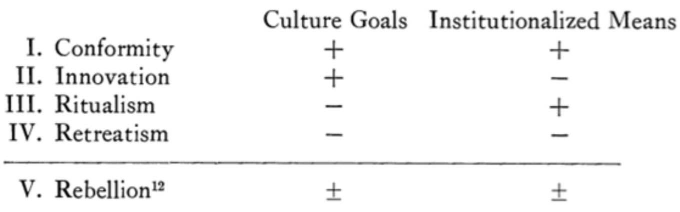
1. Conform to the goals defined by the dominant culture and the institutionalized means to achieve them.

2. Accept the goals, but reject the traditional or legitimate means to achieve them, and innovate with the methods (including criminal activities).

3. Reject the goals, but engage in ritualistic routines to achieve them.

4. Reject the goals and retreat from ever achieving them.

5. Rebel against both goals and institutionalized means by replacing both with alternatives.



	Culture Goals	Institutionalized Means
I. Conformity	+	+
II. Innovation	+	−
III. Ritualism	−	+
IV. Retreatism	−	−
V. Rebellion[12]	±	±

Alternative modes of adjustment or adaptation by individuals within the culture-bearing society or group. Robert Merton, 1938. + is acceptance, - is elimination, +- is rejection and substitution of new goals and standards.

The sociologist and Marxist historian Eric Hobsbawm provides an additional perspective. In his view, a subset termed the “social bandits” or social criminals were primitive rebels of the pre-proletarian world (Hobsbawm, 1959); those who rose up against oppressive regimes or territorial hegemons, often engaged in crime against the dominant society and were seen as heroes by their civil counterparts (Hobsbawm, 1969). Whether such a concept truly existed, the idea of the Robin Hood (Seal, 2009), romantic pirates (Rediker, 2004), and the anarchic nature of Southeast Asian hill communities (Scott, 2010) provide a strong basis. If the conception of the predatory state-making put forward by the political scientist Charles Tilly (1985) holds, the dominant society automatically marginalizes others through conquest.

From these typologies, we focus on those both social and non-social “bandits” in the physical and virtual worlds, who innovate or rebel against the dominant system – i.e. exploit it, resist its grip, take revenge for the grievances it created, or rebel against its territorial hegemony - thereby creating the conditions in which another state can benefit from. Although many rebels later became guerrillas, insurgents, and fighters for independence, we look to their roles when their power has been more constrained.

VIOLENT: Routiers, Brigands, Social Bandits, Saboteurs

Foreign in origin, some actors had a disruptive territorial presence in state other than their own, but had own personal gain in mind. Routiers (also known as coutereaux, roving knights, free companies or vagabond mercenaries) were disbanded mercenaries and soldiers, who during intermittent peace treaties in the Hundred Year War and afterwards, terrorized the French countryside (Percy, 2007) by robbing travelers, “ransoming the villages” and racketeering (see, for example: Froissart, n.d.; Seward, 1999) among other examples (see, for example: Caferro, 1996). At a later stage, the vagabond mercenaries of Cold War postcolonial Africa destabilized the region by fighting for a variety of causes and battles (Mockler, 1969), including the famous clash with the UN peacekeepers in Jadotville, Katanga (modern day Democratic Republic of Congo; Whelan, 2006).

Yet, a parallel motive of the routier type endures. Foreign actors of history were associated with their literary versions of a romantic knight-errant - a trope in literature across cultures, including the bogatyrs, youxia, rōnin on a quest, and wandering bounty hunters of the West – who is the chivalric wandering agents that always help the struggling population.

Juxtaposed with the routiers are the local brigands and robbers: the highwaymen of the medieval history (Akinwumi, 2001) or the Wild West (McGrath, 1987). From pirates to the bandits on the roads, these actors were territorially flexible and mobile, not unlike the transborder criminal enterprises of today. However, their role was often localized. As agents with localities, they sometimes evolved into an image of rebellion against oppression – the social Robin Hood-like bandits. Across the hill tribes of South-East Asia (Scott, 2010), the Hajduci of the Balkan peninsula (Kocic, 2014), the Native American tribes of the Wild West, or the briganti of the Mediterranean (Koliopoulos, 1987; Maffei & Monnier, 1865), the inherent rejection of the main host state provided ample room for some to cooperate with competing state actors (see, for example: Kocic, 2014). Whether as peacetime saboteurs (fifth column in WW2 vernacular) or disruptive elements, their role ultimately rested on the eventual nexus of personal grievances and the opportunity provided by the state rival to the host.

Wives of the brigands visiting their husbands in prison, 1842, Arthur John Strutt. In Strutt, A. (1842). A pedestrian tour in Calabria & Sicily. London: Newby.

VIRTUAL Cyboteurs, Ransomware Groups, ‘Robin Hood’ Hackers, Disgruntled Employees

Even in the early 90’s, hackers were put in the connotational dilemma of being either computer heroes or electronic highwaymen (Hollinger, 1991). Given the ubiquity of cybercrime and difficulty of attribution, it is unclear what role a state may have, if any. Still, three elements of policy goals coincide between a non-state actor and the rival state, in theory if not in practice: gathering industrial secrets, generating chaos, and disrupting infrastructure.

Industrial espionage and sabotage is a credible issue in cyberspace (Thonnard et al, 2012), although not a generally new one. These termed “cyboteurs” are considered to be threats akin to any real manifestation of “cyberterrorism” (Arquilla & Ronfeldt, 2001), with increasing asymmetric power (Danks & Danks, 2018). Industrial cyberattacks bring a credible concern around warlords and other strong actors which may sabotage and essentially hold entire companies hostage (Caltagirone, 2019). In foreign groups, Chinese hacker groups are some of the oft-cited capable actors that engage in patent theft (p. 216, Hannas, Mulvenon & Puglisi, 2013), which arguably brings economic gain to the host country. Keeping the issues of attribution in mind, signaling discontent and eventual retaliation is still one potential mechanism of deterrence for states fighting against such behavior (Meer, 2015).

Although examples of endogenous bandits in cyberspace, social or otherwise, are scarce, disgruntled employees represent a subset of vengeful actors with asymmetric capabilities; it is a concept ubiquitous enough that risk management methodologies handle this as a specific category of insider threats (Steele & Wargo, 2007; p. 267, Wilhelm & Andress, 2010). In 2017, for example, a disgruntled contractor managed to release sewage into the local ecosystem by sending corrupt messages to the managing network, before being identified three months later (Sayfayn & Madnick, 2017). Another disgruntled network administrator for the city of San Francisco managed to lock out all administrators in 2008, generating much concern but without much effect (p. 268, Wilhelm & Andress, 2011). With potentially larger plans, disgruntled employees could pose a much larger threat in the future.

In looking at endogenous or exogenous sources of disruptive or extractive hacks, ransomware groups provide an interesting case. While not attributed to states, these exploits represent the disruption happening from other countries, which, if unchecked by the host state, siphon resources from the victim (often rival) state. In the rising coronavirus crisis, both sides of the proverbial coin targeted the health sector with different goals in mind. After credible concerns that many lives are lost from IT failures and cyberattacks each year (e.g. Donelly, 2018), an uptick in ransomware attacks on hospitals (Muthuppalaniappan & Stevenson, 2020) led to the first death from the consequences directly attributable to a hack (Associated Press, 2020). In other cases, hackers declared their intention to donate the funds generated from hacks or exploits to charity. In 1989, the first ransomware attacker in history, Joseph Popp, claimed to have distributed the attack to fund AIDS research (Waddell, 2016). The secretive Darkside group declared they would give proceeds of some of their hacks to charities (Tidy, 2020), while the CryptoForHealth Instagram page took responsibility for Twitter hackers, stating that the “money will find its way to the right place” (BBC, 2020).

MORAL OUTRAGE AND PERCEIVED INSECURITY

PRIVATE ACTORS

From the Wild West of North America (Little & Sheffield, 1983) to the contemporary Africa (Pratten, 2008), vigilantism has carried the connotation of disproportional folk justice and citizen defense. With examples of racist (Mortensen, 2018) or jihadist vigilantism (Lo, 2019), it is important to distinguish between the two main drivers of vigilante movements: moral outrage and perceived insecurity.

Coined by the criminologist Stanley Cohen (2011), a moral panic is an irrational public phenomenon that occurs when societal values and interests are threatened, in which a scapegoat (i.e. a folk devil) is identified; a moral outrage is the underlying emotion that emerges when moral norm violations are seen (Crockett, 2017). Molded by the mass media, moral panics create a demand for swift justice and punishment (Cohen, 2011). State judiciaries or executive institutions are scarcely prompt, transparent and aligned enough to satisfy the demand, and in more egregious cases, citizens organize in groups to fulfill this vacuum. In that mobilization, vigilante violence carries “forward panic” (Gross, 2016): process wherein fear and tension is released suddenly, leading to disproportional extreme violence.

Communicates more about the absolute capacity of the state to provide security, than about the ability of its institutions to satisfy the demand for folk catharsis in an outrageous case. Political scientists Wilson & Kelling (1982) posited that state power is communicated by policing: if a proverbial broken window is left unattended for long enough and vandals unpunished, small crimes may evolve into larger crimes in the vacuum of policing. In the context of Max Weber’s (1919) monopoly on legitimate violence, the broken windows theory places the perpetual onus on the state to maintain the monopoly by showing its presence frequently enough. According to a study on state capacity using the spread of the US Postal system as a proxy variable, as state capacity increased, so did decrease the number of duels (Jensen & Ramey, 2019).

Although the theory is controversial today (Harcourt & Ludwig, 2006), it illustrates the way collective beliefs in norms dissipate and change. Philosopher Cristina Bicchieri (2016) proposes a concept of pluralistic ignorance, where actors collectively and ritual-istically pretend to believe in a norm for the sake of social acceptance; if this pretense in believing in the legitimacy of state monopoly is eroded, actors may feel collectively insecure. In such situations, actors may decide to retreat to defeatism or - using the aforementioned matrix of social deviance (Merton, 1938) – rebel and replace the vacuum with their own securitization.

Vigilantes fit in the state – non-state nexus when they enforce state policies and laws. While technically outside the monopoly on violence, non-state actors at times provide a complementary role to the cumbersome state bureaucracy, effectively solving some of the emerging issues without the need to engage law enforcement (or otherwise, helping the policing units). Even without condoning such behavior, state actors benefit from occasional self- or citizen-policing initiatives, where crowdsourced civil activity results in more efficient enforcement of state laws. Naturally, in areas where state actors represent less legitimate, the non-state proxy counterparts fulfill the role of inner policing regardless of whether they were officiated by the state (e.g. Oude Breuil & Rozema, 2009).

VIOLENT: Vigilantes, Militia

Vigilante justice lies in the history of all nations. The frontiersman-homesteader culture of the 18th and 19th century North America has provided ample examples of vigilantes seeking to right the perceived social “wrongs” (Little & Sheffield, 1983), clear a moral panic through extraordinary violence (Mortensen, 2018), or protect communities. In Mexico, self-defense militia called autodefensas in Michoacan organized to rebel and defend against the increasing violence of cartels, in the lack of state capacity to do so (Fuentes Diaz & Paleta Perez, 2015). In Africa, vigilante folk justice movements have provided examples of securitization, but also extreme disproportionate punishment (Pratten, 2008; Gross, 2016).

Still, the need for justice has at times led to cathartic social revolutions. In 2010-2011, the Tunisian revolution was spurred on by a victim of police corruption who immolated himself in the middle of the market in Sidi Bouzid; protesters mobilized across various social media (2015). At other times, moral and political outrage fueled a volatile reaction. A mixture of elements of the moral panic in the QAnon conspiracy (Bellingcat, 2021; Tian, 2021) and allegations of election fraud by the losing dominant party (Abilov et al, 2021) contributed to the mobilization of rioters who stormed the US capitol in search of 'folk devils' and evidence of malicious behavior (Conklin, 2021). Because of the large role of mass media in both events, the boundary between the digital and the physical – as well as the actual state and non-state goals - blurs.

Some of the modern activist-vigilantes included those aligned with social and environmental issues. Greenpeace famously organized own naval campaigns against whaling (Moffa, 2012), in evolution of the general eco-sabotage movement that was outraged by environmental exploitation and mistreatment of animals (cf. ecoterrorism; Summer & Weidman, 2013). Even in the attempt at legitimation of aspects of Somali piracy, pirates posited that their "struggle" started as a response to the illegal, unreported and unregulated fishing by other nations that devastated the fish-stocks off the Somali coast (see, for example: Westberg, 2016). Finally, social movements of moral outrage catalyzed by mass media include the recent proliferation of child safety legislation (re: "stranger danger"; Zgoba, 2006) and regulation of deviant behavior (Altheide, 2009) in response to the public pressure across the Anglo-Saxon world.

VIRTUAL: Hacktivists, Open Source Investigators

Hacktivists – or hackers with a cause – have originated in the beginnings of the open Internet. A proposed typology categorizes their digital vigilantism into flagging, investigating, hounding and organized leaking (Loveluck, 2019).

The most famous network, Anonymous, participated in several high-profile hacking cases that represented an anarchist social cause in each decentralized attack (see, for example: Colton, 2017; Goode, 2015; Klein, 2015). Although Anonymous has usually been at odds with governments, in several cases, the goals of the Anonymous coincided with the policy goals of various states – in theory, if not in practice or methods. In mid-2010s, Anonymous hackers launched a countercampaign against the Islamic State which increasingly started using the Internet to spread radicalizing propaganda (Richards & Wood, 2018).

In 2012, 2014 and 2017, Anonymous hackers targeted neo-Nazi and white supremacist media and groups which engaged in hate speech and crimes (Mello, 2012; Colton, Holmes & Walwema, 2017; Gierson & Gibbs, 2017), although each time for a "personal" focal reason. In both cases, the "cybervigilantes" were addressing a niche where their capability complemented the counterterrorist and policing units of states involved in suppressing these issues (e.g. Cimpanu, 2019). Many European parties to the additional protocol to the Budapest convention ratified the agreement to manage these elements of propaganda (Council of Europe, 2003).

Because of its stylistic ethos and loosely defined network, Anonymous has been used as a mask for activities of other actors. In fact, the journalist investigating the alleged revival of Anonymous in 2021 suspected that the movement was subsumed by a Russian troll farm, as an attempt at further polarization of US actors (Bran, 2021). Hackers under the guise of the network targeted international oil and petrol companies in #OpPetrol and #OpUSA campaigns (Johnson, 2013). A video voice impersonating the Anonymous spokesperson threatened the Israeli government in 2012 (Oboler, 2012).

At times, non-state actors provided inadvertent help to state actors, and the relevant discourse usually centers around the frosty US-Russia relations. In 2010, for example, Microsoft revoked the software used by an independent television station in neighboring Kazakhstan which was the only media covering the revolution in Kyrgyzstan, inadvertently (or on purpose) assisting the Russian-backed Kyrgyzstani government in quashing the revolution (Breton, 2013). Wikileaks and its campaign that focused primarily on the West has been accused of being a "useful idiot" for the Russian government (Marmura, 2018).

State-sponsored hacktivism gained traction as a concept in the 2000s (Lucas, 2017). This translated to a wider concern that many social movements are, in fact, sponsored by another state. In response to the color revolutions across ex-communist countries in the 2000s, the Russian and Chinese governments suspect the US intelligence agencies of being behind the triggers and catalysts for the uprisings (Bolt & Cross, 2018). However, the Russian Internet Research Agency company is also suspected by the US government and researchers (Walter, Ophir & Jamieson, 2020; Etudo, Yoon & Yaraghi, 2019; Howard et al, 2019) of fueling polarization and generating trigger events for intermittent social revolts in the US in the past decade.

In other examples of overcompensating for state security or cooperation, open-source investigations provided ample cases. In the 2013 Reddit search for the Boston bombers, amateur sleuths on Reddit doxxed and coaxed a person into committing suicide by wrongly accusing the victim of being one of the bombers (Nhan, Huey & Broll, 2017; Starbird, 2014). In the Netherlands, the emergence of "pedophile hunters" who mimic famous tv shows by baiting and confronting alleged pedophiles, recently led to a death in the city of Arnhem (AD, 2020; Kwai & Moses, 2021). Finally, a televised case of the pursuit of a Canadian serial killer by amateur investigators (Jensen, 2014) led many researchers to question whether such cases and documentaries legitimate extra-judicial pursuits (Stoneman & Packer, 2020), and others to call for laws regulating the viewing of the videos themselves without further reporting to authorities (Farmand, 2016; Kaufman, 2020).

ORIGINAL PRINCIPLES

Across the spectrum of non-state actors, it is important to acknowledge the importance of private and non-state actors whose roles have defined the principles of openness, transparency, internationalism, and security underlying the Internet, despite various attempts to undermine them. Proto-hacker communities (Kirkpatrick, 2002), the hacker ethic (Jesiek, 2003) and the Hacker Manifesto (Furnell, Downland & Sanders, 1999) provided the initial spark that translated into several movements today: the integration of 'white hats' into the cybersecurity industry (including the recruitment of capable hackers for either outcome), and the crowdsourcing for help on societal problems.

Cybersecurity Industry

The cybersecurity industry is a large field, valued at $159 billion in 2019 (Grand View Research, 2020), and many of the tasks that secure the cyber landscape are performed by private actors (Singer & Friedman, 2013). The evolution of ethical 'white hat' hacking (Martin, 2017) has translated into responsibility for security of many sectors. The extent of SolarWinds vulnerability exploitation, for example, would not have been noticed if FireEye, the private company, had not detected where government tripwires failed (Sanger, Perlroth & Barnes, 2021).

In terms of recruitment, other than conventional forms (Fandos, 2015; Russian Scientific Agency of Electronic Warfare, 2020), state agencies have sought other, more engaging forms of attracting top hacking talent. British GCHQ used games as online recruitment tools for cryptographers (BBC, 2011). Taking inspiration from the Cicada 3301 puzzles which were speculated to be a recruitment tool for NSA or other secretive actors (p. 407, Bauer, 2017), the US Navy also published online code-breaking recruitment games, Project Architeuthis (McEvoy, 2014) and Operation Sleeper Shark (Navy Recruiting Command Public Affairs, 2015).Due to the pandemic-induced drop in recruitment, the US Army deployed a dedicated esports team to fulfill the role of recruiters across esports tournaments (Kesling, 2020).

Crowdsourced help

Vigilante hacking and erroneous investigations are not the only avenues where citizens have been involved. In view of legitimate activities where citizens support the state, many state agencies have opened up platforms for civil society engagement. Europol has designed a system for citizens to identify different clothes, objects and locations in cases of child sexual abuse (Europol, n.d.). Following upon the low-fidelity policy in asking citizens to report sightings of suspects, the US FBI (n.d.), Europol (n.d., b) and Interpol (n.d.) published lists of most wanted or missing individuals on public platforms. Non-profit organizations have themselves been active on doing the digital OSINT investigations to support government agencies; Bellingcat (2021) is one such example. Civil experts have provided assistance in some of the long-standing cases: professional codebreakers submitted the deciphered text of the San Francisco Zodiac serial killer to the authorities after successfully cracking the key many decades after the case revealed little traces (Fagan, 2020). Finally, bug bounties (Akgul et al, 2020), vulnerability reward programs (Chatfield & Reddick, 2017) and cybercrime reporting platforms (Bidgoli et al, 2019) invite citizens and hackers alike to contribute to securitization. Putting an interesting label on the concept, in China, these crowdsourced investigators are referred to as a "human flesh search engine" (Chang & Poon, 2016).

Credible concerns

Many terms delineated historical violent non-state actors: jihadists, terrorists, drug-trafficking organizations, militia, youth gangs, guerrillas, criminal organizations, warlords, insurgents (Williams, 2008). However, the dimensions of how comparable these actors are can vary according to: motivation and purpose, strength and scope, ways in which they obtain funding or access to resources, organizational structure, role of violence, relationship with state authorities. We have attempted to illustrate many of the comparable actors in the terminology proposed by the experts.

Based on these conceptions, the following represent some of the salient discussions today:

1. Defining actors such as mercenaries is difficult and full of criticism (see, for example: Hampson, 1991; Milliard, 2003). Should the labeling convention continue or are there new avenues for looking at cyber-actors?
2. There are fears that outsourcing brings lower quality service in private security (p. 339, Amiti & Wei, 2005). Are these fears justified in the cyberspace?
3. The costliness of war has transformed conflicts into small, indirect, high-tech conflicts (p. 77, Shaw, 1999). Will the conflicts stay low-intensity, or is there a prelude to larger wars where untested cyber means will prove their worth?
4. Some cases include warlords using cyber means to achieve their profit- or territory-oriented goals (Caltagirone, 2019). Will the phenomena of warlordism and hacking coincide in the future?
5. Curiosity hacking played a role in the original hacker communities (Zetter, 2015). Some of the modern recruitment capitalize on such puzzle-solving curiosity. Will future hackers be recruited or "baited" by engaging with their natural curiosity?
6. Swatting – the false reporting of a serious crime with the intention of sending a SWAT police team to the victim's house – has become an example of a state – non-state nexus where the supply and demand roles are reversed (Jaffe, 2016; Calabro, 2020). One such "attack" led to a death in 2020 (Bahadur Lamb, 2020). Some have argued that given the danger it poses, swatting should be its own crime (Hoeferkamp, 2020). What is the future of swatting and are there historical precedents to learn from?
7. Troll farms are relatively novel forms of propagandization of discourse and polarization of societies for the purposes of a state (Reynard, 2019; Bradshaw & Howard, 2017). Increasing use of social media has led to increased susceptibility to polarization and radicalization (Singer, 2019). Where will the future of trolling take politics?
8. Ransomware groups have proven quite powerful in disrupting healthcare infrastructure, especially in critical situations such as the coronavirus pandemic (e.g. Associated Press, 2020). What does the future entail for these modern free companies?
9. The use of robotics for military purposes has increased over the past decades (Singer, 2009). Experts including the AI researcher Stuart Russell posit that swarm drone technology has the potential to overwhelm our current levels of security (Future of Life Institute, 2018). The examples of Iranian hackers (Carlin, 2016), Egyptian patriots (Zelalem, 2020) or disgruntled employees (Sayfayn & Madnick, 2017) affecting water flows has become a real threat. Any violent state response against hackers has been afforded a precedent after the Israel's airstrike in 2019 (Hewman, 2019). Will activities in the cyberspace get increasingly physical?

CHAPTER 3

WHAT POLICY GOALS DO STATES SEEK THROUGH CYBERSPACE?

Wordcloud of Key Concepts

Chapter 3: What Policy Goals do States seek through Cyberspace?

unauthorized
triad
information
technologies
russia
property
focus
dominance
project
success
development
political
domestic
states
cyber
attacks
disruption
resiliency
private
estonia
digital
campaigns
american
conflict
denial
objectives
targets
hackers
attacker
actor
beijing
defence
networks
traditional
china
access
fraud
system
integrity
doctrine
availability
extensive
covert
advantage
operation
regarding
war
military
cyberattacks
adversary
cia
data
malicious
theft
pursued
stability
economic
confidentiality
cybersecurity
operations
weakening
cyberspace
espionage
strategy
international
goals
security

Data source: Chapter 3

CONTENTS

WHAT GOALS CAN BE PURSUED

CHAPTER 3

As is mentioned in the interview with Prof. Dr. Choucri, in the long term the goals that states pursue in cyberspace are the same goals they pursue in more traditional domains, because the fundamental goals remain the same (e.g. security, well-being, preservation).

Thus, there is a convergence in the long run of ultimate goals. With regards to the short term, it is possible, however, to differentiate amongst sub-goals in particular domains.

In this project we have identified three broad categories of short-term goals that states pursue in cyberspace. The first and best understood category concerns the expansion of the technology itself and its integration within a country. This is pursued because of the economic benefits that digital technologies bring to business, such as efficiency and access to larger markets. The second and third goals relate directly to cybersecurity, each one reflecting the two sides of the security coin: defence and attack. Thus, the second category focuses on defending a nation's information and the infrastructure that houses and/or depends on it, whilst the third category relates to aggressive (often illicit) actions that involve breaching other actors' private cyber systems in order to gain an advantage. Given this project's topic, we will focus on the latter two categories concerning cybersecurity-related goals.

The digital domain and its insecurities provides states with unique opportunities to pursue and fulfil a large array of policy objectives, both licit and illicit. Focused on the manipulation of information and the technology that processes it, cyber operation applications range from the ideological to the infrastructural, and from domestic policies to grand strategy. Furthermore, the way cyber operations are conducted also provides unique advantages; as Valeriano et al put it, "the ambiguity of cyberspace shields decision makers from hawks, who will demand higher rates of escalation, and doves, who will demand appeasement." (2018, p. 78). The versatility of cyber tools is due to some of the characteristics already mentioned, including low costs, anonymity and a low risk of reprisal through plausible deniability.

In order to understand how states can pursue such varied goals in the digital domain, one should be aware of the main security aspects of cyber technologies. The security challenges (or, from the attackers perspective, opportunities) of cyberspace are typically summarized in what is know as the CIA triad of cybersecurity. This acronym stands for Confidentiality, Integrity, and Availability, and each of these concepts are defined by the authors Hoffman and Zahadat as follows:

Confidentiality

"The protection of information from unauthorized or unintended disclosure. Threats to confidentiality can include data exfiltration, spyware, or network snooping, among others." (2018, p. 120) When it comes to confidentiality, the attacker's goal tends to be focused on gaining access to data, whether the motivation be disclosure or intelligence. The common way in which confidentiality is protected, is through encryption, however, depending on its sophistication, the attacker could still gain access.

Integrity

"The integrity prong of the CIA triad refers to the protection of information againstunauthorized alterations." (2018, p. 121) When an actor attacks the integrity of a target's data, the goal is to change, delete or otherwise corrupt valuable assets. This kind of attack is typically carried out via malware, which can use such techniques as buffer overflows, taking advantage of how computers' memories work to overwhelm them, compromising the integrity of sensitive data.

Availavility

“The availability prong of the CIA triad refers to ensuring that the information can actually be accessed by the appropriate parties. Availability is important because there is no point to securing information systems if that information cannot be accessed.” (2018, p. 122) When availability is compromised, it means the attacker is seeking to prevent legitimate users from accessing the data. In other words, it is a malicious blocking or unauthorized denial of access to resources. A typical example of this is a Denial of Service attack (DoS), which is achieved by disrupting services to a host connected to the internet by flooding the targeted machine with superfluous requests in an attempt to overload the system.

These are the traditional three components of the CIA triad of cybersecurity. However, it isworth mentioning that Edward Amoroso (2013) adds a fourth element to the triad, Fraud as a separate item. Thus including a fourth element, we may refer to the group as the CIA triad + F. Fraud involves the malicious theft or unauthorized use of services without payment. In this case, the greatest motivation for the perpetrator is financial gain.

The following table summarizes these key characteristics of cybersecurity:

Type	Motivation for Attack	Definnig Attributes
Confidentiality	Gain access to secret information	Personal and business information
Integrity	Degradation of the target’s data	Remote operational control and/ or change
Availability	Disruption of access to resources	Distributed botnet attacks are common
Fraud / Theft	Gain money and/ or goods	Ingenious means for theft

When states pursue covert objectives in cyberspace they are usually directly related to the security challenges of the CIA triad + F, as well as their motivations. In the case of defence goals, the overarching purpose is to protect all four elements from any kind of malicious access, modification, corruption, compromise or theft. Regarding goals involved in the attack perspective, spying in cyberspace fits with the confidentiality category, destruction of information or even of hardware comes under integrity, blocking access to internet-based information or services is a violation of availability, and, to include the fourth element, any kind of theft, for example that of intellectual property, comes under the fraud category. The following table summarizes these key characteristics of cybersecurity.

Having explored this, let us look at the nature of cyber attacks themselves. The types of vulnerabilities and motivations are made clear by CIA triad + F, but what type of goals predominate? It is important to stress that what we witness in cyberspace is a limited kind ofconflict and it is not war. This conflict "...mainly falls in the domain of limited coercive operations and actions designed to alter the balance of information as well as manage escalation risks in long-term competitive interactions." (Valeriano et al., 2018, p. 2).

According to the same authors, in general terms, the cyber strategy of states regarding "attacks" includes the following activities and/or goals in the international arena: disruption, espionage, and degradation.

These goals are pursued with varying degrees of success and intensity by different states, but in all cases, the cyber attacks do not come within the range of provocation of what would traditionally constitute an act of war. These dampened weapons "...are now used by nations every day, not to destroy an adversary but rather to frustrate it, slow it, undermine its institutions, and leave its citizens angry or confused. And the weapons are almost always employed just below the threshold that would lead to retaliation." (Sanger, 2018, p. xvii)

In addition to these goals, Valeriano et al also note that cyber technologies aid states in achieving goals related to covert power-signalling and sometimes even coercion. Although the use of cyber operations to attain goals related to compelling other actors does occur, the authors state that they are more often used to "…signal and steal as a means of shaping long-term competition". The breadth of scope that cyber operations provide also makes them useful as part of "crisis bargaining strategies" amongst states. (2018, pp. 9–10) Similarly, Joseph Nye identifies four strategies in cyberspace that states follow as forms of deterrence: punishment, denial, entanglement, and norms: "…entanglement and norms are restraining factors, while punishment and denial are traditional coercive options where costs are imposed." (2017, p. 30)

Although generally cyberattacks are carried out below the conflict level of war, this does not mean that they are not used directly for martial purposes. Indeed, they have already been used in war (see the example of Russia below) and have proven to be a valuable addition to conventional military tools. Some authors aver that, for cyber offensives to have lasting effects in a military setting, the virtual attack must be combined with physical intervention. In other words, rather than referring to an independent domain of "cyberwar" this operations function as part of a broader coordinated military action. (Gartzke, 2013, p. 63)

COUNTRY SAMPLES

CHAPTER 3

To illustrate what goals states pursue in cyberspace, we now explore a couple of concrete examples of key states in the international arena and how they have used the digital domain to advance their interests. Note that there are many states that pursue important goals in cyberspace. However, due to the nature of this project, it is not possible to include all countries. The following states were chosen to be included because of their impact on the international system and their dexterity in cyberspace.

RUSSIA

Russia has been a fast and keen adaptor to cyberspace as a new domain for competitionand conflict in the international arena. “While ranked sixth in latent cyber capacity, Russia is the second most active state when it comes to going on the offence in cyberspace.” (Valeriano et al., 2018, p. 110) The Kremlin has made extensive use of this kind of operations as support in military campaigns and also in broader political objectives internationally. Valeriano et al (2018, p. 112) highlight the importance of non-state actors for the country’s success in this domain asserting that Russia’s entire cyber ecosystem is “...integrated into an extensive criminal network” and that there exists “...a symbiotic relationship between Kremlin cyber operatives and cyber criminals.” In terms of its goals, Russia tends to use cyberspace to disrupt its opponent’s functioning by means such as DDoS (Distributed Denial of Service), trolling and vandalism in general. (Valeriano et al., 2018, p. 159) .

In a different case of Russia benefiting from sowing confusion abroad, there is the wellknown case of the country's social media meddling during the 2016 elections in the United States of America. The goal here was to exacerbate political polarization across American society with the intention of weakening the country from within instead of mounting an external attack. This use of information is closely linked to the Gerasimov doctrine and the blurring of war and peace. This doctrine recognises that power no longer resides solely in physical space and its main purpose is not to augment war (though this may be so in some cases), but to "circumvent it by opposing the adversary where his vulnerability is greatest and his doctrinal understanding retarded". (Kello, 2017, p. 219) In the case of democratic countries such as the USA, the target of this doctrine becomes the open information spaces that allow democracies to function.

Although it may be difficult to quantify the level of success that Russia has had with these goals in cyberspace, it is clear that this domain has enabled it to achieve, or at least, come closer, to its goals. However, "despite Moscow's frequent use, not to mention the sheer audacity and high-profile character of targets" Valeriano et al (2018, p. 141) affirm that Russia is not a cyber superpower; there are other countries more capable in this domain.

CHINA

The case of China with regards to cyberspace is noteworthy for the scale of its activity and the nature of its goals. The East Asian giant has been a key player in cyberspace in recentyears, at once conducting extensive covert cyber operations and also, more recently, seeking to shape an international order around cyberspace. China is considered the "most active cyber state in the international system to date" and has had two main areas of focus: first, using cyber-espionage as a tool for catching up technologically with more advanced countries, and second, employing cyber-surveillance and control as a means for Beijing to maintain political dominance within the country as well as across the broader Asia-Pacific region. (Valeriano et al., 2018, pp. 142–143).

The main goals that China pursues in cyberspace can actually be recognised within the December 2016 Chinese National Cyberspace Security Strategy. This document is organized around three grave threats: political stability, economic progress, and culture solidarity. (Creemers, 2016) Technological development is essential for economic growth, and this, along with the country's extensive cyber-surveillance systems are instrumental in maintaining the current political order. When it comes to China's use of cyber tools in the international arena, whether this be for theft or for defence purposes, in general, Beijing's "cyber doctrine specifically focuses on three tasks: (1) identify vulnerabilities and exfiltrate data, (2) target communications networks to constrain the adversary, and (3) serve as a force multiplier". (Pollpeter, 2015, p. 157)

One of the most infamous cases of Chinese theft of intellectual property carried out through cyberspace was that of the American F-25 fighter jet. Throughout the 2000s Chinese attacks against American targets were increasing. In particular, an important goal was to gain access to military hardware secrets that could be used by China to replicate the technology without first having to go through the arduous process of developing it themselves. By 2008 Chinese hackers had got into Lockheed Martin's supposedly confidential networks and stolen plans related to the F-35 fighter jet. This impressive victory for the Chinese predictably caused outrage and even lead the head of the National Security Agency to aver that that operation constituted "the greatest transfer of wealth in history". (Sanger, 2018, pp. 18, 203)

Throughout its history with cyberspace, China has been renowned for its espionage and theft. However, nowadays the country seems to be adding a new trait to the mix, presenting itself as a responsible actor, focusing more on stability than on quick gains. Valeriano et al observe that currently "China is not an aggressive actor" and is instead acting in a more restrained manner since the 2015 diplomatic agreement between Obama and Xi, a moment these academics believe to be a likely watershed moment in international cybersecurity relations. (Valeriano et al., 2018, p. 147)

As mentioned in the interview with Prof. Dr. Choucri, China practically has no non-state actors in the cyber domain. Interestingly, though, China has made use of the plausible deniability characteristic of cyber-attacks in an attempt to mask its direct responsibility for some attacks, albeit without much success. Thus, to carry out its operations, China has consistently relied on state-connected actors with a semi-independent appearance over the past years. This has allowed Beijing to obtain the information it seeks, whilst having a way of denying official involvement, although it has not been very plausible. An important case of this are the groups of hackers who work for Unit 61398, the cyber force of the People's Liberation Army (PLA). Although these hackers have "clear ties to the PLA", they are known to operate from private addresses rather than official buildings. Furthermore, these "prodigious thieves" have multiple employers in Chinese companies, blurring the origin of their orders, but nonetheless making it easy to conclude that there is state involvement.(Sanger, 2019, p. 102-103)

The following table summarises the country examples concerning their immediate goals through cyberspace and how they relate to the CIA triad + F.

	Russia	China
Goals in cyber-space	• Cutting and corrupting information flows in adversary states • Aiding military campaigns by disrupting enemy communications	• Espionage of foreign countries and businesses • Information exfiltration • Theft of intellectual property • Domestic surveillance
Ultimate goals	• Psychological weakening of adversaries • Political and institutional erosion in adversary states	• Maintaining rapid economic development • Building a strategic advantage in cyberspace • Ensuring political stability and dominance domestically and regionally
Often-exploited elements of the CIA triad + F	• Integrity • Availability	• Confidentiality • Fraud/theft

CONCLUSION

CHAPTER 3

As we have seen, the immediate goals that states seek in cyberspace are diverse and manifold. In general, whether the goals are related to security and defence, or attacks, these can generally be evaluated through the lens of the CIA triad +F of cybersecurity. Different countries have diverging specific goals depending on their priorities: Russia for instance, has focused its offensive goals on disruption and weakening of adversary states, in line with its military campaigns and gran strategy; China has steered its goals towards espionage and IP theft, to aid its goal of economic development, and towards domestic surveillance, to help maintain political stability.

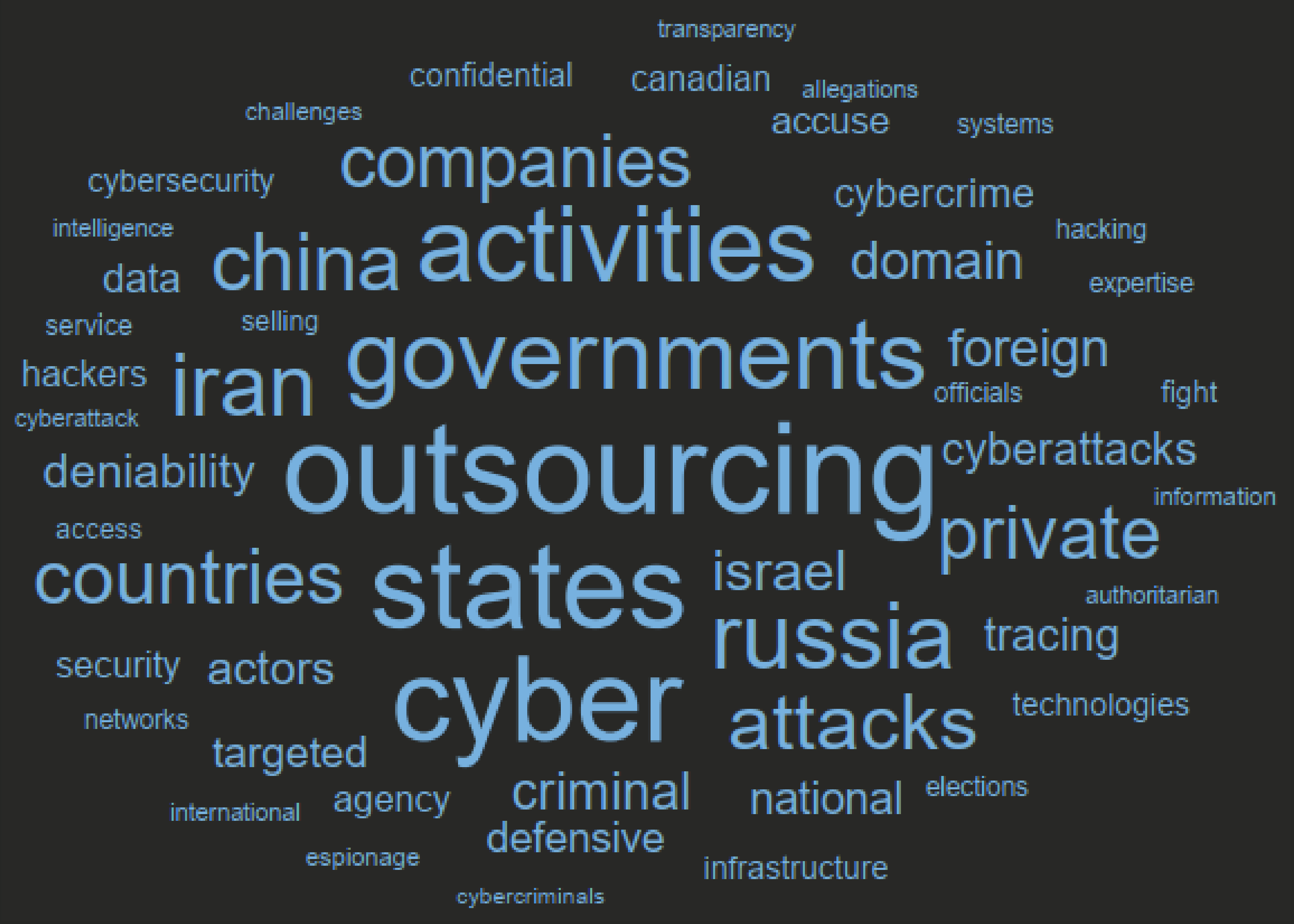
Regardless of country variations, Valeriano et al affirm that a goal that should always be present and that must be sought in cyberspace is that of resiliency (2018, p. 209) In spite of the insecurities inherent to cyber technologies explored in this chapter, these technologies offer profound advantages to humanity in developing and building resiliency across many areas; however, resiliency must also be constructed within cyberspace itself, and this requires understanding its global dynamics.

CHAPTER 4

HOW IS OUTSOURCING DONE BY DIFFERENT STATE ACTORS?

Wordcloud of Key Concepts

Chapter 4: How is outsourcing done by different state actors?



Data source: Chapter 4

CONTENTS

INTRODUCTION

CHAPTER 4

It is widespread known that many governments are turning a blind eye to cybercrime as long as foreign governments are targeted. Through outsourcing, states can make use of the deniability regarding being related to the crimes. Today, the practice is seen all over the world – particularly in authoritarian countries, such as China, Russia, Iran, and North Korea. However, this does not mean that other states do not outsource their cybercrime activities; the difference lies in the fact that these countries are more successful in lifting the link between the state and cybercriminals. An example of outsourcing activities, or in other words, government-backed cybercrime, is simple hacking. The private actor works to promote a nation's interest at home or abroad, which could be ranging from a critical website for a state to financial systems of an entire country. Most of the time, confidential information is being leaked through these activities, and generate revenue, status, and reliability loss for the state at stake.

The impact on the national stage of such outsourcing is immense, with the attacks surrounding the US 2016 presidential elections as an example. In this instance, attackers had gained access to large amounts of sensitive data, showing their ability to influence a national election. Plausible deniability plays the biggest role in outsourcing: We all know the truth, but it cannot be proven. The effect of this 'unproven' relationship between the state and cybercriminals has developed a sophisticated and semi-protected criminal industry.

Outsourcing cyber activities to private actors has become so widespread today, that there is a global chess game going on between states. A big motivation behind outsourcing – and not just leaving the activities to the criminal's nationalist beliefs – is that huge government funding makes attacks noteworthy and effective. With more resources, foreign companies and states can be targeted directly. According to Verizon's 2019 Data Breach Investigations Report, nation-state attacks have risen from 12% to 23% (rate of state-sponsored cybercrime). This has made it necessary for it necessary for states to invest in the cyber domain and acquire the necessary expertise to either resist or oppose cyberattacks.

OUTSOURCING EXAMPLES FROM STATES

RUSSIA

In the last decade, most news around outsourcing cyber activities revolves around Russia. This could be due to the reason that Russian president Vladimir Putin himself served for 16 years in the KGB, Russia's primary security agency. He is very experienced in the area of international intelligence and espionage. Even though Russian high-executives obviously deny such outsourcing activities, Putin's tone regarding the issue is quite different: "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," he said on the fact that patriotic Russian hackers may have been involved in the DNC hacks in 2016. This shows that some countries do not even consider using a negative tone towards cyber criminals and define them as "patriotic" personages. Also, in Rossiiskaya Gazeta (government newspaper) a deputy minister of defense, Gen. Oleg Ostapenko, said the science squadrons might include hackers with criminal histories. He claimed that it is a matter of discussion to use scientific potential. There are many more incidents in which we see Russia outsourcing their cyberactivity, but one last noteworthy example is an article from online newspaper Meduza, in which it is stated that "the Russian intelligence community is still actively recruiting hackers in exchange for closing the criminal cases against them". In July 2018, for instance, a court in Belgorod dropped the charges against a local man accused of committing 545 cyber-attacks against the Federal Security Service (FSB), but the case was dismissed at the service's request.

CHINA

Another example is the case of China. Despite the fact that many countries such as the United States, Germany, New Zealand, and Belgium have made loud public allegations that they had been the subject of cyber infiltration from China, the technological challenge of tracing the attacks is very complex, creating a plausible deniability case for the Chinese. This being the case, it remains unknown how these countries are so confident in their allegations, but it is seen that without clear evidence (which is almost impossible), the Chinese government is getting away with the activities. Even when there is link to China (e.g the case of Ghostnet), there is no clear link to the Chinese government.

IRAN - ISRAEL

Reports from both Iran and Israeli state officials have claimed that their governments have been under cyberattacks. Even though the two parties do not accuse each other directly, private actors within the borders of the two countries are taking the responsibility. In July 2020, an anonymous Iranian group, Cyber Avengers, claimed to have launched a series of cyberattacks on Israel's rail infrastructure in retaliation, and warned that "the worst is yet to come". Iranian Cyberwarfare analyst Hussein Estahdadi claims that Iran themselves face cyberattacks every 15 seconds, but that most of them don't affect infrastructure, and that "Iran has now revolutionized its cyberspace capabilities which don't allow adversaries to cross the red line". In May 2020, an Iranian port suffered a major cyberattack that was linked to Israel and was viewed as a response to Iran's cyberattack on Israel's water distribution system earlier.

PRIVATE COMPANIES

Even though it is outside the scope of this particular topic, it is noteworthy to mention that not only states outsource their cyber activities. Companies that have no direct connection with the government are pushing attacks for economic purposes as well, with the example of Chinese-based companies targeting a European company tech company that specializes in drones. This case beclouds tracing and linking even more, because governments could always twist the situation into a “privately motivated attack where economic benefit was the motivation”, instead of taking responsibility for the activity itself.

ISSUE IN DEFENSIVE OUTSOURCING

There is an entire twist to the outsourcing situation too. Governments tend to outsource their cybersecurity to private companies/actors as well, simply because they lack the infrastructure and expertise to secure their networks individually. Besides that, they save time and guarantee 24/7 protection. But outsourcing cybersecurity means that private companies will have direct access to confidential files, creating a big problem in the defensive side of outsourcing. Despite the fact that keeping a blind eye towards cyber activity against foreign countries is quite simple, when it comes to outsourcing defensive activities, it becomes a very serious decision. Here, effective agency and espionage plays a key role in governments' approach towards the cyber domain.

WHAT CAN BE DONE TO FIGHT AGAINST OUTSOURCING CYBER ACTIVITY?

Due to the complexity in tracing an attack, there is no simple solution to the challenges. However, there are some steps that could be taken. Some Canadian companies like Vineyard Networks and Sandvine have been accused of selling surveillance technologies to foreign governments, in which these private companies also sell private information regarding Canadian citizens, government officials, or military forces. Here, we require a greater transparency in Canadian law with regard to cyber-security breaches, such as stronger data breach disclosure laws. Besides that, governments must adapt the cyber domain directly in their foreign policy as well. Cyber related issues should be given priority when negotiating bilateral or multilateral arrangements, especially with authoritarian regimes. Here, countries should be pressured to take more responsibility in the cyber domain which originate from their borders. Also, there will be left a void left by the international agencies and rules, which should be filled by NGO's with tracking, monitoring, and exposure activities. Most likely, they will do a much more transparent reporting compared to the governments themselves.

Even though these suggestions are not entirely demolishing the power of plausible deniability, they could be initial steps. One thing we know is that threats around the cyber domain are growing and getting more complex lately, which shows that we cannot ignore them. States and organizations across the world need to be ready for the possibility of a highly targeted and effective attacks.

APPENDIX

TEXT ANALYSIS

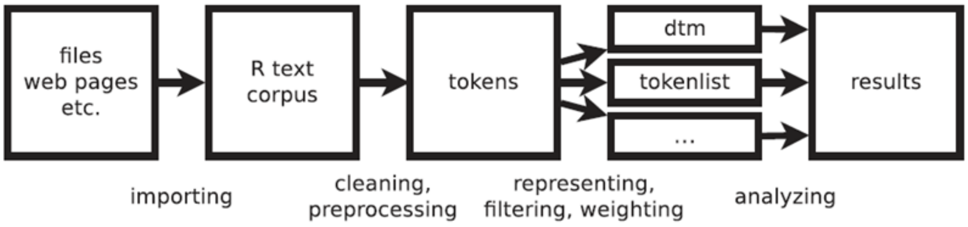
METHODOLOGY OF THE TEXT ANALYSIS

APPENDIX

In order to perform a complementary analysis of the bibliographic references used in this research, a text analysis was implemented using the text mining approach (Silge and Robinson, 2017), with the statistical software R. Taking into consideration this approach, a series of text analyses were implemented at a statistical level, resulting in a series of visualisations projected through the website designed within the framework of this project, in order to identify a series of patterns, relationships between concepts, actors involved, among other elements.

Based on above, a network graph was developed, taking into consideration all the bibliographical references used in this document. In addition, this analysis allowed the identification of those concepts that are frequent in each chapter of this document, which were visualised through the word cloud graph.

In general terms, the approach used was carried out considering the following information processing and analysis stages (Welbers et. al., 2017):



In this context, for the implementation and vizualization of the network graph, were considered the following steps.

1. All the bibliographic resources used in the research were classified according to the type (paper, article, book, news, journal, among others).

2. All the bibliographic resources were consolidated in one file in order to proceed to its upload in the software.

3. Once the file is uploaded in the software a first step is to consolidate the data in a dataframe, in order to create a table where each word is allocated in each row of the table.

4. Then was applied a clean process of the data, in order to its standardization and remotion of all the elements that nor contribute to the qualitative analysis making it easier to compare or combine the data with other datasets. In order to implement this process, the following steps were taken:.
   1.
   - Remotion of the punctuation of the data.
   - Becoming all the characters to lowercase.
   - Delete double or more spaces between words.
   - Remotion of the numbers of the data.
   - Remove stopwords, which are all those words that are frequent in the english grammar, but provide little information about the essence of the text. In this context, these types of words are articles, prepositions, conjunctions, among others that the only function is to provide context and connection among the words that conform the text.
   - Remove all the blank rows as a result of the implementation of the previous steps.

5. Once the text is cleaned, the data is analysed according to the frequency of each word in relation to the text, storing the data in a new table with the frequency number.

6. Then the data is organized into consecutive sequences of words, called n-grams. In the case of this analysis, bigrams were created in order to establish the correlation between a tuple of words.

7. The next step is to extract a sample of the correlated tuple of words of the data, in order to visualise it.

8. Finally, the data is visualized in a network graph, in order to identify not only the correlations among words, but also those keywords related to data analyzed.

In order to visually identify the level of correlation among words, the variables “stronger” and “less stronger” are defined. Based on this, each word was tokenized into consecutive sequences of words, in this case in bigrams as was previously mentioned. According to this definition, it is possible to identify how often the word A is followed by word B, allowing to build a model of the relationships between them (Silge and Robinson, 2017).

Therefore, a network graph is created considering several nodes of relationship, classified by the nature of the word inside this network. In this context, the “stronger” variable is defined for those words which represent the highest rate of correlation among the following words in the graph. On the other hand, the “less stronger” group considers all those words, whose correlation rate is fewer than the stronger ones. However, this does not mean that there is no correlation between a stronger word and a less stronger word, but the correlation rate is fewer.

In addition, based on this approach and according to the information of each chapter a word cloud graph was developed for the purpose of identifying and communicating the key concepts of each chapter of this document (Silge and Robinson, 2017). Thus, once the data processing in step 5 (above) had been completed, a manual cleaning of the collected data was conducted, in order to eliminate all words that were not related to the purpose of this project, and then graphed with the assistance of the statistical software R.

SOURCE CODE

APPENDIX

VIZUALIZATION 01: NETWORK GRAPH

```
#Establish of the workplace

setwd(dirname(rstudioapi::getActiveDocumentContext()$path))

getwd()

#Upload the packages used

Packages <- c("dplyr", "ggplot2", "readr",

          "stopwords","tidytext",

          "stringi", "stringr", "scales",

          "tidyr", "widyr", "ggraph", "igraph",

          "quanteda", "topicmodels","lattice",

          "robustbase", "cvTools", "NLP", "tm",

          "readxl", "ggnet", "network", "sna",

          "visNetwork", "htmltools","xlsx", "htmlwidgets" , "networkD3")

lapply(Packages, library, character.only = TRUE)

#Consolidation of the data

text_lines1 <- readLines(text1)

text_lines1<- paste(text_lines1,collapse = " ")

text_lines1 <- strsplit(text_lines1, split = " ") %>% unlist()
```

```
#Cleaning of the data
text_lines1 <- sapply(text_lines1,”removePunctuation”,USE.NAMES = FALSE)
text_lines1 <- sapply(text_lines1,”tolower”,USE.NAMES = FALSE)
text_lines1 <- sapply(text_lines1,”stripWhitespace”,USE.NAMES = FALSE)
text_lines1 <- sapply(text_lines1,”removeNumbers”,USE.NAMES = FALSE)
text_lines1 <- text_lines1[text_lines1!=””]
text_lines1 <- text_lines1[text_lines1!=” “]

remove <- c(stopwords(“eng”))
text_lines1 <- sapply(text_lines1,”removeWords”,words=remove, USE.NAMES = FALSE)
text_lines1 <- text_lines1[text_lines1!=””]
text_lines1 <- text_lines1[text_lines1!=” “]

#Creation of a data frame (table) once the data was standardized
part1 <- as.data.frame(line = 1:n, text_lines1)
#Word frequency analysis (creation of table with the frequencies)
count_table <- part1 %>%
  dplyr::count(text_lines1, sort = TRUE)
#Word frequency analysis (creation of bar graph with the frequencies)
count_table %>%
        mutate(text_lines1 = reorder(text_lines1, n)) %>%
        ggplot(aes(text_lines1, n)) +  geom_col(fill = “blue”) +
        theme_gray()+  theme(text = element_text(family=”Segoe UI”),
                axis.text = element_text(size = 10),
                axis.title.x = element_text(size = 10))+
        scale_y_continuous(labels = comma_format()) +  coord_flip() +
        labs(x = “ “, y = “Mentions”,  title = “Text Analysis”,
              subtitle = “Word frequency of references used”) +
        geom_text(aes(label = n, hjust = 1.2), color = “white”, fontface = 2)


#Prepare table for comparison for each part
backupdata1 <- cbind(Part1 = 1, count_table)


#Save table in xlsx format
write.xlsx(backupdata1,”backupdata1.xlsx”)
#Creation of bigrams
bigrams1<-lapply(ngrams(text_lines1,2), paste, collapse=” “) %>% unlist()
bigrams1 <- table(bigrams1) %>% as.data.frame()
bigrams1 <- bigrams1 %>% separate(bigrams1,into=c(“word1”,”word2”),sep=” “)
#Extraction of the sample
sample1 <- bigrams1 %>% filter(Freq>10)
#Implementation of the network graph
sample1 <- bigrams1 %>% filter(Freq>10)
firstposition <- sample1$word1
secondposition <- sample1$word2
network <- data.frame(firstposition,secondposition, stringsAsFactors = FALSE)
#Make a nodes data frame out of all unique nodes in networkData
nodes <- data.frame(name = unique(c(network$firstposition,
                                    network$secondposition)))
#Make a group variable where nodes in networkData$src are identified
nodes$group <- ifelse(nodes$name %in% network$firstposition, “Stronger”, “Weaker”)
#Make a links data frame using the indexes (0-based) of nodes in ‘nodes’
links <- data.frame(source = match(network$firstposition, nodes$name) - 1,
                   target = match(network$secondposition, nodes$name) - 1)
```

```
#Network graph

network <-forceNetwork(Links = links, Nodes = nodes, Source = “source”,

                    Target = “target”, NodeID =”name”, Group = “group”, opacity = 1,

                    opacityNoHover = -1, height = NULL, width = NULL,

           colourScale = JS(‘d3.scaleOrdinal().domain([“Stronger”,”Weaker”]).range([“#81BEF7”,
“#81F781”]);’),

                    fontSize = 15, fontFamily = “serif”, linkDistance = 30,

                    linkWidth = JS(“function(d) { return Math.sqrt(d.value); }”),

                    radiusCalculation = JS(“ Math.sqrt(d.nodesize)+6”), charge = -30,

                    linkColour = “#FBFBEF”, zoom = TRUE, legend = TRUE,

                    arrows = FALSE, bounded = FALSE, clickAction = FALSE)

network <- htmlwidgets::prependContent(network, htmltools::tags$h1(“Network of correlation
between words”))

network <- htmlwidgets::prependContent(network, htmltools::tags$h2(“To see the connected
labels, please click on one of the nodes”))

#Adding style parameters

network <- htmlwidgets::onRender(

  network, ‘function(el, x) {

d3.selectAll(“.legend text”).style(“fill”, “white”);

    d3.select(“body”).style(“background-color”, “black”);

    d3.select(“h1”).style(“color”, “white”).style(“font-family”, “sans-serif”);

    d3.select(“h2”).style(“color”, “white”).style(“font-family”, “sans-serif”);

    d3.select(“body”)

         .style(“background-image”,”url(file://C:/Users/isaac/OneDrive/Escritorio/Trabajos_R/
TUMProject/Part4/first.jpg)”)

      .style(“background-repeat”, “no-repeat”)

      .style(“background-position”, “right bottom”);

    }’

)
```

```
customJS <- ‘
function(el,x) {
  var link = d3.selectAll(“.link”)
  var node = d3.selectAll(“.node”)
  var options = { opacity: 1,
          clickTextSize: 10,
          opacityNoHover: 0.1,
          radiusCalculation: “Math.sqrt(d.nodesize)+6”
         }
  var unfocusDivisor = 4;
  var links = HTMLWidgets.dataframeToD3(x.links);
  var linkedByIndex = {};
  links.forEach(function(d) {
   linkedByIndex[d.source + “,” + d.target] = 1;
   linkedByIndex[d.target + “,” + d.source] = 1;
  });
  function neighboring(a, b) {
   return linkedByIndex[a.index + “,” + b.index];
  }
  function nodeSize(d) {
      if(options.nodesize){
          return eval(options.radiusCalculation);
      }else{
          return 6}
  }
  function mouseover(d) {
   var unfocusDivisor = 4;
   link.transition().duration(200)
    .style(“opacity”, function(l) { return d != l.source && d != l.target ? +options.opacity / unfocusDivisor : +options.opacity });
   node.transition().duration(200)
     .style(“opacity”, function(o) { return d.index == o.index || neighboring(d, o) ? +options.opacity : +options.opacity / unfocusDivisor; });
   d3.select(this).select(“circle”).transition()
    .duration(750)
    .attr(“r”, function(d){return nodeSize(d)+5;});
    node.select(“text”).transition()
      .duration(750)
      .attr(“x”, 13)
      .style(“stroke-width”, “.5px”)
      .style(“font”, 24 + “px “)
      .style(“opacity”, function(o) { return d.index == o.index || neighboring(d, o) ? 1 : 0; });
  }
  function mouseout() {
    node.style(“opacity”, +options.opacity);
    link.style(“opacity”, +options.opacity);

    d3.select(this).select(“circle”).transition()
      .duration(750)
      .attr(“r”, function(d){return nodeSize(d);});
    node.select(“text”).transition()
      .duration(1250)
      .attr(“x”, 0)
      .style(“font”, options.fontSize + “px “)
      .style(“opacity”, 0);
  }

  d3.selectAll(“.node”).on(“mouseover”, mouseover).on(“mouseout”, mouseout);
}
‘
network <- onRender(network, customJS)


#Export network graph (html format)
saveNetwork(network,      “C:/Users/isaac/OneDrive/Escritorio/Trabajos_R/TUMProject/Network_Graph_Final.html”, selfcontained = TRUE)
```

VIZUALIZATION 02: WORDCLOUD GRAPH

```
#Establish of the workplace

setwd(dirname(rstudioapi::getActiveDocumentContext()$path))

getwd()

#Upload the packages used

Packages <- c(“dplyr”, “ggplot2”, “readr”, “pdftools”,”stopwords”,”tidytext”,

          “stringi”, “stringr”, “scales”, “tidyr”, “widyr”, “ggraph”, “igraph”,

          “quanteda”, “topicmodels”,”lattice”, “robustbase”, “cvTools”, “NLP”, “tm”,

          “readxl”, “ggnet”, “network”, “sna”, “visNetwork”, “threejs”, “networkD3”,

          “ndtv”, “htmltools”,”xlsx”,”SnowballC”, “RColorBrewer”, “ggthemes”,

          “extrafont”,”readr”,”wordcloud”, “wordcloud2”, “ggwordcloud”,”reshape2”)

lapply(Packages, library, character.only = TRUE)

#Upload of the data

data<- read_excel(“data.xlsx”)
```

Note: This file is the consolidation of all the references used in the research.

```
#Consolidation and cleaning of the data

data <- file(“ChapterX.txt”)

data <- readLines(data)

data <- paste(data, collapse = “ “)

data <- strsplit(data, split = “ “) %>% unlist()

corpus <- table(data) %>% as.data.frame()

corpus <- sapply(corpus,”removePunctuation”,USE.NAMES = FALSE)

corpus <- sapply(corpus,”tolower”,USE.NAMES = FALSE)

corpus <- sapply(corpus,”stripWhitespace”,USE.NAMES = FALSE)

corpus <- sapply(corpus,”removeNumbers”,USE.NAMES = FALSE)
corpus <- Voices[corpus!=””]
corpus <- Voices[corpus!=” “]
remove <- c(stopwords(“eng”))
corpus <- sapply(corpus,”removeWords”,words=remove, USE.NAMES = FALSE)
corpus <- corpus [corpus!=””]
corpus <- corpus [corpus!=” “]
corpus_table <- as.data.frame(line = 1:N, corpus)

#Creation of WordCloud
count_table <- corpus_table %>%  dplyr::count(corpus, sort = TRUE)
write.xlsx(count_table,”tableX.xlsx”)
finaltable <- read_excel(“tableX.xlsx”)
sample <- finaltable %>% filter(n>X)

#Vizualization of WordCloud
ggplot(sample, aes(label = Voices, size = n)) +
  geom_text_wordcloud(area_corr = TRUE, color= ‘#78b1e0’, eccentricity = 1.3) +
  scale_size_area(max_size = 10) + theme_minimal() +
  theme(text = element_text(family=”Segoe UI”),
        plot.title = element_text(hjust = 0.5, color = “#78b1e0”, size = 16, face= “bold”),
        plot.subtitle = element_text(hjust = 0.5, color = “white”, size = 10,face= “bold”),
        plot.caption = element_text(hjust = 0, color = “white”, size = 7,face= “bold”),
        plot.background = element_rect(fill = “#292927”)) +
  labs(title = “Wordcloud of Key Concepts”,
       subtitle = “Chapter X: XXX”,
       caption = “Data source: Chapter X”)
```

PROJECT GROUP

REFERENCES

Abdollah, T. & Tucker, E. (2019 July 6). Mystery of NSA leak lingers as stolen document case winds up. ABC News. Retrieved from https://abcnews.go.com/Technology/wireStory/mystery-nsa-leak-lingers-stolen-document-case-winds-64163448

Abilov, A., Hua, Y., Matatov, H., Amir, O. & Naaman, M. (2021). VoterFraud2020: a Multi-modal Dataset of Election Fraud Claims on Twitter. arXiv. Retrieved on 31st January 2021 from https://arxiv.org/abs/2101.08210

AD. (2020 November 20). Politie is klaar met 'pedojagers' die mannen opwachten en belagen. AD. Retrieved from https://www.ad.nl/binnenland/politie-is-klaar-met-pedojagers-die-mannen-opwachten-en-belagen~a14e4b43/?referrer=https%3A%2F%2Fwww.google.com%2F

Adams, J. (1996). Principals and Agents, Colonialists and Company Men: The Decay of Colonial Control in the Dutch East Indies. American Sociological Review, 61 (1), 12 – 28.

Ahn, W., Chung, M., Min, B. & Seo, J. (2015). Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs. International Journal of Distributed Sensor Networks, 11 (9).

Akgul, O. et al. (2020). The Hackers' Viewpoint: Exploring Challenges and Benefits of Bug-Bounty Programs. In 6th Workshop on Security Information Workers (WSIW 2020), Hannover, August 9th 2020.

Akinwumi, O. (2001). Princes as highway men: A consideration of the phenomenon of armed banditry in precolonial Borgu. Cahiers d'Etudes africaines, 162, 333 – 350.

Alessio, D. & Villegas-Aristizabal, L. (2020). Re-thinking Religion and Empire: Non-State Organizations from the Knights Hospitallers to ISIS. Journal of Balkan and Near Eastern Studies, 22 (5), 580 – 596.

Allen, P. & Gilbert, D. (2009). The Information Sphere Domain Increasing Understanding and Cooperation. In C. Czosseck & K. Geers, The Virtual Battlefield: Perspectives on Cyber Warfare, 132 - 142. Amsterdam: IOS Press.

Altheide, D. (2009). Moral panic: From sociological concept to public discourse. Crime, Media, Culture: An International Journal, 5 (1), 79 – 99.

Amiti, M. & Wei, S. J. (2005). Fear of service outsourcing: is it justified?. Economic policy, 20 (42), 307-347.

Amoroso, E. G. (2013). Cyber attacks: Protecting national infrastructure (Student ed). Butterworth-Heinemann/Elsevier.

Anderson, N. (2012 June 1). Confirmed: US and Israel created Stuxnet, lost control of it. ArsTechnica.

Apps, P. (2011 October 26). Analysis: Agreement seen distant at London cyber conference. Reuters. Retrieved from https://de.reuters.com/article/us-technology-cyber-conference-idUSTRE79P2MC20111026

Arquilla, J. & Ronfeldt, D. (2001). Networks and netwars: the future of terror, crime, and militancy. Santa Monica, CA: Rand.

Associated Press. (2020 September 17). German hospital hacked, patient taken to another city dies. AP News. Retrieved from https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94

Auger, V. (2020). Right-Wing Terror: A Fifth Global Wave? Perspectives on Terrorism, 14 (3), 87 – 97.

Auley, J., Tonge, J. & Shirlow, P. (2009). Conflict, Transformation, and Former Loyalist Paramilitary Prisoners in Northern Ireland. Terrorism and Political Violence, 22 (1), 22 – 40.

Australian Government. (2021). Strategies to Mitigate Cyber Security Incidents. Retrieved from: https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

Avant, D. (2000). From Mercenary to Citizen Armies: Explaining Change in the Practice of War. International Organization, 54 (1), 41 – 72.

Avant, D. (2007). The emerging market for private military services and the problem of regulation. In S. Chesterman & C. Lehnardt (eds.), From Mercenaries to Market: The Rise and Regulation of Private Military Companies. Oxford: Oxford University Press.

Avramov, K. (2019 March 30). The Advent of the “Digital Mercenaries”. Small Wars Journal. Retrieved from https://smallwarsjournal.com/jrnl/art/advent-digital-mercenaries

Baesso Moura, M. (2020). Operação Gedeón: o uso de companhias militares privadas na Venezuela. Revista Brasileira de Estudos Latino-Americanos, 10 (3), 457 – 471.

Baezner, M. (2018 August). Hotspot Analysis: Regional rivalry between IndiaPakistan: tit-for-tat in cyberspace. Center for Security Studies, ETH Zurich.

Bahadur Lamb, J. (2020). Death by SWAT: The three elements of swatting. In A. Lynes, K. Hoffin & C. Kelly (eds.), Video Games, Crime and Next-Gen Deviance: Reorienting the Debate. Bingley: Emerald Publishing Ltd

Bamford, J. (2016 August 22). Commentary: Evidence points to another Snowden at the NSA. Reuters. Retrieved from https://www.reuters.com/article/us-intelligence-nsa-commentary-idUSKCN10X01P

Barber, R. (2001). Hackers Profiled — Who Are They and What Are Their Motivations? Computer Fraud & Security, 2001(2), 14–17.

Bauer, C. (2017). Unsolved!: The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies. Princeton, NJ: Princeton University Press.

BBC. (2011 December 1). GCHQ challenges codebreakers via social networks. BBC. Retrieved from https://www.bbc.com/news/technology-15968878

BBC. (2017 June 1). Putin: Patriotic Russians may be involved in hacking. BBC. Retrieved from https://www.bbc.com/news/technology-40122943

BBC. (2020 July 17). Twitter hack: FBI investigates major Twitter attack. BBC. Retrieved from https://www.bbc.com/news/technology-53439585

BBC. (2021 January 19). US Capitol riots: Trump supporter arrested after Pelosi 'data theft'. BBC. Retrieved from https://www.bbc.com/news/election-us-2020-55711200

Bearpark, A. & Schulz, S. (2007). The future of the market. In S. Chesterman & C. Lehnardt (eds.), From Mercenaries to Market: The Rise and Regulation of Private Military Companies. Oxford: Oxford University Press.

Becke, J. (2019). Varieties of expansionism: A comparative-historical approach to the study of state expansion and state contraction. Political Geography, 72, 64 – 75.

Belfer Center for Science and International Affairs. (2020 September). National Cyber Power Index 2020. Harvard Kennedy School.

Bellingcat. (2021 January 7). The Making of QAnon: A Crowdsourced Conspiracy. Bellingcat. Retrieved from https://www.bellingcat.com/news/americas/2021/01/07/the-making-of-qanon-a-crowdsourced-conspiracy/

Bendrath, Ralf, Johan Eriksson, and Giampiero Giacomello. 2007. 'From "Cyberterrorism" to "Cyberwar", Back and Forth: How the United States Securitized Cyberspace'. In International Relations and Security in the Digital Age, Routledge, 57–82.

Bidgoli, M., Knijnenburg, B., Grossklags, J. & Wardman, B. (2019). Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting. In 2019 APWG Symposium on Electronic Crime Research (eCrime), Pittsburgh, PA, 13-15 November 2019.

Bigoli, M. & Grossklags, J. (2017). “Hello. This is the IRS calling.”: A Case Study on Scams, Extortion, Impersonation, and Phone Spoofing. In 2017 APWG Symposium on Electronic Crime Research, Scottsdale, AZ, 25-27 April 2017.

Bocetta, S. (2017 November 23). Chinese state sponsored hacking. RealClearDefense. Retrieved from: https://www.realcleardefense.com/articles/2017/11/23/chinese_state_sponsored_hacking_112675.html

Bolt, P. & Cross, S. (2018). Emerging Non-traditional Security Challenges: Color Revolutions, Cyber and Information Security, Terrorism, and Violent Extremism. In China, Russia, and Twenty-First Century Global Geopolitics. Oxford: Oxford University Press.

Bossert, T. (2017 December 19). Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea [Press Release]. United States White House. Retrieved from https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

Boulet, G. (2015). Cyber Operations by Private Actors in the Ukraine-Russia Conflict: From Cyber War to Cyber Security. American Society of International Law, 19 (1). Retrieved from https://www.asil.org/insights/volume/19/issue/1/cyber-operations-private-actors-ukraine-russia-conflict-cyber-war-cyber

Boyd, A. (2015 August 18). FBI tries to recruit hackers as cyber special agents. Federal Times. Retrieved from https://www.federaltimes.com/2015/08/18/fbi-tries-to-recruit-hackers-as-cyber-special-agents/

Bradshaw, S. & Howard, P. N. (2017). Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation [Working paper no. 2017.12]. University of Oxford. Retrieved from http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf

Bran, D. (2021). The Return of Anonymous. The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/

Breton, L. & Pearson, A. (2010). Contextual Truth-Telling to Counter Extremist-Supportive Messaging Online: The Wikileaks “Collateral Murder” Case Study. Small Wars Journal. Retrieved from https://smallwarsjournal.com/jrnl/art/contextual-truth-telling-to-counter-extremist-supportive-messaging-online

Breton, L. Virtual non-state actors as Clausewitzian Centers of Gravity. Journal of Information Warfare, 12 (1), 63 – 69.

Breuer, A., Landman, T. & Farquhar, D. (2015). Social media and protest mobilization: evidence from the Tunisian revolution. Democratization, 22 (4), 764 – 792.

Brown, C. (2015). White or Black Hat? An Economic Analysis of Computer Hacking [Working Paper]. Washington, DC: Georgetown University.

Brundage, M. et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute. Retrieved from https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf

Bunker, R. & Heal, C. (2014). Fifth Dimensional Operations: Space-Time-Cyber Dimensionality in Conflict and War. Bloomington, IN: iUniverse.

Burt, T. (2020 September 10). New cyberattacks targeting U.S. elections. Microsoft. Retrieved on 31st January 2021 from https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/

Byman, D. (2008). Understanding Proto-Insurgencies. Journal of Strategic Studies, 31 (2), 165 – 200.

Caferro, W. (1996). Italy and the Companies of Adventure in the Fourteenth Century. The Historian, 58 (4), 795 – 810.

Calabro, S. (2020). From the Message Board to the Front Door: Addressing the Offline Consequences of Race- and Gender-Based Doxxing and Swatting. Suffolk University Law Review, 51 (1), 55 – 75.

Caltagirone, S. (2019 December 3). Industrial Cyber Attacks: A Humanitarian Crisis in the Making. Retrieved from https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/

Carlin, J. (2016 March 24). Assistant Attorney General John P. Carlin Delivers Remarks at Press Conference Announcing Seven Iranians Charged for Conducting Cyber Attacks against U.S. Financial Sector. US Department of Justice. Retrieved from https://www.justice.gov/opa/speech/assistant-attorney-general-john-p-carlin-delivers-remarks-press-conference-announcing

Carter, D. (2016). Provocation and the Strategy of Terrorist and Guerrilla Attacks. International Organization, 70 (1), 133 – 173.

Casanovas, P. (2009). Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT). In M. Taddeo, L. Glorioso (eds.), Ethics and Policies for Cyber Operations. Retrieved from https://uploads-ssl.webflow.com/5cd23e823ab9b1f01f815a54/5cff33b8bbb1f7b1327173ed_Cyber%20Warfare%20and%20Organised%20Crime.%20A%20Regulatory%20Model%20and%20Meta-Model%20for%20Open%20Source%20Intelligence%20(OSINT).pdf

Centeno, M., Cruz, J., Flores, R., & Cano, G. (2013). Internal wars and Latin American nationalism. In J. Hall & S. Malešević (Eds.), Nationalism and War (pp. 279-305). Cambridge: Cambridge University Press.

Chadwick, N. (1970). The Celts. London: Penguin Books.

Chan, T., Cheung, C. & Wong, R. (2019). Cyberbullying on Social Networking Sites: The Crime Opportunity and Affordance Perspectives. Journal of Management Information Systems, 36 (2), 574 – 609.

Chang, L. & Poon, R. (2016). Internet Vigilantism: Attitudes and Experiences of University Students Toward Cyber Crowdsourcing in Hong Kong. International Journal of Offender Therapy and Comparative Criminology, 61 (16), 1912 – 1932.

Chappell, D. & Di Martino, V. (2006). Violence at Work (3rd edition). Geneva: International Labour Organization.

Chapsos, I. & Holtom, P. (2015). Floating Armouries in the Indian Ocean. In Small Arms Survey 2015: Weapons and the World, 216 - 241. Cambridge: Cambridge University Press.

Chatfield, A. & Reddick, C. (2017). Cybersecurity Innovation in Government: A Case Study of U.S. Pentagon’s Vulnerability Reward Program. In dg.o ‘17: Proceedings of the 18th Annual International Conference on Digital Government Research, June 2017, 64 -73.

Chen, M., Fischer, F., Meng, N., Wang, X. & Grossklags, J. (2019). How Reliable is the Crowdsourced Knowledge of Security Implementation? 2019 IEEE/ACM 41st International Conference on Software Engineering (ICSE), Montreal, QC, 25 – 31 May 2019.

Cheong, P. & Gong, J. (2010). Cyber vigilantism, transmedia collective intelligence, and civic participation. Chinese Journal of Communication, 3 (4), 471 – 487.

Chisholm, A. (2015). From Warriors of Empire to Martial Contractors: Reimagining Gurkhas in Private Security. In M. Eichler (ed.), Gender and Private Security in Global Politics, 95 - 113. Oxford: Oxford University Press.

Cimpanu, C. (2020 January 13). Report: Chinese hacking group APT40 hides behind network of front companies. ZDNet. Retrieve from: https://www.zdnet.com/article/report-chinese-hacking-group-apt40-hides-behind-network-of-front-companies/

Cimpanu, C. (2019 November). Mysterious hacker dumps database of infamous IronMarch neo-nazi forum. ZDNet. Retrieved from https://www.zdnet.com/article/mysterious-hacker-dumps-database-of-infamous-ironmarch-neo-nazi-forum/

Clausewitz, C. von. (1832). On War [Vom Krieg] (M. Howard & P. Paret, eds.). Princeton, NJ: Princeton University Press.

Clayton, R. (2005). Anonymity and traceability in cyberspace [Technical Report no. 653]. Cambridge: University of Cambridge. Retrieved from https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf

Clayton, R. (2010). Might Governments Clean-up Malware? Communications & Strategies, 1 (81), 87 – 104.

Cohen, S. (2011). Folk Devils and Moral Panics. London: Routledge.

Collier, J. (2017). Proxy Actors in the Cyber Domain. St Antony's International Review, 13 (1), 25 - 47. Retrieved from https://www.jstor.org/stable/26229121?seq=1

Collin, B. (1997). Future of Cyberterrorism: The Physical and Virtual Worlds Converge. Crime and Justice International, 13 (2), 15 -18.

Colton, J., Holmes, S. & Walwema, J. (2017). From NoobGuides to #OpKKK: Ethics of Anonymous' Tactical Technical Communication. Technical Communication Quarterly, 26 (1), 59-75.

Conklin, M. (2021). Capitol Offense: Is Donald Trump Guilty of Inciting a Riot at the Capitol? SSRN.

Conway, M. (2014). Reality Check: Assessing the (Un)Likelihood of Cyberterrorism. In T. Chen, L. Jarvis & S. Macdonald (eds.), Cyberterrorism. New York, NY: Springer New York.

Cormac, Rory, and Richard J. Aldrich. 2018. 'Grey Is the New Black: Covert Action and Implausible Deniability'. International Affairs 94(3): 477–94.

Council of Europe. (2003). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems [Treaty no. 189].

Council of Europe. (2004). Convention on Cybercrime [Treaty no. 185].

Creemers, R. (2016). Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. Journal of Contemporary China, 26 (103), 85 – 100. Retrieved from https://www.tandfonline.com/doi/full/10.1080/10670564.2016.1206281

Creemers, R. (2016, December 27). National Cyberspace Security Strategy. China Copyright and Media. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyber-spacesecurity-strategy/

Cristina Bicchieri. (2016). Norms in the Wild. How to Diagnose, Measure, and Change Social Norms. Oxford: Oxford University Press.

Crockett, M. (2017). Moral outrage in the digital age. Nature Human Behaviour, 1, 769 – 771.

Croninn, A. K. (2006 September 10). Cyber-Mobilization: The New Levee en Masse. US Army. Retrieved from https://www.army.mil/article/40/cyber_mobilization_the_new_levee_en_masse

Cruz, J. da & Pedron, S. (2020). Cyber Mercenaries: A New Threat to National Security. International Social Science Review, 96 (2).

Dahan, M. (2013). Hacking for the Homeland: Patriotic Hackers Versus Hacktivists. In D. Hart, ICIW 2013 Proceedings of the 8th International Conference on Information Warfare and Security: ICIW 2013, Denver: CO.

Danet, D. (2019). Hackers and the Military: How to Recruit and Manage Hidden Talents. In T. Cruz & P. Simoes (eds.), ECCWS 2019 18th European Conference on Cyber Warfare and Security, 124 – 131.

Danks, D. & Danks, J. (2018). Beyond Machines: Humans in Cyber Operations, Espionage, and Conflict. Carnegie Mellon University.

DeLuca, C. (2013). The Need for International Laws of War to Include Cyber Attacks: Involving State and Non-State Actors. Pace International Review Online Companion, 278. Retrieved from https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1033&context=pilronline

Dempsey, G. (2002). Napoleon's Mercenaries: Foreign Units in the French Army under the Consulate and Empire, 1799-1814. London: Greenhill Books.

Donald C. Hellman Task Force Program. (2020). The World Wide Race for Artificial Intellligence: A Path Forward for US Policy. Henry M. Jackson School of International Studies.

Donelly, L. (2018 February 6). More than 900 NHS deaths yearly may be caused by IT failings. The Telegraph. Retrieved from https://www.telegraph.co.uk/news/2018/02/06/900-nhs-deaths-yearly-may-caused-failings/

Dorfman, Z. (2020 December 21). China used stolen data to expose CIA operatives in Africa and Europe. Foreign Policy. Retrieve from: https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/#

Dunn Cavelty, Myriam Dunn. 2008. 'Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate'. Journal of Information Technology & Politics 4(1): 19–36.

Dunn Cavelty, Myriam Dunn. 2015. ‘Die Materiellen Ursachen Des Cyberkriegs Cybersicherheitspolitik Jenseits Diskursiver Erklärungen’. Journal of self-regulation and regulation 1: 167–84.

Egloff, F. J. 2015. Cybersecurity and the Age of Privateering: A Historical Analogy. Oxford: Cyber Studies Programme. Working Paper. https://ora.ox.ac.uk/objects/uuid:a93b3385-0a5d-4df3-ac30-88532af9ca93.

Egloff, F. (2016 November 17). Cyber Privateering: A Risky Policy Choice for the United States. Lawfare. Retrieved from https://www.lawfareblog.com/cyber-privateering-risky-policy-choice-united-states

Egloff, F. (2017 October 16). Cybersecurity and the Age of Privateering. Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2017/10/16/cybersecurity-and-age-of-privateering-pub-73418

Egloff, F. (2018). Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates [PhD Thesis]. University of Oxford. Retrieved from https://ora.ox.ac.uk/objects/uuid:77eb9bad-ca00-48b3-abcf-d284c6d27571/download_file?file_format=pdf&safe_filename=Florian%2BEgloff%2BDPhil%2BCybersecurity%2Band%2BNon-State%2BActors%2BA%2BHistorical%2BAnalogy%2Bwith%2BMercantile%2BCompanies%2BPrivateers%2Band%2BPirate.pdf&type_of_work=Thesis

Etudo, U., Yoon, V. & Yaraghi, N. (2019). From Facebook to the Streets: Russian Troll Ads and Black Lives Matter Protests. Proceedings of the 52nd Hawaii International Conference on System Sciences.

Europol. (n.d.). Europe’s Most Wanted Fugitives. Retrieved on 31st January 2021 from https://eumostwanted.eu/

Europol. (n.d.). Stop Child Abuse – Trace an Object. Retrieved on 9th December 2020 from https://www.europol.europa.eu/stopchildabuse

Fagan, K. (2020). Zodiac ‘340 Cipher’ cracked by code experts 51 years after it was sent to the S.F. Chronicle. San Francisco Chronicle. Retrieved from https://www.sfchronicle.com/hdn/hrlm/p/fastly_redirect.html?dm=https%3A%2F%2Fwww.sfchronicle.com%2Fcrime%2Farticle%2FZodiac-340-cypher-cracked-by-code-expert-51-years-15794943.php

Falconer, R. (2019 April 22). Russia’s increasingly working with cyber criminals, former national security official warns. Axios. Retrieve from: https://www.axios.com/russia-spies-working-with-cyber-criminals-5c2f12f7-8f25-419a-a850-3bc89de346a3.html

Fandos, N. (2015 July 17). N.S.A. Summer Camp: More Hacking Than Hiking. The New York Times. Retrieved from https://www.nytimes.com/2015/07/18/us/nsa-summer-camp-hacking-cyber-defense.html?emc=eta1&_r=0

Farmand, M. (2016). Who Watches This Stuff: Videos Depicting Actual Murder and the Need for a Federal Criminal Murder-Video Statute. Florida Law Review, 68, 1915.

Farnelli, G. (2015). Vessel Protection Detachments and Maritime Security: An Evaluation of Four Years of Italian Practice. Maritime Safety Law Journal, 1, 16 – 32.

Federal Bureau of Investigations. (2020 December 23). Iranian Cyber Actors Responsible for Website Threatening U.S. Election Officials. FBI. Retrieved on 12 January 2021 from https://www.fbi.gov/news/pressrel/press-releases/iranian-cyber-actors-responsible-for-website-threatening-us-election-officials

Federal Bureau of Investigations. (2021 January 5). JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA). FBI. Retrieved on 13th January 2021 from https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

Federal Bureau of Investigations. (n.d.). Ten Most Wanted Fugitives. Retrieved on 31st January 2021 from https://www.fbi.gov/wanted/topten

FireEye Inc. (2013). Operation Safron Rose. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf

Foltz, B. (2004). Cyberterrorism, computer crime, and reality. Information Management & Computer Security, 12 (2), 154 – 166.

Fortune. (2020, July 22). It’s getting harder to tell state-sponsored hackers and cybercriminals apart. Fortune. Retrieved from: https://fortune.com/2020/07/22/state-sponsored-hacking-cybercrime-china-hong-kong/

Foxall, A. (2016). Putin’s Cyberwar: Russia’s Statecraft in the Fifth Domain. Henry Jackson Society.

Froissart, J. (n.d.). Chronicles of England, France, Spain, and the adjoining countries. 1857 Translation by Thomas Jonhes. Retrieved from https://catalog.hathitrust.org/Record/000537473

Fuentes Diaz, A. & Paleta Perez, G. (2015). Violencia y autodefensas comunitarias en Michoacán, México. Iconos: Revista de Ciencias Sociales, 53, 171 – 186.

Bamford, J. (2016 August 22). Commentary: Evidence points to another Snowden at the NSA. Reuters. Retrieved from https://www.reuters.com/article/us-intelligence-nsa-commentary-idUSKCN10X01P

Barber, R. (2001). Hackers Profiled — Who Are They and What Are Their Motivations? Computer Fraud & Security, 2001(2), 14–17.

Bauer, C. (2017). Unsolved!: The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies. Princeton, NJ: Princeton University Press.

BBC. (2011 December 1). GCHQ challenges codebreakers via social networks. BBC. Retrieved from https://www.bbc.com/news/technology-15968878

BBC. (2017 June 1). Putin: Patriotic Russians may be involved in hacking. BBC. Retrieved from https://www.bbc.com/news/technology-40122943

BBC. (2020 July 17). Twitter hack: FBI investigates major Twitter attack. BBC. Retrieved from https://www.bbc.com/news/technology-53439585

BBC. (2021 January 19). US Capitol riots: Trump supporter arrested after Pelosi 'data theft'. BBC. Retrieved from https://www.bbc.com/news/election-us-2020-55711200

Bearpark, A. & Schulz, S. (2007). The future of the market. In S. Chesterman & C. Lehnardt (eds.), From Mercenaries to Market: The Rise and Regulation of Private Military Companies. Oxford: Oxford University Press.

Becke, J. (2019). Varieties of expansionism: A comparative-historical approach to the study of state expansion and state contraction. Political Geography, 72, 64 – 75.

Belfer Center for Science and International Affairs. (2020 September). National Cyber Power Index 2020. Harvard Kennedy School.

Bellingcat. (2021 January 7). The Making of QAnon: A Crowdsourced Conspiracy. Bellingcat. Retrieved from https://www.bellingcat.com/news/americas/2021/01/07/the-making-of-qanon-a-crowdsourced-conspiracy/

Bendrath, Ralf, Johan Eriksson, and Giampiero Giacomello. 2007. 'From "Cyberterrorism" to "Cyberwar", Back and Forth: How the United States Securitized Cyberspace'. In International Relations and Security in the Digital Age, Routledge, 57–82.

Bidgoli, M., Knijnenburg, B., Grossklags, J. & Wardman, B. (2019). Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting. In 2019 APWG Symposium on Electronic Crime Research (eCrime), Pittsburgh, PA, 13-15 November 2019.

Funk, M. (2015 January 30). The Hack that Warmed the World. Foreign Policy. Retrieved from https://foreignpolicy.com/2015/01/30/climate-change-hack-carbon-credit-black-dragon/

Furnell, S., Downland, P. & Sanders, P. (1999). Dissecting the "Hacker Manifesto". Information Management & Computer Security, 7 (2).

Futter, A. (2016). Cyber Threats and Nuclear Weapons. RUSI. Retrieved from https://rusi.org/sites/default/files/cyber_threats_and_nuclear_combined.1.pdf

Future of Life Institute. (2018 November 13). Slaughterbots. Youtube. Retrieved from https://www.youtube.com/watch?v=HipTO_7mUOw

Galeotti, M. (2018). The mythical 'Gerasimov Doctrine' and the language of threat. Critical Studies on Security, 7 (2), 157 – 161.

Gardner, B. (2018). Social Engineering in Non-Linear Warfare. Journal of Applied Digital Evidence, 1 (1), 1 – 29.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.

International Security, 38(2), 41–73. https://doi.org/10.1162/ISEC_a_00136

Gattiker, U. (2004). The Dictionary of Information Security. Boston, MA: Springer Science.

Geers, K. (2017). Cyberspace and the Changing Nature of Warfare. NATO. Retrieved from https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf

Gierson, J. & Gibbs, S. (2017 August 14). Message showing apparent hack appears on neo-Nazi Daily Stormer website. The Guardian. Retrieved from https://www.theguardian.com/technology/2017/aug/14/anonymous-hackers-take-over-neo-nazi-website-daily-stormer-charlottesville-heather-heyer

Goode, L. (2015). Anonymous and the Political Ethos of Hacktivism. International Journal of Media and Culture, 13 (1), 74 – 86.

Goodin, D. (2015 February 16). How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last. ArsTechnica. Retrieved from https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/

Goodin, D. (2019 May 7). Stolen NSA hacking tools were used in the wild 14 months before Shadow Brokers leak. ArsTechnica. Retrieved from https://arstechnica.com/information-technology/2019/05/stolen-nsa-hacking-tools-were-used-in-the-wild-14-months-before-shadow-brokers-leak/

Goodwin, B. (2016). Using Political Ideas, 6th Edition. Hoboken, NJ: Wiley.

Gordon, S. & Ford, R. (2002). Cyberterrorism? Computers & Security, 21 (7), 636 – 647.

Gorr, David, and Wolf J. Schünemann. 2013. 'Creating a Secure Cyberspace – Securitization in Internet Governance Discourses and Dispositives in Germany and Russia'. International Review of Information Ethics 20(12): 37–51.

Grand View Research. (2020 June). Cyber Security Market Size, Share & Trends Analysis Report By Component, By Security Type, By Solution, By Service, By Deployment, By Organization, By Application, By Region, And Segment Forecasts, 2020 – 2027. Retrieved from https://www.grandviewresearch.com/industry-analysis/cyber-security-market

Gross, M. (2016). Vigilante violence and "forward panic" in Johannesburg's townships. Theory and Society, 45, 239 – 263.

Hampson, F. J. (1991). Mercenaries: Diagnosis before Proscription. Netherlands Yearbook of International Law, 22, 3-38.

Hannas, W., Mulvenon, J. & Puglisi, A. (2013). Chinese Industrial Espionage: Technology Acquisition and Military Modernisation. New York City, NY: Routledge.

Harcourt, B. & Ludwig, J. (2006). Broken Windows: New Evidence from New York City and a Five-City Social Experiment. Univesity of Chicago Law Review, 73 (1), 271 - 320.

Hare, F. (2017). Privateering in Cyberspace: Should Patriotic Hacking Be Promoted as National Policy? Asian Security, 15 (2), 93 – 102.

Hewman, L. (2019 June 5). What Israel's Strike on Hamas Hackers Means For Cyberwar. Wired. Retrieved from https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

Hobsbawm, E. (1959). Primitive Rebels: Studies in Archaic Forms of Social Movement in the 19th and 20th Centuries. Norton Library. Norton, KS: Norton Public Library.

Hobsbawm, E. (1969). Bandits. London: Weidenfeld & Nicolson.

Hoeferkamp, J. (2020). Combatting the Swatting Problem: The Need for a New Criminal Statute to Address a Growing Threat. Michigan State Law Review, 2019(4), 1133 – 1175.

Hoekstra, Q. (2018). Helping the Contras: The Effectiveness of U.S. Support for Foreign Rebels During the Nicaraguan Contra War (1979–1990). Studies in Conflict & Terrorism.

Hoffman, L., & Zahadat, N. (2018). Securing Democracy: A Comparative Look at Modern and Future US Voting Systems Through the Lens of the CIA Triad. Journal of

Information Assurance and Security, 13, 118–124.

Hollinger, R. (1991). Hackers: computer heroes or electronic highwaymen? ACM SIGCAS Computers and Society, 21 (1).

Honig, O. & Yahel, I. (2017). A Fifth Wave of Terrorism? The Emergence of Terrorist Semi-States. Terrorism and Political Violence, 31 (6), 1210 – 1228.

Hosenball, M. (2020 December 23). U.S. suspects Iranians created website threatening U.S. election officials. Reuters. Retrieved from https://www.reuters.com/article/us-usa-elections-iran/u-s-suspects-iranians-created-website-threatening-u-s-election-officials-idUSKBN28X2M4

Hou, T. & Wang, V. (2020). Industrial espionage – A systematic literature review (SLR). Computers Security, 98.

Howard, P., Ganesh, B., Liotsiou, D., Kelly, J. & Francois, C. (2019). The IRA, Social Media and Political Polarization in the United States, 2012-2018. Select Committee on Intelligence United States Senate.

Iasiello, Emilio. 2015. 'Are Cyber Weapons Effective Military Tools?' Military and Strategic Affairs 7(1): 23–40.

Ingrao, C. (1987). The Hessian Mercenary State: Ideas, Institutions, and Reform under Frederick II, 1760 – 1785. Cambridge: Cambridge University Press.

International Convention against the Recruitment, Use, Financing and Training of Mercenaries, Dec. 4, 1989, A/RES/44/34

Interpol. (n.d.). View Red Notices. Retrieved on 31st January 2021 from https://www.interpol.int/en/How-we-work/Notices/View-Red-Notices

Jaffe, E. (2016). Swatting: The New Cyberbullying Frontier After Elonis v. United States. Drake Law Review, 64, 455 – 483.

Jarvis, L. & Macdonald, S. (2014). What Is Cyberterrorism? Findings From a Survey of Researchers. Terrorism and Political Violence, 27 (4), 657 – 678.

Jenkins, B. (2008). Will Terrorists Go Nuclear? RAND. Retrieved from https://www.rand.org/pubs/commercial_books/CB413.html

Jensen, B. (2014 March 19). Animal Instinct: How Cat-Loving Sleuths Found an Accused Killer Sadist. Rolling Stone. Retrieved from https://www.rollingstone.com/culture/culture-news/animal-instinct-how-cat-loving-sleuths-found-an-accused-killer-sadist-111273/

Jensen, J. & Ramey, A. (2019). Going Postal: State Capacity and Violent Dispute Resolution. Journal of Comparative Economics, 48 (4), 779 – 796.

Jesiek, B. (2003). Democratizing software: Open source, the hacker ethic, and beyond. First Monday, 8(10).

Johnson, A. L. (2013 June 19). Prepare for #OpPetrol Targeting Gas and Oil. Retrieved from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=310e8c92-02c8-4064-9c54-fbc-56cb3233d&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

Jones, S. (2017 March 16). Licensed to hack: the rise of the cyber privateer. Financial Times. Retrieved from https://www.ft.com/content/21be48ec-0a48-11e7-97d1-5e720a26771b

Josefsson, A., Anderson, J., Norlander, A. & Marcusson, B. (2019). Mission Command when waging cyber operations. 24th International Command and Control Research & Technology Symposium, Laurel: MA, 29-31 October 2019. Retrieved from https://www.fhs.se/download/18.7cc6824116dedebbe60639e5/1572899607668/Mission%20Command%20in%20Cyber%20Operations.pdf

Kaldor, M. (2013). New and Old Wars: Organized Violence in a Global Era (3rd Edition). Stanford, CA: Stanford University Press.

Kasper Welbers, Wouter Van Atteveldt & Kenneth Benoit (2017) Text Analysis in R, Communication Methods and Measures, 11:4, 245-265, DOI: 10.1080/19312458.2017.1387238

Kaufman, Z. (2020). Digital Age Samaritans. Boston College Law Review, 62 (4).

Kelling, G. & Wilson, J. (1982). Broken Windows: The police and neighborhood safety. The Atlantic Magazine. Retrieved from https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/

Kello, Lucas. 2017. The Virtual Weapon and International Order. New Haven: Yale University Press.

Kerr, O. & Murphy, S. (2017). Government Hacking to Light the Dark Web: Risks to International Relations and International Law? Stanford Law Review, 70. Retrieved from https://www.stanfordlawreview.org/online/government-hacking-to-light-the-dark-web/

Kesling, B. (2020 May 17). Army Deploys Videogames to Reach Recruits Amid Pandemic. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/army-deploys-videogames-to-reach-recruits-amid-pandemic-11589734800

Kirkpatrick, G. (2002). The Hacker Ethic and the Spirit of the Information Age. Max Weber Studies, 2 (2), 163 – 185.

Klein, A. (2015). Vigilante Media: Unveiling Anonymous and the Hacktivist Persona in the Global Press. Communication Monographs, 82 (3), 379 – 401.

Klimburg, A. (2011). Mobilising Cyber Power. Global Politics and Strategy, 53 (1), 41 – 60.

Koch, A. (2019). The Non-Jihadi Foreign Fighters: Western Right-Wing and Left-Wing Extremists in Syria.

Kocic, M. (2014). Venice and Hajduci in the Era of the Morean War [Venecija i Hajduci u doba Morejskog rata]. Belgrade: Hesperia.

Kohn, H. (1944). The Idea of Nationalism: A Study in its Origins and Background [Republished 2005]. London: Routledge.

Koliopoulos, J. (1987). Brigands with a Cause: Brigandage and Irredentism in Modern Greece 1821 – 1912. Oxford: Oxford University Press.

Koller, C. (2013). Recruitment Policies and Recruitment Experiences in the French Foreign Legion. In, N. Arielli & B. Collins (eds.), Transnational Soldiers. London: Palgrave Macmillan.

Kreegipuu, T. & Lauk, E. (2007). The 1940 Soviet Coup-d'État in the Estonian Communist Press: Constructing History to Reshape Collective Memory. Westminster Papers in Communication and Culture, 4 (4), 42 – 64.

Kwai, I. & Moses, C. (2021 January 15). Dutch Police Urge Public to Stop 'Pedo-Hunting' After Vigilante Violence. The New York Times. Retrieved from https://www.nytimes.com/2020/11/19/world/europe/netherlands-pedophile-hunters.html

Leaven, T. & Dodge, C. (2010). The United States Cyber Command: International Restrictions vs. Manifest Destiny. North Carolina Journal of Law & Technology, 12(3), 1-28.

Lee, S. (2014). The Ethics of Cyberattack. In L. Floridi & M. Taddeo (eds.), The Ethics of Information Warfare, 105 - 122. Cham: Springer International Publishing.

Leventopoulos, S. & Benias, N. (2017). Cyber Warfare Affecting Land, Sea, Air and Space Operations. Journal of Computations & Modelling, 7 (1), 29 – 56.

Leyden, J. (2020 October 7). Researchers map threat actors' use of open source offensive security tools. The Daily Swig. Retrieved from https://portswigger.net/daily-swig/researchers-map-threat-actors-use-of-open-source-offensive-security-tools

Lindvall, A. (2019). Political Hacktivism: Doxing & the First Amendment. Creighton Law Review, 53 (1), 1 – 14.

Linvill, D. & Warren, P. (2020). Troll Factories: Manufacturing Specialized Disinformation on Twitter. Political Communication, 37 (4), 447 – 467.

Little, C. & Sheffield, C. (1983). Frontiers and Criminal Justice: English Private Prosecution Societies and American Vigilantism in the Eighteenth and Nineteenth Centuries. American Sociological Review, 48 (6), 796 – 808.

Liu, H. (2015). Cybersecurity and Cyberwarfare as Emerging Gaps in Private Military and Security Company Regulation: Thoughts for the UN Working Group on the Use of Mercenaries. OHCHR. Retrieved from https://ohchr.org/Documents/Issues/Mercenaries/WG/Event2015/HinYanLiu.pdf

Lo, M. (2019) The Islamic State: The Rise of Vigilante Justice. In: Political Islam, Justice and Governance. Political Economy of Islam. Cham: Palgrave Macmillan.

Lokot, T. (2017). Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism. Irish Studies in International Affairs, 28, 99 – 116.

Loveluck, B. (2019). The many shades of digital vigilantism. A typology of online self-justice. Global Crime, 21 (3-4), 213 – 241.

Lucas, G. (2014). Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets. In L. Floridi & M. Taddeo (eds.), The Ethics of Information Warfare, 73 - 84. Cham: Springer International Publishing.

Lucas, G. (2017). State-sponsored hacktivism and the advent of "Soft War". In M. Gross & T. Meisels (eds.), Cyber Warfare, Media Warfare, and Lawfare, 77 - 87. Cambridge: Cambridge University Press. http://www.ethikundmilitaer.de/en/full-issues/20142-cyberwar/lucas-state-sponsored-hacktivism-and-the-advent-of-soft-war/

Luceri, L., Giordano, S., & Ferrara, E. (2020). Detecting Troll Behavior via Inverse Reinforcement Learning: A Case Study of Russian Trolls in the 2016 US Election. Proceedings of the International AAAI Conference on Web and Social Media, 14(1), 417-427.

Machiavelli, N. (1521). The Prince. Translation to English, 1996, Milner, S. Phoenix, AZ: Phoenix Press.

Maffei, A. & Monnier, M. (1865). Brigand life in Italy: A history of Bourbonist reaction. Los Angeles, CA: University of California. Retrieved from https://archive.org/details/brigandlifeinit-05monngoog/page/n21/mode/2up

Makuch, B. (2020 April 21). Neo-Nazis Are Spreading a List of Emails and Passwords for Gates Foundation and WHO Employees. VICE. Retrieved from https://www.vice.com/en/article/akwxzp/neo-nazis-are-spreading-a-list-of-emails-and-passwords-for-gates-foundation-and-who-employees

Marmura, S. (2018). Emerging Affinities: WikiLeaks in the Context of a Legitimation Crisis. In: The Wikileaks Paradigm, 87 – 108. Cham: Palgrave Pivot.

Martin, C. (2017). White hat, black hat: the ethics of cybersecurity. ACM Inroads, 8 (1), 33

Masood, R. (2016 August). Assessment of Cyber Security Challenges in Nuclear Power Plants: Security Incidents, Threats, and Initiatives. Cyber Security and Privacy Research Institute. Retrieved from https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/GW-CSPRI-2016-03+MASOOD+Rahat+Nuclear+Power+Plant+Cybersecurity.pdf

Maur, J. auf der. (2011). Söldner für Europa: Mehr als eine Schwyzer Familiengeschichte. Basel: Echtzeit Verlag.

Maurer, T. & Hoffman, W. (2019). The Privatization of Security and the Market for Cyber Tools and Services [Business and Security Series No. 3]. Geneva Centre for Security Sector Governance. Retrieved from https://www.dcaf.ch/sites/default/files/publications/documents/Carnegie_MaurerHoffmann_July2019.pdf

Maurer, T. (2018). Cyber Mercenaries: The State, Hackers, and Power. Cambridge: Cambridge University Press.

Maurer, T. (2016). 'Proxies' and Cyberspace. Journal of Conflict and Security Law, 21 (3), 383 - 403. Retrieved from https://carnegieendowment.org/files/JConflictSecurityLaw-2016-Maurer-383-403.pdf

McEvoy, M. (2014 April 30). US Navy attempting to recruit cryptologists through Facebook game. The Telegraph. Retrieved from https://www.telegraph.co.uk/news/worldnews/northamerica/usa/10799470/US-Navy-attempting-to-recruit-cryptologists-through-Facebook-game.html

McGrath, R. (1987). Gunfighters, Highwaymen, and Vigilantes: Violence on the Frontier. Berkeley, CA: University of California Press.

McGuffin, C. & Mitchell, P. (2014). On domains: Cyber and the practice of warfare. International Journal, 69 (3), 394 – 412.

Meer, van der S. (2020 June). How states could respond to non-state cyber-attackers. Clingendael. Retrieved from https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_non-state_June_2020.pdf

Meer, S. van der. (2015 December). Signalling as a foreign policy instrument to deter cyber aggression by state actors. Clingendael Netherlands Institute of International Relations.

Meduza. (2018, August 7). 'It's our time to serve the motherland' how Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers — Meduza. Retrieve from: https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland

Mello, J. P. (2012 January 4). Anonymous Targets Neo-Nazi Sites: Anti-Hate Groups Condemn Action. PCWorld. Retrieved from https://www.pcworld.com/article/247271/anonymous_targets_neo_nazis_sites_anti_hate_groups_condemn_action.html

Merari, A. (1993). Terrorism as a strategy of insurgency. Terrorism and Political Violence, 5 (4), 213 – 251.

Merton, R. (1938). Social Structure and Anomie. American Sociological Review, 3 (5), 672 – 682.

Miller, G. (2020 February 11). The intelligence coup of the century. The Washington Post. Retrieved from https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Milliard, T. (2003). Overcoming Post-Colonial Myopia: A call to recognize and regulate private military companies. Military Law Review, 176, 1 – 95.

Mockler, A. (1969). The Mercenaries. London: Macdonald.

Moffa, A. (2012). Two Competing Models of Activism, One Goal: A Case Study of Anti-Whaling Campaigns in the South Ocean. Yale Journal of International Law, 37 (1), 201 - 215.

Moghadam, A., Berger, R. & Beliakova, P. (2014). Say Terrorist, Think Insurgent: Labeling and Analyzing Contemporary Terrorist Actors. Perspectives on Terrorism, 8 (5), 2 – 17.

Mohurle, S. & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. International Journal of Advanced Research in Computer Science, 8 (5), 1938 – 1940.

Moncada, E. (2017). Varieties of vigilantism: conceptual discord, meaning and strategies. Global Crime, 18 (4), 403 – 423.

Moore, D. & Rid, T. (2016). Cryptopolitik and the Darknet. Global Politics and Strategy, 58 (1), 7 - 38. Retrieved from https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085

Morozov, E. (2008 August 14). An Army of Ones and Zeroes. Slate. Retrieved from https://slate.com/technology/2008/08/how-i-became-a-soldier-in-the-georgia-russia-cyberwar.html

Morozov, E. (2009 April 9). Do governments enlist cybergangs in their war efforts? Foreign Policy. Retrieved from https://foreignpolicy.com/2009/04/09/do-governments-enlist-cyber-gangs-in-their-war-efforts/

Mortensen, E. (2018). The Mode of Lynching: One Method of Vigilante Justice. Canadian Review of American Studies, 48 (1), 20 – 39.

Moyer, E. (2013 September 12). NSA disguised itself as Google to spy, say reports. CNET. Retrieved from https://www.cnet.com/news/nsa-disguised-itself-as-google-to-spy-say-reports/

Muthuppalaniappan, M. & Stevenson, K. (2020). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. International Journal for Quality in Health Care, 2020. Retrieved from https://academic.oup.com/intqhc/advance-article/doi/10.1093/intqhc/mzaa117/5912483?login=true

Navy Recruiting Command Public Affairs. (2015 February 5). Navy Recruiting Command Cryptology & Technology Facebook Page Launches New Challenge. Retrieved on 30th January 2021 from https://www.doncio.navy.mil/%28npmedcusnh5gftzqz2wvrp55%29/CHIPS/ArticleDetails.aspx?ID=6013

Nelsen, J. (1987). “Auftragstaktik”: A Case for Decentralized Battle. The US Army War College Quarterly: Parameters, 17 (1), 21 – 34.

Nhan, J., Huey, L. & Broll, R. (2017). Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings. British Journal of Criminology, 57 (2), 341 – 361.

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Oboler, A. (2012 February 12). Impersonating Anonymous: Is it state sponsored terrorism? The Jerusalem Post. Retrieved from https://www.jpost.com/blogs/internet-engagement/impersonating-anonymous-is-it-state-sponsored-terrorism-366110

O’Brien, K. (2000). Private Military Companies and African Security 1990–98. In A. F. Musah & J. K. Fayemi (eds.), Mercenaries: An African Security Dilemma. Sterling, VA: Pluto Press.

O’Sullivan, K. & Turnbull, B. (2015). The cyber simulation terrain: Towards an open source cyber effects simulation ontology. Australian Information Warfare and Security Conference, 2015. Retrieved from https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1059&context=isw

Oude Breuil, B. & Rozema, R. (2009). Fatal imaginations: death squads in Davao City and Medellín compared. Crime, Law and Social Change, 52, 405 – 424.

P&S Intelligence. (2020 August). Global Artificial Intelligence (AI) in Cyber Security Market 2020. PS Market Research. Retrieved on 13th January 2021 from https://www.psmarket-research.com/market-analysis/artificial-intelligence-in-cyber-security-market

Palou-Loverdos, J. & Armendariz, L. (2011). The Privatization of Warfare, Violence and Private Military & Security Companies: A factual and legal approach to human rights abuses by PMSC in Iraq. Nova Inovacio Social. Retrieved from https://novact.org/wp-content/uploads/2012/09/The-privatization-of-warfare.pdf

Pan, N. (2018). The Mobilization of Cyber-Nationalism by the Communist Youth League: Pressure, Opportunity and Strategy. Journal of Asia-Pacific Studies, 30, 139 – 157. Retrieved from https://core.ac.uk/download/pdf/159504217.pdf

Paszyn, D. (2000). The Extent of Soviet Military and Economic Assistance to the Sandinista Leftist Regime prior to Gorbachev Assuming Office. In: The Soviet Attitude to Political and Social Change in Central America, 1979–90. Studies in Russia and East Europe. London: Palgrave Macmillan.

Penney, J. (2012, May 25). The outsourcing of the Cyberwar. Open Canada. Retrieve from: https://opencanada.org/the-outsourcing-of-the-cyberwar/

Percy, S. (2007). Mercenaries: The History of a Norm in International Relations. Oxford: Oxford University Press.

Percy, S. (2014). The Unimplemented Norm: Anti-Mercenary Law and the Problems of Institutionalization. In A. Betts & P. Orchard, Implementation and World Politics: How International Norms Change Practice, Oxford: Oxford University Press.

Peterson, A. (2015 October 24). How the government tries to recruit hackers on their own turf. The Washington Post. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/10/24/how-the-government-tries-to-recruit-hackers-on-their-own-turf/

Phillips, A. (2016). Company sovereigns, private violence and colonialism. In R. Abrahamsen & A. Leander, Routledge Handbook of Private Security Studies, London: Routledge

Pollpeter, K. (2015). Chinese Writings on Cyberwarfare and Coercion. In J. R. Lindsay, T. M. Cheung, & D. S. Reveron (Eds.), China and Cybersecurity (pp. 138–162). Oxford

University Press. https://doi.org/10.1093/acprof:oso/9780190201265.003.0006

Porup, J. (2016 May 18). Hacking Team hacker steals €10K in Bitcoin, sends it to Kurdish anticapitalists in Rojava. ArsTechnica.

Pratten, D. (2008). 'The Thief Eats His Shame': Practice and Power in Nigerian Vigilantism. Africa: Journal of the International African Institute, 78 (1), 64 – 83.

Prem B. (2018) Who Am I? The Blurring of the Private Military and Security Company (PMSC) Category. In: Bures O., Carrapico H. (eds) Security Privatization. Springer, Cham.

Raffield, B. (2019). The slave markets of the Viking world: comparative perspectives on an 'invisible archaeology'. Slavery & Abolition, 40 (4), 682 – 705.

Rapoport, D. C. (2004). The four waves of modern terrorism. In A. K. Cronin & J. M. Ludes (Eds.), Attacking terrorism: Elements of a grand strategy (pp. 46–73). Washington, DC, Georgetown University Press.

Rathaur, K. (2001). British Gurkha Recruitment : A Historical Perspective. Voice of History, 16 (2), 19 -24.

Rediker, M. (2004). Villains of All Nations: Atlantic Pirates in the Golden Age. Boston, MA: Beacon Press.

Reeves, S. & Wallace, D. (2015). The Combatant Status of the 'Little Green Men' and Other Participants in the Ukraine Conflict. International Law Studies, 91, 361 – 401.

Reynard, L. (2019). Troll Farm: Anonymity as a Weapon for Online Character Assassination. In I. Chiluwa & S. Samoilenko (eds.), Handbook of Research on Deception, Fake News, and Misinformation Online. Hershey, PA: IGI Global.

Richards, I. & Wood, M. (2018). Hacktivists against terrorism: a cultural criminological analysis of anonymous' anti-IS campaigns. International Journal of Cybercriminology, 12 (1), 187 – 205.

Richardson, D. (1976). FOREIGN FIGHTERS IN SPANISH MILITIAS: THE SPANISH CIVIL WAR 1936-1939. Military Affairs, 40 (1), 7 - 14.

Ricks, T. (2014 April 29). Cyber-privateers. Foreign Policy. Retrieved from https://foreignpolicy.com/2014/04/29/cyber-privateers/

Russian Scientific Agency of Electronic Warfare. (2020 December 3). VKontakte Pinned Post. VKontakte. Retrieved on 31st January 2021 from https://web.archive.org/web/20210131205200/https://vk.com/wall-94744292_77

Sadok, M., Welch, C. & Bednar, P. (2019). A socio-technical perspective to counter cyber-enabled industrial espionage. Security Journal, 33, 27 – 42.

Sanford, V. (2003). Learning to Kill by Proxy: Colombian Paramilitaries and the Legacy of Central American Death Squads, Contras, and Civil Patrols. Social Justice, 30 (3), 63 – 81.

Sanger, D. E. (2018). The perfect weapon: War, sabotage, and fear in the cyber age (First paperback edition). Crown Publishing.

Sanger, D., Perlroth, N. & Barnes, J. (2021 January 5). As Understanding of Russian Hacking Grows, So Does Alarm. The New York Times. Retrieved from https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

Sauter, M. (2016). Kevin Mitnick, the New York Times, and the Media's Conception of the Hacker. In J. Hunsinger & A. Schrock (eds.), Making Our World: The Hacker and Maker Movements in Context. New York City, NY: Peter Lang Publishing.

Sayfayn, N. & Madnick, S. (2017 May). Cybersafety Analysis of the Maroochy Shire Sewage Spill [Working Paper CISL# 2017-09]. MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. Retrieved from http://web.mit.edu/smadnick/www/wp/2017-09.pdf

Schmitt, M. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press.

Schneier, B. (2016 September 13). Someone Is Learning How to Take Down the Internet. Lawfare. Retrieved from https://www.lawfareblog.com/someone-learning-how-take-down-internet

Schneier, B. (2017 May 23). Who are the Shadow Brokers? The Atlantic. Retrieved from https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/

Schulze, Matthias. 2015. 'Patterns of Surveillance Legitimization. The German Discourse on the NSA Scandal'. Surveillance & Society 13(2): 197–217.

Schulze, Matthias. 2018. 'From Cyber-Utopia to Cyber-War. Normative Change in Cyberspace.'

Scott, J. (2010). The Art of Not Being Governed: An Anarchist History of Upland Southeast Asia. New Haven, CT: Yale University Press.

Seal, G. (2009). The Robin Hood Principle: Folklore, History, and the Social Bandit. Journal of Folklore Research, 46 (1), 67 – 89.

SecurityWeek.Com. (2017). Russian outsourcing provides plausible deniability for state-sponsored hacking. SecurityWeek. Retrieved from: https://www.securityweek.com/russian-outsourcing-provides-plausible-deniability-state-sponsored-hacking

Seligman, Lara. 2018. 'Why the Military Must Learn to Love Silicon Valley'. Foreign Policy. https://foreignpolicy.com/2018/09/12/why-the-military-must-learn-to-love-silicon-valley-pentagon-google-amazon/ (February 1, 2020).

Serracino-Inglott, P. (2017). Is it OK to be an Anonymous? In K. Miller & M. Taddeo (eds.), The Ethics of Information Technologies. London: Routledge.

Seward, D. (1999). The Hundred Years War. The English in France 1337 – 1453. London: Penguin Books.

Shamir, E. (2011). Transforming Command: The Pursuit of Mission Command in the U.S., British, and Israeli Armies. Stanford: Stanford University Press.

Shane, S. (2017 May 16). Malware Case is Major Blow for the NSA. The New York Times. Retrieved from https://www.nytimes.com/2017/05/16/us/nsa-malware-case-shadow-brokers.html

Shaw, M. (1999) 'War and globality: the role and character of war in the global transition', in Ho-won Jeong (ed.), The New Agenda for Peace Research, Abingdon: Ashgate pp. 61–80

Shearing, C. & Stenning, P. (1981). Modern Private Security: Its Growth and Implications. Crime and Justice, 3, 193 – 245.

Sigholm, J. (2016). Non-State Actors in Cyberspace Operations. Journal of Military Studies, 4 (1), 1 – 37.

Silge, Julia; Robinson, David (2017): Text mining with R. A tidy approach / Julia Silgeand and David Robinson. First Edition. Sebastopol, CA: O'Reilly.

Simone, A. (2017 May 17). The strange history of ransomware. Public Radio International. Retrieved from https://www.pri.org/stories/2017-05-17/strange-history-ransomware

Simpson, T. (2014). The Wrong in Cyberattacks. In L. Floridi & M. Taddeo (eds.), The Ethics of Information Warfare, 141 - 154. Cham: Springer International Publishing.

Singer, P. & Friedman, A. (2013). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press.

Singer, P. (2003). Corporate Warriors: The Rise of the Privatized Military Industry. Ithaca, NY: Cornell University Press.

Singer, P. (2009). Wired for War: The Robotics Revolution and Conflict in the 21st Century. London: Penguin Books.

Singer, P. (2019). LikeWar: The Weaponization of Social Media. Boston, MA: Houghton Mifflin Harcourt.

Sossai, M. (2016). The legal framework for the armed forces and the regulation of private security. In R. Abrahamsen & A. Leander, Routledge Handbook of Private Security Studies, London: Routledge.

Spearin, C. (2014). Promising Privateers?: Understanding the Constraints of Contemporary Private Security at Sea. Naval War College Review, 67 (2), 97 – 116.

Speech by Foreign Minister Heiko Maas on European digital sovereignty on the occasion of the opening of the Smart Country Convention of the German Association for Information Technology, Telecommunications and New Media (Bitkom). Retrieved from https://www.auswaertiges-amt.de/en/newsroom/news/maas-bitkom/2410398

Starbird, K., Maddock, J., Orand, M., Achterman, P., & Mason, R. M. (2014). Rumors, False Flags, and Digital Vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing. In iConference 2014 Proceedings, 654 - 662.

Steele, S. & Wargo, C. (2007). An Introduction to Insider Threat Management. Information Systems Security, 16 (1), 23 – 33.

Stoneman, E. & Packer, J. (2020). Reel cruelty: Voyeurism and extra-juridical punishment in true-crime documentaries. Crime, Media, Culture: An International Journal.

Storr, J. (2003). A command philosophy for the information age: The continuing relevance of mission command. Defence Studies, 3 (3), 119 – 129.

Stubbs, J. (2021 January 11). SolarWinds hackers linked to known Russian spying tools, investigators say. Reuters. Retrieved from https://www.reuters.com/article/global-cyber-solarwinds/solarwinds-hackers-linked-to-known-russian-spying-tools-investigators-say-idINKBN29G16Z

Sullivan, J. (2018 November 28). Russian Cyber Operations: State-led Organised Crime. RUSI. Retrieved from https://rusi.org/commentary/russian-cyber-operations-state-led-organised-crime

Summer, D. & Weidman, L. (2013). Eco-terrorism or Eco-tage: An Argument for the Proper Frame. ISLE: Interdisciplinary Studies in Literature and Environment, 20 (4), 855 – 876.

Taddeo, M. & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. Nature, 556, 296 – 298.

The Economist. (2008 December 6). Marching off to cyberwar. The Economist. Retrieved from https://www.economist.com/technology-quarterly/2008/12/06/marching-off-to-cyberwar

The New York Times. (2016, December 29). How Russia recruited elite hackers for its Cyberwar (Published 2016). Retrieved from: https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html

The New York Times. (2017 March 13). How Russia recruits hackers. Podcast. Retrieved from: https://www.nytimes.com/2017/03/13/podcasts/the-daily/the-daily-how-russia-recruits-hackers.html

The Washington Post. (2015 October 24). How the government tries to recruit hackers on their own turf. The Washington Post. Retrieve from: https://www.washingtonpost.com/news/the-switch/wp/2015/10/24/how-the-government-tries-to-recruit-hackers-on-their-own-turf/

Thomson, J. (1994). Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe. Princeton, NJ: Princeton University Press.

Thonnard, O., Bilge, L. O'Gorman, G., Kiernan, S. & Lee, M. (2012). Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat. In: Balzarotti D., Stolfo S.J., Cova M. (eds) Research in Attacks, Intrusions, and Defenses. RAID 2012. Lecture Notes in Computer Science, vol 7462. Berlin: Springer.

Tian, E. (2021 January 29). The QAnon Timeline: Four Years, 5,000 Drops and Countless Failed Prophecies. Bellingcat. Retrieved from https://www.bellingcat.com/news/americas/2021/01/29/the-qanon-timeline/

Tidy, J. (2020 October 19). Mysterious 'Robin Hood' hackers donating stolen money. BBC. Retrieved from https://www.bbc.com/news/technology-54591761

Tilly, C. (1975). The formation of national states in Europe. Princeton, NJ: Princeton University Press.

Tilly, C. (1985). War making and state making as organized crime. In Evans, P., Rueschemeyer, D., & Skocpol, T. (Eds.), Bringing the State Back In (169-187). Cambridge: Cambridge University Press.

Titahena, J. & Sumser-Lupson, K. (2013). Privately Contracted Armed Security Personnel (PCASP) On Ships in High Risk Areas: Impacts, Concerns and Challenges. In E. Bosse, E. Shahbazian & G. Rogova (eds.), Prediction and Recognition of Piracy Efforts Using Collaborative Human-Centric Information Systems. Amsterdam: IOS Press.

Townsend, C. (2019). Fifth Sun: A New History of the Aztecs. Oxford: Oxford University Press.

Treebridge, P., Westbrook, J. & Sharevski, F. (2018). Sorry: Ambient Tactical Deception Via Malware-Based Social Engineering. Journal of Cognition and Neuroethics, 6 (1), 103 -123. Retrieved from https://www.researchgate.net/publication/328575878_Sorry_Ambient_Tactical_Deception_Via_Malware-Based_Social_Engineering

Trundle, M. (2004). Greek Mercenaries: From the Late Archaic Period to Alexander. London: Routledge.

Tuchman, B. (1987). A Distant Mirror: The Calamitous 14th Century. London: Random House Trade.

U.S-China Economic and Security Review Commission (USCC). (2009 November). 2009 Report to Congress of the US-China Economic and Security Review Commission. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a520210.pdf

US Cybersecurity & Infrastructure Security Agency (CISA). (2017 August 23). HIDDEN COBRA – North Korea’s DDoS Botnet Infrastructure. CISA. Retrieved on 13th January 2021 from https://us-cert.cisa.gov/ncas/alerts/TA17-164A

US Cybersecurity & Infrastructure Security Agency (CISA). (2020 April 15). Guidance on the North Korean Cyber Threat. CISA. Retrieved on 13th January 2021 from https://us-cert.cisa.gov/ncas/alerts/aa20-106a

US Department of Justice (DoJ). (2018 September 6). North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions. US DoJ Office of Public Affairs. Retrieved from https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

US Department of Justice. (2018 July 13). Indictment Case 1:18-cr-00215-ABJ [Indictment of 12 Russian Officers]. US Department of Justice. Retrieved from https://www.justice.gov/file/1080281/download

US White House. (2018 February 15). Statement from the Press Secretary. US White House. Retrieved from https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/

US White House. (2021 January 26). Readout of President Joseph R. Biden, Jr. Call with President Vladimir Putin of Russia. Retrieved from https://www.whitehouse.gov/briefing-room/statements-releases/2021/01/26/readout-of-president-joseph-r-biden-jr-call-with-president-vladimir-putin-of-russia/

Uzelac, A. (2009). Kumani u srednjovekovnoj Srbiji. Glasnik, 43.

Valeriano, B. & Maness, R. (2015). Cyber War versus Cyber Realities: Cyber Conflict in the International System. Oxford: Oxford University Press.

Valeriano, B., Jensen, B., & Maness, R. C. (2018). Cyber Strategy: The Evolving Character

of Power and Coercion. In Cyber Strategy. Oxford University Press.

https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190618094.001.

0001/oso-9780190618094

Vallor, S. (2014). Armed Robots and Military Virtue. In L. Floridi & M. Taddeo (eds.), The Ethics of Information Warfare, 169 - 185. Cham: Springer International Publishing.

Verton, D. (1999). Serbs launch cyberattack on NATO. Federal Computer Week. Retrieved from: https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx?m=2

Vincent, A. (2017). State-sponsored hackers: The new normal for business. Network Security, 9, 10-12.

Vlahakis, J. & Partridge, W. (1989). Assessment of Security at Facilities That Produce Nuclear Weapons. In: Golden B.L., Wasil E.A., Harker P.T. (eds) The Analytic Hierarchy Process. Heidelberg: Springer.

Voss, K. (2014). Washingtons Söldner: Verdeckte US-Interventionen im Kalten Krieg und ihre Folgen. Hamburg: Hamburger Edition.

Waddell, K. (2016 May 10). The Computer Virus That Haunted Early AIDS Researchers. The Atlantic. Retrieved from: https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/

Wall, J. (2017). Where to prosecute cybercrimes. Duke Law & Technology Review, 17 (1), 147 – 61. Retrieved from: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1335&context=dltr

Walpen, R. (2005). Die Päpstliche Schweizergarde: acriter et fideliter - tapfer und treu. Padernborn: Schöningh Paderborn.

Walter, D., Ophir, Y. & Jamieson, K. (2020). Russian Twitter Accounts and the Partisan Polarization of Vaccine Discourse, 2015–2017. American Journal of Public Health, 110 (5), 718 – 724.

Ware, V. (2016). Military migrants and mercenary markets. In R. Abrahamsen & A. Leander, Routledge Handbook of Private Security Studies, London: Routledge.

Watkins, J. (2018). No Good Deed goes Unpunished: The Duties Held by Malware Researchers, Penetration Testers, and White Hat Hackers. Minnesota Journal of Law, Science & Technology, 19, 535.

Weber, M. (1919). Politics as a Vocation.

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? Studies in Conflict & Terrorism, 28 (2), 129 – 149.

Westberg, A. (2016). Anti-piracy in a sea of predation: the interaction of navies, fishermen and pirates off the coast of Somalia. Journal of the Indian Ocean Region, 12 (2), 209 – 226.

Wheeler, T. (2020 December 22). NATO, We Want to Go to War With You. Foreign Policy. Retrieved from: https://foreignpolicy.com/2020/12/22/nato-we-want-to-go-to-war-with-you/

Whelan, M. (2006). The Battle of Jadotville: Irish Soldiers in Combat in the Congo 1961. Dublin: South Dublin Libraries.

Wickham-Crowley, T. (1987). The Rise (And Sometimes Fall) of Guerrilla Governments in Latin America. Sociological Forum, 2 (3), 473 – 499.

Wilhelm, T. & Andress, J. (2010). Ninja Hacking: Unconventional Penetration Testing Tactics and Techniques. Amsterdam: Syngress.

Williams, C. (2005). From Conscripts to Volunteers. Naval War College Review, 58 (1), 1 – 28.

Williams, P. (2008). Violent Non-State Actors and National and International Security.

Young, P. (2019 May 1). Artificial Intelligence: A Non-State Actor's New Best Friend. Over the Horizon Journal. Retrieved from: https://othjournal.com/2019/05/01/artificial-intelligence-a-non-state-actors-new-best-friend/

Zannettou, S., Caulfield, T., Setzer, W., Sirivianos, M., Stringhini, G., & Blackburn, J. (2019). Who let the trolls out? Proceedings of the 10th ACM Conference on Web Science - WebSci '19.

Zelalem, Z. (2020 June 27). An Egyptian cyber attack on Ethiopia by hackers is the latest strike over the Grand Dam. Quartz Africa. Retrieved from: https://qz.com/africa/1874343/egypt-cyber-attack-on-ethiopia-is-strike-over-the-grand-dam/

Zetter, K. (2015 May 15). Feds Say That Banned Researcher Commandeered a Plane. Wired. Retrieved from: https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/

Zgoba, K. (2006). Spin doctors and moral crusaders: the moral panic behind child safety legislation. Criminal Justice Studies, 17 (4), 385 – 404.

Zilber, N. (2018 August 31). The Rise of the Cyber-Mercenaries. Foreign Policy. Retrieved from: https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/

Zwanenburg, M. (2012). Military Vessel Protection Detachments: The Experience of the Netherlands. Military Law and Law of War Review, 51, 97.

Project Name

Outsourcing of State Cyber Goals to
Non-State Actors