DIANA FRANCO FREIRE

OFFENSIVE CYBER CAPABILITIES AND STATE VIOLENCE

Dissertation to obtain a Master's Degree in
Law, in the specialty of Law and Security

Supervisor:

Dr. Armando Marques Guedes, Professor of the NOVA School of Law

September 2023

ANTI PLAGIARISM STATEMENT

I hereby declare that the work I present is my own work and that all my citations are correctly acknowledged. I am aware that the use of unacknowledged extraneous materials and sources constitutes a serious ethical and disciplinary offence.

Lisbon, 13 September 2023

Diana Franco Freire

“We are called to be the architects of our future, not its victims”

— R. BUCKMINSTER FULLER

AKNOWLEDGEMENTS

It is with a feeling of academic and personal achievement that I wish to express my deepest gratitude to every single one of the people with whom I had the privilege to meet along the way and that, in some capacity, have contributed to this dissertation:

To my supervisor, Professor Armando Marques Guedes, to whom I am immensely grateful for his invaluable guidance and continuous support throughout this dissertation.

To my parents, for providing me with this opportunity and always pushing me to be better.

To my family and friends for their unconditional support, encouragement, and patience throughout my academic and personal journey.

To my former IT colleague who restored my laptop and saved this dissertation at one point.

And last but not least, I want to thank me for believing in me and putting my all into everything I do.

QUOTING AND OTHER CONVENTIONS

The citation style used in this Master’s dissertation is Norma Portuguesa 405 of the Portuguese Institute of Quality *(Instituto Português da Qualitied*).

Citation follows the rules of the 7th Edition of the American Psychology Association (APA) style. Throughout this dissertation, quotes follow the rule of in-text citations, which included the following elements presented within parentheses: (i) author’s or authors’ surname(s) or the designation of the entity responsible for elaborating the source cited; (ii) the year of publication; and (iii) the page(s) from which the information was cited.

All references are listed in full in the bibliography.

This dissertation follows the rules of American English.

LIST OF ACRONYMS AND ABBREVIATIONS

APTs - Advanced Persistent Threats

CCDCOE - Cooperative Cyber Defence Centre of Excellence (NATO)

CEO - Chief Executive Officer

CFA - Council on Foreign Affairs

CI - Critical Infrastructure

CIA - Central Intelligence Agency (US)

CRD - Civil Rights Defenders

CyCon - International Conference on Cyber Conflict

DDoS - Distributed Denial of Service

ECNL - European Center for Not-for-Profit Law

EPRS - European Parliamentary Research Service (EU)

EU - European Union

FSB - Federal Security Service (Russia)

GCHQ - Government Communications Headquarters (UK)

GRU - Main Intelligence Directorate (Russia)

GTsST - Main Center for Special Technology (Russia)

ICG - International Crisis Group

ICRC - International Committee of the Red Cross

ICTs - Information and Communication Technologies

IIFFMCG - Independent International Fact-Finding Mission (EU)

HRW - Human Rights Watch

IHL - International Humanitarian Law

IL - International Law

IR - International Relations

IS - Islamic State

ISSP - Information Systems Security Partners

JPKF - Joint Peacekeeping Forces

JWT - Just War Theory

NATO - North Atlantic Treaty Organization

NCSC - National Cyber Security Centre (UK)

NHS - National Health Service (UK)

NSA - National Security Agency (US)

OCCs - Offensive Cyber Capabilities

OCOs - Offensive Cyber Operations

OSCE - Organization for Security and Cooperation in Europe

PSYOPS - Psychological Operations

PTI - Press Trust of India

PTSD - Post-Traumatic Stress Disorder

RAM - Random Access Memory

RBN - Russian Business Network

ROCOR - Russian Orthodox Church Outside of Russia

SAIC - Science Applications International Corporation (US)

SQL - Structured Query Language

STOP - Shutdown Tracker Optimization Project

UAVs - Unmanned Aerial Vehicles

UK - United Kingdom

UN - United Nations

US-CCU - United States' Cyber Consequences Unit

USD - United States dollar

VoIP - Voice over Internet Protocol

VPN - Virtual Private Network

WHO - World Health Organization

NUMBER OF CHARACTERS

I hereby declare that this dissertation’s body, including spaces and footnotes, occupies a total of 211.036 characters.

Index

Index of Figures

ABSTRACT

Throughout history, the technological progress and transformations in state violence have been closely intertwined. Despite this connection, prominent studies on cyber conflict often overlook the theoretical examination of violence. Thus, the topic of political violence appears to be fundamentally separated from the analysis of offensive cyber operations, as the prevailing belief is that cyber capabilities constitute mostly non-violent alternatives to traditional means. Nonetheless, as I will argue, academia takes upon a realist, narrow definition of violence, entirely reliant on kinetic force and physical harm. This notion, however, has become obsolete when examining the growingly complex phenomenon. A nascent branch of scholarship sheds light on an extensive array of "under-the-threshold" effects of cyberattacks. These escape conventional doctrines as they are deeply impacting individuals and communities around the world, gradually corroding the very foundations of our modern societies. Using Egloff and Shires' extended notion of "violence" and proposed framework on assessing states' violent uses of cyber capabilities, I aim to examine the violent conduct of one the most prominent and ingenious global players in cyberspace – Russia. These lenses will allow me to run a comprehensive analysis, thereby building a better understanding of the real danger posed by these technologies, both in interstate and repressive contexts.

Keywords: offensive cyber capabilities; cyber operations; state violence; cyberattacks; three logics of integration; digital repression; Russia.

ABSTRATO

Ao longo da história, o progresso tecnológico e as transformações na violência estatal permaneceram intimamente interligados. Apesar desta ligação, os principais estudos sobre os conflitos cibernéticos ignoram frequentemente a análise teórica da violência. Assim, o tópico da violência política parece estar fundamentalmente separado da análise das operações cibernéticas ofensivas, uma vez que a crença predominante é que as capacidades cibernéticas constituem, na sua maioria, alternativas não violentas aos meios tradicionais. No entanto, como argumentarei, o meio académico adota uma definição realista e restrita de violência, inteiramente baseada da força cinética e nos danos físicos. Esta noção, porém, tornou-se obsoleta quando se examina este fenómeno cada vez mais complexo. Um ramo nascente da literatura foca-se nesta vasta gama de efeitos "under-the-threshold" dos ciberataques. Estes escapam às doutrinas convencionais, enquanto detêm um impacto profundo nos indivíduos e nas comunidades de todo o mundo, gradualmente corroendo as próprias fundações das nossas sociedades modernas. Utilizando a definição alargada de "violência" de Egloff e Shires e o quadro proposto para avaliar a violência inerente no uso destas capacidades cibernéticas por parte dos Estados, tenciono examinar a conduta violenta de um dos mais proeminentes e engenhosos atores globais no ciberespaço – a Rússia. Esta perspetiva permitir-me-á efetuar uma análise abrangente, de forma a compreender o perigo real representado por estas tecnologias, tanto em contextos interestatais como repressivos.

Palavras-chave: capacidades cibernéticas ofensivas; operações cibernéticas; violência estatal; ciberataques; três lógicas de integração; repressão digital; Rússia.

I. INTRODUCTION

> "Internet technology has outstripped strategy or doctrine—at least for the time being. In the new era, capabilities exist for which there is as yet no common interpretation—or even understanding. Few if any limits exist among those wielding them to define either explicit or tacit restraints."
>
> - H. Kissinger in *World Order* (2014, p. 334)

Like previous era-defining technologies, global digital networks have been reshaping state violence in ways that academia still struggles to grasp (Gorwa & Smeets, 2019). Over the last decades, the ability to conduct cyber operations has emerged as an important offensive capability, as well as a major national security concern for states (Wittes & Blum, 2016; Sanger, 2018). Some intellectuals contend that war has fundamentally changed, others claim that it has been migrating to cyberspace. Undoubtedly, Offensive Cyber Capabilities (OCCs) pose one of the most urgent issues of our time, with both state and non-state actors increasingly turning to the cyber domain to conduct their illicit actions and practice this type of "modern warfare" (Hoisington, 2009, p. 439). In fact, 'state-driven' cyberattacks are becoming ever more frequent in the international arena, whether they are officially endorsed, sponsored, or 'allowed' by a nation-state (Maurer, 2018). Presently, over 100 countries are capable of launching cyberattacks, more than 30 states have their own cyber forces, and at least 200 state-to-state cyberattacks have been conducted over the past decade (Sanger, 2018; Smeets, 2018).

Nevertheless, few have a handle on how this new 'revolution' is reshaping global power (Sanger, 2018). According to David E. Sanger (2018), in the cyber universe, we find ourselves somewhere in World War I, where cyber capabilities have become as essential to the arsenal of states as airpower was in 1918. In fact, even though no major cyberattacks have seriously crippled the critical infrastructure of a state so far, this reality is not totally farfetched, as their pace of proliferation and scale has been increasing exponentially over the years (Hadji-Janev & Aleksoski, 2013). Ultimately, the consequences that such a premeditated cyberattack could provoke can be comparable to those inflicted by a mass destruction attack (*Ibid.*). Parallelly, others argue that we have now entered into an era of constant, low-level cyber conflicts, which are waged continuously in a "gray area" between war and peace (Valeriano & Maness, 2015; Nye, 2016; Sanger, 2018; Smeets, 2018), or "unpeace" (Kello, 2017). Authors like Valeriano and Maness (2015) oppose the 'revolution in military affairs thesis', as well as the proposition that "cyber weapons will come to dominate the system and will change how states and individuals interact" (p. 2).

These contradicting opinions represent the two dominating positions in cyberwar literature. On the one end, the "cyber hype" (or alarmist perspective) is associated with claims of an incoming "cyber Pearl Harbor"[1], warnings of an ever-pending threat, dramatic scenarios of large-scale disruption, and the emergence of revolutionary military tech (Clark, 2010; Gartzke, 2013). On the other end of the spectrum, the sceptics question the real disruptive and destructive capacity of cyberattacks, together with the very reality of cyberwarfare. In that understanding, offensive cyber operations are solely a "form of cheating", that embody a proxy dominion for the physical realm (Lindsay, 2017, p. 498). Other proponents, like Thomas Rid (2013), draw on Clausewitz's classical teachings to contend that cyberwarfare lacks the crucial factor of lethal force to fit in the definition of war.

The impacts of states' OCCs are vast, with harms ranging from leaked or deleted personal data and extortion to the crippling of critical infrastructures, such as energy grids, transportation infrastructure, or healthcare systems.[2] Indeed, the strategic studies field concedes that Offensive Cyber Operations (OCOs) can provide considerable strategic value to states, as the availability of offensive cyber capabilities expands the panoply of options at the state leader's disposal, across a wide variety of scenarios. In Holsti's (1964) words, "[a]s technological levels rise, other means of inducement become available and can serve as substitutes for force" (p. 190). In truth, they can represent both a valuable force multiplier for conventional capabilities and an independent asset. It follows that these capabilities can be used effectively with few casualties to achieve a form of strategic and psychological superiority. Still, the promise of their strategic value carries a set of conditions, that may at times lead to rather complex trade-offs (Smeets, 2018).

Irrespective of the different positions, the field of political violence seems to be entirely removed from the study of offensive cyber operations, mainly because the present consensus is that cyber operations are almost always non-violent (Egloff & Shires, 2022). Indeed, academia appears to convey to the idea that OCCs represent a significant technological development that offers the possibility of reducing overall levels of state violence (*See* Maurer, 2011; Valeriano & Maness, 2015; Vijaykumar, 2021). As I will demonstrate, in the study of

[1] Warnings of an imminent large-scale cyberwar triggered by a "digital Pearl Harbor" were frequently supported by the U.S. military and defense doctrines (*See* Gartzke, 2013).

[2] Definitions of 'critical infrastructure' (CI) vary across nations. According to the OECD cross-country survey on critical infrastructures from 2017-2018, "half of the 28 definitions gathered from the survey and desk-research, critical infrastructure is described as a combination of both vital processes for societal well-being and a security concern of the state. The other half remain focused on societal well-being and safety only" (OECD, 2019, p. 46). Moreover, this study revealed a "growing concern around interconnectedness and interdependencies of critical infrastructure", given that most definitions include the "combination of networks, systems, facilities, and technologies that contribute to delivering essential services or support vital functions" (*Ibid.*).

cyber conflicts, strategists have systematically prioritized the question of effectiveness and the escalatory potential of OCOs over the assessment of their (potentially) violent impacts (Gartzke, 2013; Gartzke & Lindsay, 2015; Gorwa & Smeets, 2019). Certainly, academics and policymakers are often concerned about escalation and spill-over effects precisely because of their potential for increased levels of violence. However, it should be noted that escalatory effects don't necessarily correlate with growing violent impacts (Egloff & Shires, 2022).

Nonetheless, the general direction has disregarded a significant range of "under the threshold" violent effects. Particularly, the political violence field, which regards violence as its primary object of study, has accepted the premise that OCCs are "largely non-violent alternatives to conventional means" (*Ibid*., p. 4). In reality, it is difficult to conceive of a cyberattack causing the same degree of destruction as bombs or guns, given that the most impactful cyber operations to date have resulted in extensive disruption with substantial economic costs. In most cases, systems could be recovered afterwards and there were no linked fatalities. Therefore, this (seeming) absence of violent effects has largely entertained the thought that offensive cyber operations offer a more 'civilized way' to conduct covert actions and political conflicts (*See* Maurer, 2011; Valeriano & Manness, 2015; Vijaykumar, 2021). These studies, however, focus on a rather 'minimalistic' concept of violence, centered on kinetic force, physical destruction, and human casualties.

That being said, with this research study, I plan to address this gap in the literature. In line with Egloff & Shires (2023), I believe that these capabilities' power to inflict harm through informational means introduces a new category of non-kinetic violence. Following this reasoning, Brantly (2017) contends that offensive cyber capabilities are constitutive of "both physical and non-physical, threatened, and applied forms of violence" (p. 73). In this sense, I will take on Egloff and Shires' model to access violent uses of OCCs and apply this framework to famous cyberattacks that made global headlines and transformed our views on the (violent) potential of OCOs. Delimiting my study to the Russian state as the perpetrator, due to its foremost importance in international cyber conflicts, I will analyze the use of OCCs at the onset of Georgia's invasion and the unprecedented NotPetya malware attack. In addition, I will strive to comprehend Russia's use of cyber tools for repression purposes, both domestically and abroad. I maintain that examining these forms of violence is key to understanding the broad array of harms that these new weapons cause in their wake. This is an essential step in the process of comprehending this complex phenomenon, so that it can be properly addressed and integrated into theoretical, legal, and policy frames.

1.1. Literature Review

Despite the growing relevance of cyber operations in modern foreign policy, the academic literature on cyber conflict remains fairly nascent (Gorwa & Smeets, 2019). It can be argued that political experts are still struggling to grasp the full extent of the lessons on offense, defense, deterrence, escalation, norms, arms control in cyberspace, and how they fit together into a national strategy (Nye, 2011a). In the words of Adam Liff (2012), while scholars like Bernard Brodie have highlighted the transformations and implications of nuclear weapons on state interaction, "[n]o comparable comprehensive assessment of the impact of cyberwarfare capabilities exists. Outside the slowly emerging policy literature, there is limited scholarly work on the topic, leaving important theoretical questions unexamined". From the perspective of international security, his study shows that the current literature has prioritized theoretical work over empirical research (*Ibid.*; Valeriano & Maness, 2015).

A 2019 study on the prevalence of cyber conflict literature revealed that, notwithstanding the two decades of research, this topic remains of relatively small importance within the field of political science (Gorwa & Smeets, 2019). This paper uncovered that the main three topics explored in cyber conflict literature, discussed since the early works published in 1995, were "Cyberwar", "Coercion"[3], and "IL [International Law] and Norms", respectively (*Ibid*., p. 9; *See* Fig. 1). Likewise, cyber deterrence and the problem of attribution have also raised significant interest in scholars. Still, while being extensively studied themes in the broader literature, they have not received the expected attention in this field (*Ibid.*). Notably, the topic of 'violence' does not enter this chart (at least not as a separate area of study).

In fact, as mentioned above, the strategic studies field has systematically neglected the concept of violence over more analytical terms. As a consequence, important studies on cyber conflict tend to overlook the concept of violence from a theoretical and empirical perspective, prioritizing more strategic dimensions. For instance, Kello (2017) claims that OCCs generate instabilities within the international system, thereby focusing on the distribution and transfers of power, irrespective of their violent nature. Conversely, Nye (2011a) suggests that cyberwar could be realistically defined as hostile actions in cyberspace, whose effects are equivalent to or may even amplify those of kinetic violence. In this regard, it remains unclear whether such effects are strategically equivalent, regardless of their level of violence, or equivalent in terms of the degree of violence they entail (Egloff & Shires, 2022).

[3] In line with Shelling (1966), coercion refers to both 'deterrence' and 'compellence' in the cyber context. I will expand on these concepts *infra*.

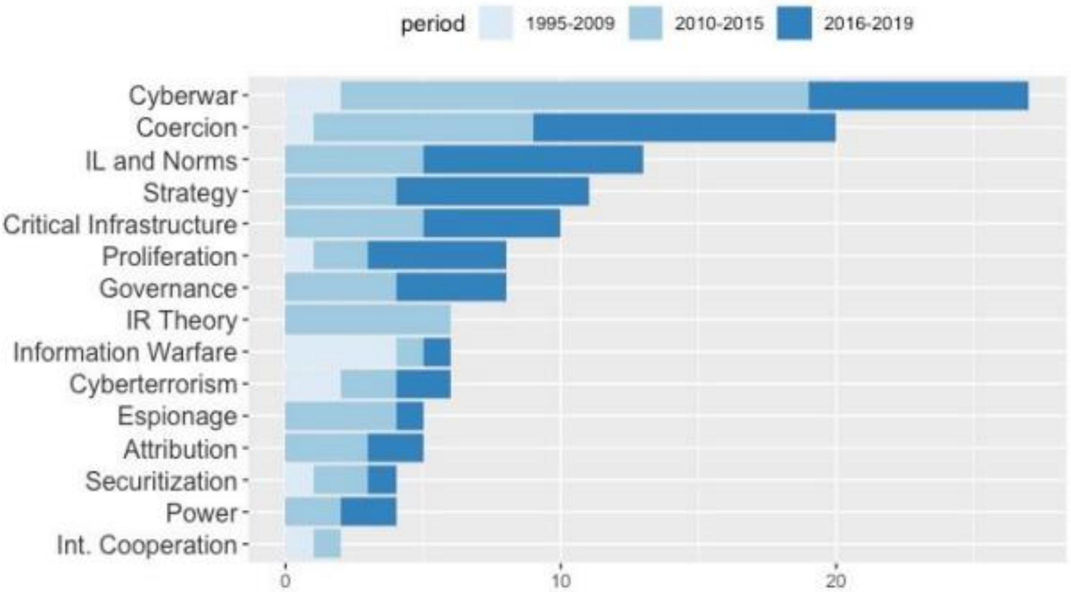


Figure 1: Main topics in Cyber Conflict literature (1995-2019)

Source: Gorwa & Smeets (2019, p. 9)

On the other hand, Betz and Stevens (2011) wrote that the "[p]opular discourse on cyberwar tends to focus on the vulnerability of the physical layer of cyberspace to cyberattacks and how this may permit even strong powers to be brought to their knees by weaker ones, perhaps bloodlessly" (p. 76). The 'bloodless war'[4] argument rests primarily on the assumption that cyberwar would be less violent than conventional warfare (*See* Smeets, 2018). Maurer (2011) concluded that "[the] evidence so far suggests, however, that a digital Pearl Harbor would cost fewer lives than the attack 70 years ago. It might not be pretty, but from a humanitarian point of view, that's good news". Other proponents of the 'peaceful nature thesis', like Thomas Rid and John Arquilla, reason that the potential for fewer casualties calls for the use of cyber capabilities at the expense of conventional warfare means (*See* Arquilla & Ronfeldt, 2001; Libicki, 2016; Rid, 2017).

In response to what was perceived as an overly statistical focus on strategic issues during the Cold War (e.g., nuclear deterrence), the political violence subfield emerged with the intent to redirect scholars toward the study of violent acts perpetrated for political ends. This included violence committed by state and non-state actors during wars or social unrest periods. This theoretical reorientation rested on the normative premise that the study of conflicts should be focused on the prevention and minimization of their harms and devastating outcomes (Egloff

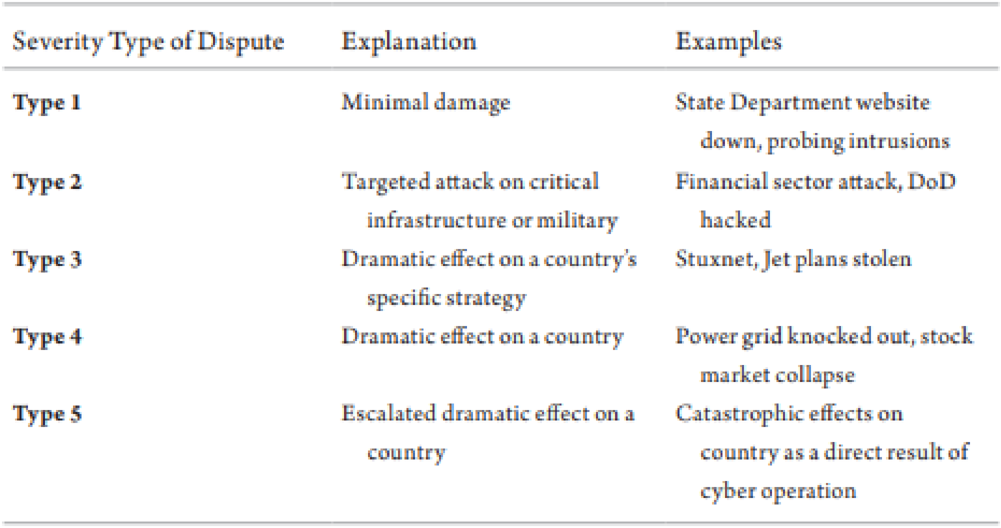
[4] In a speech during the launch of the "Digital India Week", in 2015, India's Prime Minster Narendra Modi stated that "clouds of a bloodless war are hovering in the world" (PTI, 2015).

& Shires, 2021). Accordingly, extensive theoretical analysis of the term has led to its division between narrower and broader understandings of violence (Bufacchi, 2005; Baron *et al*., 2019; Egloff & Shires, 2021). Henceforth, fruitful research agendas spurred from both conceptions.

In brief, the narrow definition of violence is largely physical, centered on kinetic force and lethal destruction. In this light, Rid (2013) asserts that "most cyberattacks are not violent and cannot sensibly be understood as a form of violent action" (p. 12). His famous work *Cyber War Will Not Take Place*, which was built on a narrow understanding of violence (detached from other forms of harm), set the tone for the subsequent literature (*See* Gartzke, 2013; Valeriano & Maness, 2015; Gartzke & Lindsay, 2017). These studies, many of which were produced in the aftermath of the Stuxnet[5] cyberattack, concluded that OCCs couldn't produce a level of destruction equivalent to that of traditional weapons (Denning, 2012). Accordingly, "[w]eaponized computer code and computer-based sabotage operations make it possible to carry out highly targeted attacks on an adversary's technical systems without directly and physically harming human operators and managers" (Vijaykumar, 2021). In truth, the major cyberattacks so far may have caused widespread disruption and immense financial losses, however, no casualty resulted from these attacks. Today, the 'nonviolent nature' claim seems to have prevailed, according to Florian J. Egloff and James Shires (2022; 2023).

Nonetheless, some studies attempted to assess violence in OCOs more closely. For instance, Valeriano and Maness (2015) – one of the few quantitative research projects in the field – endeavored to advance a "severity scale" from type 1 to 5 (the latter being the most severe of incidents, labeled "escalated dramatic effect on a country") for cyber violence (p. 85; *See* Fig. 2). In this case, the authors are not explicit about their definition of violence, which appears to be mistaken with the severity of effects directly resulting from a cyber operation. On this topic of escalation, cyber capabilities are still regarded as largely nonviolent means of state action (*Ibid*.). Libicki (2012), in his turn, contrasts "the limited risks of cyberescalation with the nearly unlimited risks of violent escalation" (p. 78). In general, although these analyses address political violence more forwardly, they tend to examine violence primarily regarding "spill-over" effects to the physical world (Egloff & Shires, 2022, p. 4).

[5] Stuxnet is a malicious computer worm that is believed to have been developed as a joint operation between US and Israeli intelligence services and used to compromise the industrial control systems at the Natanz nuclear material enrichment facility in Iran, in 2010. This OCO was allegedly codenamed 'Olympic Games' (Fruhlinger, 2022).



Severity Type of Dispute	Explanation	Examples
Type 1	Minimal damage	State Department website down, probing intrusions
Type 2	Targeted attack on critical infrastructure or military	Financial sector attack, DoD hacked
Type 3	Dramatic effect on a country's specific strategy	Stuxnet, Jet plans stolen
Type 4	Dramatic effect on a country	Power grid knocked out, stock market collapse
Type 5	Escalated dramatic effect on a country	Catastrophic effects on country as a direct result of cyber operation

Figure 2: Severity scale of OCOs, in crescent order

Source: Valeriano & Maness (2015, p. 85)

Some authors set out to challenge this purely kinetic view on violence. In his article entitled *The Violence of Hacking: State Violence and Cyberspace*, Aaron F. Brantly (2017) argues that violence at the state level cannot be limited to "pre-digital static definitions", invariably focused on what constitutes a use of force in cyberspace (p. 73). Instead, similarly to conventional violence, cyber violence committed by state actors comprises both physical and non-physical acts. Importantly, whereas Lupovici (2016) highlights the social-constructivist nature of violence in the cyber sphere, Stevens (2015) introduces the "affective implications" of cyber operations into the equation, which may involve feelings of insecurity or fear (p. 103). Agrafiotis *et al*. (2018), in their turn, advance a taxonomy of cyber-harms that encompasses physical or digital harm, economic harm, psychological harm, reputational harm, and social and societal harm. In this logic, Egloff and Shires (2022) developed a definition of violence that includes non-physical forms of cyber violence, particularly those that "intentionally cause harm to the affective life of individuals or community values and identities" (p. 5).

Furthermore, numerous scholars uphold the idea that, while most displays of violence are prompted by direct or threatened physical force, the cyber domain rarely owns a direct causal relationship with the force it generates (*See* Kello, 2013). These are also the same theorists that reduce the conception of cyber violence to instances of manipulation or subversion (*See* Rid, 2013). Nonetheless, as stressed by Brandy (2017), the present focus on first-order effects of violence disregards a vast array of second and third-order consequences. In this context, Baron *et al*. (2019) don't distinguish between 'structural' and 'affective' impacts, instead placing them within what the author comprehends as a broader concept of violence. Moreover, Egloff and Shires (2022; 2023) contend that, considering this expanded conception, OCCs don't lead to the reduction, but rather the relocation, of state violence. Finally, the recognition of violence as a complex phenomenon that cannot be limited to physical actions could provide a venue for rethinking legal and policy concepts in ways more adjusted to the specificities of the digital era (Egloff & Shires, 2022).

1.2. Detailed Description and Methodology

I approach this research project with two basic questions in mind. First, I plan to uncover whether offensive cyber capabilities – "the combination of various elements that jointly enable the adversarial manipulation of digital services or networks" – truly are the non-violent alternatives to conventional means that the academia suggests they are (Egloff and Shires, 2023). Opposing the present academic consensus, Egloff and Shires (2022; 2023) reasoned that OCCs don't exactly reduce the overall levels of state violence; instead, these capabilities can often lead to the diffusion (or even increase) of violence in the extended sense. Hence, as I will describe, the abovementioned authors center their hypothesis on a definition of violence that comprises bodily, affective and community harms, thereby moving beyond the solely physical conception. Essentially, I agree that academic research should overcome the purely strategic analysis of cyber conflict, towards creating a more holistic understanding of cyber violence. Crucially, it should also focus on identifying the various forms of violence and harms inflicted by these new kinds of weapons.

Secondly, I aim to assess whether Egloff and Shires' proposed framework constitutes an effective model to examine the violent implications of the use of OCCs. In this regard, I begin by laying out the conceptual framework developed by these scholars, which draws on the current branch of literature that focuses on the extensive conception of violence. Additionally, in order to understand the incorporation of OCCs into states' violent capabilities, these scholars propose three logics of integration – substitution, supportive, and complementary – to guide the subsequent research work on the topic. Following this reasoning, I plan to assess the state violence intrinsic in these uses of cyber capabilities, thereby comparing both the strict and the extended definitions. Here, these authors assert that, contrarily to substitutive and supportive logics, that can be mostly adjusted to present legal frameworks, the complementary use of OCCs raises a whole new normative challenge to policymakers, given that it can also lead to improved levels of violence (*Ibid.*).

1.2.1. Florian J. Egloff and James Shires' mode of analysis

1.2.1.1. Defining 'State Violence'

In principle, violence is interpreted by these authors as "intentional proximate harm to areas of human value, including the body, affective life, and social relationships" (Egloff & Shires, 2023, pp. 131-132). As demonstrated *supra*, this view consolidates a substantial body of research that is theoretically separated from the strategic studies field. By introducing this wider conception of violence, Egloff and Shires (2023) not only expand the study of complex violent dynamics in cyberspace, but also push to the redirection of research and policymaking towards countering and alleviating those problems. Foremost, this definition is anthropocentric, as it focuses on human entities and the harms that might befall them. Moreover, it is constrained to a specific type of actor – the state. Notwithstanding the prominent role of non-state actors in political violence, these academics reckon that state violence remains central in most studies of OCCs (*Ibid.*).

Respectively, the criterion of intention establishes that for an act to be considered violent, it must be intended to cause harm. Therefore, this definition doesn't comprise structural harms (caused, for example, by ethnicity, gender, or capitalism), since social structures cannot be attributed intention in themselves (*Ibid.*). In addition, states' reliance on proxies and private contractors further obscures these estimates (*See* Maurer, 2018). Plus, when considering accidental or negligent action (e.g., collateral damage), some theoretical challenges arise. To counter these problems, the authors maintain that intention constitutes a "socially ascribed quality" (Egloff and Shires, 2023, p. 139). Accordingly, drawing on legal traditions worldwide, intent can be ascribed if the harm could have been reasonably projected or anticipated by the perpetrators. Of course, this parameter is particularly context-dependent.

Subsequently, an act must be deemed a proximate cause of harm so as to be considered violent. This definition concedes that the impacts of cyber operations are sufficiently proximate to be assigned a violent connotation. On the contrary, scholars like Kello (2013) maintain that cyberattacks "lack a proximate cause of injury" (p. 25). This factor touches upon the second and third-order effects argument brought above, as well as on the main division between material and informational means. Indeed, temporality and distance play an influential role in determining proximity. Yet, how violence is committed ascribes causal importance to different factors. Besides, informational and material means are not mutually exclusive in the deployment of cyber capabilities. To illustrate this, Egloff and Shires (2023) compare OCCs with armed unmanned aerial vehicles (UAVs). Contrary to OCCs, UAVs are viewed as remote means capable of provoking kinetic violence, although their informational infrastructure is equally complex and, in some ways, similar to OCCs (*Ibid.*). Specifically in the case of drones, the missile's causal impact (material means) surpasses that of the command-and-control structure when it comes to inflicting harm. On the other hand, considering a hypothetical situation in which OCCs were to be used to provoke explosions on a military complex, comparable to those of a UAVs attack, this scenario would still qualify as an informational means of violence. This is justified by the greater causal weight assigned to the assumed virus that alters the facility's systems and causes them to detonate.[6]

Finally, this concept comprehends a wider understanding of the harms provoked by cyber operations – bodily, affective, and communal (Egloff & Shires, 2022). These constitute the main three "areas of human value". Importantly, the authors view these areas as socially constructed realities, instead of biologically pre-given facts, which speaks to their non-exhaustiveness and non-generalizable nature (Egloff & Shires, 2023). Whereas measuring bodily violence is relatively straightforward, affective harms – which comprise harms to a person's emotional and psychological state – raise more analytical difficulties, due to its non-physicality (*Ibid.*). As for community harms, in this sense, they do not only involve social relationships, but also collective identities, symbols, and traditions. Similarly, in its definition of violence, the World Health Organization (WHO, 2022) encompasses the intentional nature of the use of (in this case) physical force "threatened or actual, against oneself, another person, or against a group or community, which either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation" (p. 1).

Consequently, a cyberattack that intentionally causes harm to crucial human interests, specifically to the body, the affective life of individuals, or communities' systems and relationships, can be considered violent in the broad sense. What is more, the bandwidth of harms defended by the authors denotes the absence of a minimal threshold of violence. Thus, any use of OCCs that causes harm in this sense falls within the violence spectrum. Certainly, the 'severity scale' of harms is especially relevant to assess. As it is context-dependent, it varies greatly between and within these different areas of value, that nevertheless interconnect and overlap each other. In this regard, their authors advance that harms that affect communities ought to be equated, or even prioritized, to individual affective harms, revealing a utilitarian

[6] Nonetheless, it is worth mentioning that this theoretical scenario was oversimplified to illustrate this point. A real-life situation would demand a comprehensive examination grounded on the components laid out by this definition.

logic. Taking into consideration that violence is both an analytical and a normative concept, they do still refuse the systematic prioritization of bodily harms over other forms of violence.

Following this logic, Distributed Denial of Service (DDoS) attacks (*See* Fig. 4), generally regarded as non-violent protests, may constitute violent uses of OCCs in the extended sense, provided that they negatively affect individuals' lives or communities (i.e., by diminishing or degrading these areas of human value) (*See* Asal *et al.*, 2016). In addition, forced internet shutdowns, mass digital surveillance, or repressive cyber-espionage campaigns on certain communities directly fall within these categories of harm. Critically, in the strict sense, such capabilities wouldn't be deemed violent, unless they led directly to physical acts of aggression (e.g., bodily punishments or torture). Most importantly, these authors maintain that recognizing how the use of cyber capabilities is inserted into states' broader decisions is central to assessing this phenomenon.

1.2.1.2. The Three Logics of Integration

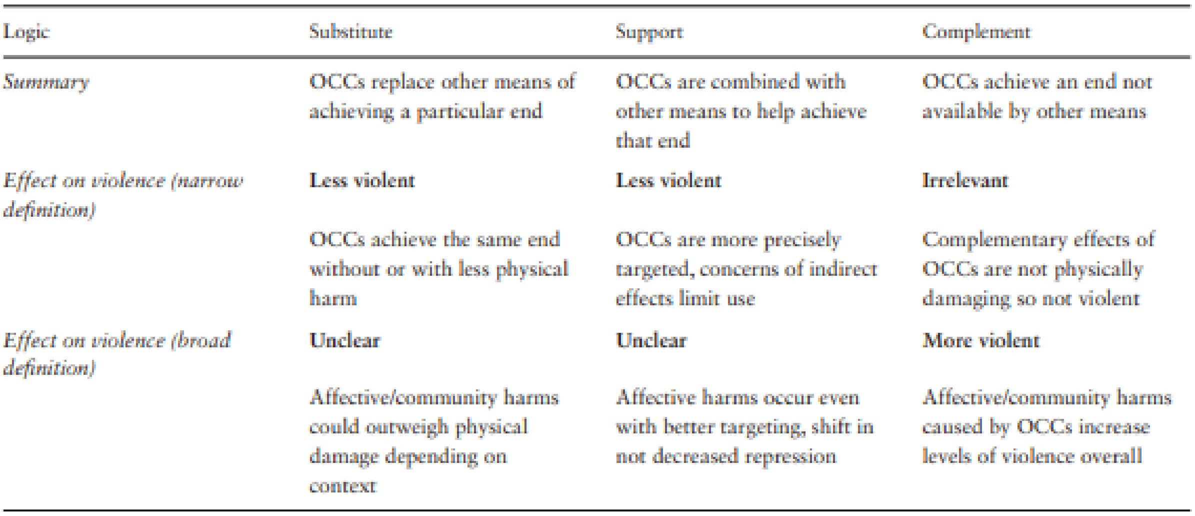
Egloff and Shires (2022) add that the offensive uses of cyber tech must be analyzed in relation to other forms of political violence, particularly by examining how they integrate within these manifestations. In this regard, Eric Gartzke (2013) wrote that "'cyber war' is not likely to serve as the final arbiter of competition in an anarchical world and so should not be considered in isolation from more traditional forms of political violence" (p. 42). Therefore, the authors view these decisions between cyber and non-cyber operations within larger campaigns. They assume that there's no such thing as a strictly 'cyber' campaign, as they are inserted into different forms of state action (e.g., intelligence gathering, logistic support, military action, etc.). Accordingly, these logics of integration – *substitution*, *support*, and *complement* – shed light on the advantages of employing OCCs against an opponent *instead of*, *as part of*, and *in addition to* other means of violence, respectively (Egloff & Shires, 2022; 2023).

As mentioned *supra*, the role of OCCs as non-violent alternatives to traditional means makes them a reliant substitute for force in an interstate clash. Examples of such cyber operations replacing destructive physical methods (but achieving similar effects) include the Olympic Games (more famously known as Stuxnet), as well as various forms of digital repression or intimation (for instance, by using spyware to surveil, control and coerce political adversaries or other dissidents). In terms of repressive state surveillance, OCCs stand out as the easiest and cheaper substitute for gathering information, considering that this method allows states to remotely breach into their citizen's private lives (Asal *et al.*, 2016). What is more, instances of targeted surveillance, blackmail, sabotage, or hacking and leaking of sensitive information are common uses of cyber capabilities by (particularly authoritarian) states, in a substitutive logic. Nonetheless, while many believe that a cyber operation involves less violence than their physical alternatives, these authors reason that non-bodily harms could tilt the equation, especially in repressive contexts.

Following this reasoning, supportive uses of OCCs – used in combination with non-cyber tactics – can also lead to violence, particularly when they enhance the accuracy, scope, and power of traditional means. At the interstate level, we can point out the 2007 Israeli hybrid attack against a Syrian nuclear facility. The network attack aimed at blinding and disabling (or jamming) the entire Syrian air defense radar system to facilitate and secure the kinetic operation – destroying the nuclear reactor (Cenciotti, 2013). Likewise, OCCs may also support repressive means. On this topic, the Citizen Lab, an interdisciplinary research center, reveals instances in which OCCs led to arbitrary arrests, torture, or even extrajudicial assassinations within states' security structures (Deibert, 2020). Fundamentally, supportive uses of OCCs often take part in broader conflicts involving other warfighting or oppression means.

The third logic of integration – complementary uses of OCCs – stands out as the most dangerous one, as it brings digital ways of generating harm to a whole new level (Egloff & Shires, 2023). Contrary to substitutive or supportive uses of OCCs, the complementary capabilities deliver a result that could not have been accomplished by any other means. As to illustrate their potential, the authors hypothesize the simultaneous prompting of numerous system failures across an adversary's networks. In his book *The Perfect Weapon*, Sanger (2018) mentions the "Nitro Zeus" project, which referred to the US covert plan of launching a crippling full-scale cyber assault on vital Iranian networks. Allegedly, this would plunge the whole country into a digital blackout and thus prevent any possible retaliation in case of an open nuclear conflict with Iran (*See* Sanger & Mazzetti, 2016). Crucially, these scholars defend that complementary uses of OCCs raise the total levels of violence of an operation, as they add novel capabilities to the state.

Another example is the capacity to maintain extensive surveillance networks across the globe, that are at the same time highly targeted on specific opposition nets. In this regard, these abilities may help build a context of widespread censorship and control, intrusive incursions into people's privacy, and growing fear. There are many cases associated with this type of autocratic terror (e.g., China, Russia, Syria), which can be linked to highly damaging impacts on citizens' rights, lives, and relationships. Regarding interstate disputes, the WannaCry ransomware attack (as I will explain *infra*) can be signaled as a violent operation in the extensive sense, given that it spread profusely throughout multiple countries, directly disrupting the UK National Health System and delaying patients' treatments. Similarly, the 2016 malware attack by Russian hackers on Ukraine's national grid (*Ukrenergo*) provoked an electrical shutdown in the midst of winter. Had it been prolonged for longer than several hours (as the perpetrators arguably intended), this situation could have resulted in Ukrainian casualties (*See* Greenberg, 2019a).



Logic	Substitute	Support	Complement
Summary	OCCs replace other means of achieving a particular end	OCCs are combined with other means to help achieve that end	OCCs achieve an end not available by other means
Effect on violence (narrow definition)	**Less violent**	**Less violent**	**Irrelevant**
	OCCs achieve the same end without or with less physical harm	OCCs are more precisely targeted, concerns of indirect effects limit use	Complementary effects of OCCs are not physically damaging so not violent
Effect on violence (broad definition)	**Unclear**	**Unclear**	**More violent**
	Affective/community harms could outweigh physical damage depending on context	Affective harms occur even with better targeting, shift in not decreased repression	Affective/community harms caused by OCCs increase levels of violence overall

Figure 3: The Three Logics of Integration and their effect on state violence

Source: Egloff & Shires (2022, p. 12).

All in all, these examples seem to imply that the use of offensive cyber capabilities, in all three logics of integration, is an increasing trend, both in tactical and strategical fields of decision. Still, this division is essential to calculate the exact logic of integration. For instance, whilst targeted surveillance on political dissidents using spyware could be regarded as a substitutive use of cyber capabilities at the tactical level, strategically, this decision is supportive of a broader goal of controlling the opposition. The WannaCry worm – which was supposedly leaked by a North Korean hacking group named 'Lazarus Group' – brought "unprecedented economic damage and disruption to businesses in the United States and around the globe" (US Department of Justice, 2018). In strategic terms, this cyberattack can be viewed as supportive of a much larger destabilization (or power projection) campaign carried out by North Korea (Hern & MacAskill, 2017).[7] On the other hand, tactically, the degree of

[7] According to the BBC News (2017a), both the U.S. and the U.K. blamed North Korea for the WannaCry attack. In an article for The Guardian, the threat intelligence company Recorded Future added that the "[u]se of

indiscriminate disorder caused by this weapon seems to constitute a complementary use of OCCs, as it did not support nor substitute any traditional means of violence.

1.2.2. Main Research Questions:

After having delineated the model of analysis proposed by Egloff and Shires (2022; 2023), I will attempt to test whether specific offensive cyber operations can be considered violent. In doing so, the division established *supra* between traditional (mainly physical) and broader definitions of violence is key, provided that the violent impacts of OCCs are contingent to both the notion of violence adopted and to which logic of integration is verified. Here, two assumptions are central to the work of these scholars, which I will carry into mine. First, purely cyber campaigns don't exist, as the employment of cyber operations is always part of wider, more complex decisions made by states (Gartzke & Lindsay, 2017). Secondly, I regard interstate and repressive displays of state violence as part of a single continuum of state violence (*See* Chenoweth *et al.*, 2019; Egloff & Shires, 2022). In this work, I will focus on a prominent global actor in the cyber sphere: the Russian Federation, in an endeavor to test these authors' theory. To clarify, I won't try to uncover whether Russia's offensive actions in cyberspace are more violent than this nation's conventional means of power, inasmuch as I will analyze their violent character in respect to the logic of integration they bear.

To answer the main questions, I will start Chapter II by reviewing leading scholarship in the field, as well as numerous case studies, news articles, legal reviews, and relevant surveys. Following a brief introductory analysis of the relationship between the evolution of state violence and emerging technologies, I will discuss pertinent topics in cyber conflict studies that touch upon information ethics, military and legal doctrines, cyberpsychology, and the known impacts of OCOs. Accordingly, in this section, I will concentrate on the concepts of 'violence' and 'harm'. With this, I plan to investigate not only the ethical and legal foundations of this hypothesis, but also their plausibility. Afterwards, while focusing on the 'three areas of human value', I will try to understand the social and psychological impacts following a cyberattack (or an act of cyber terror) by analyzing recent surveys on the topic. Relevantly, one of these studies compares the effects on people of hypothetical instances of cyber terrorism to those of physical and lethal acts of terror. Hence, I will gather some important insights from this

ransomware to raise funds for the state would fall under both North Korea's asymmetric military strategy and 'self-financing' policy, and be within the broad operational remit of their intelligence services" (Hern & MacAskill, 2017).

emerging research that contraries the prominent focus on physical harm in political violence studies.

Subsequently, in Chapter III, I'll scrutinize the theoretical foundations of cyber conflict literature, actual international trends, and pertinent debates. Hereafter, using this broad definition founded on a multidisciplinary approach on violence, I intend to analyze expressions of violent character in both interstate and repressive contexts. In this regard, the employment of OCCs in a particular campaign is violent to the extent that it results in bodily, societal, or psychological harm to its victims. Of course, the more victims it leaves in its wake, the more violent it is deemed (*See Ibid.*). At the same time, I will assess them in light of the different logics of integration within the states' violent apparatus. In an incipient field like cyber violence, where core concepts are still underdeveloped and data collection methods are embryonic, I have chosen to replace quantitative analysis with qualitative, hypothesis-testing case studies.[8]

Now, this dissertation's case studies – the Georgia's invasion in 2008, the NotPetya attack in 2017, and an analysis of Russia's (and Chechnya's) digital repression technics – were selected based on their manifest importance in this evolving domain.[9] In truth, the Georgia invasion figures as the first conflict where OCOs were deployed in tandem with the hostilities, whereas the NotPetya worm revolutionized modern cyberattacks and took the international community by surprise with its unparalleled scale, scope, and sophistication degree (Sanger, 2018). Here, I will primarily rely on the Council on Foreign Affairs' (CFA) database and the CCDCOE database (and the associated open sources) in order to build a holistic understanding of both cases. In this sense, I will examine case studies, official reports, news articles, think tank publications, and governmental press releases. In the end, I will draw my conclusions using both the narrow and the broader definitions so as to contrast my findings.

In Chapter IV, I will dive into the question of digital repression before turning to the analysis of Russia's repressive machine. Overall, this country's multifaceted, highly aggressive approach makes up a unique take on cyberspace as an effective vector for transnational state violence. In this case, I will base my analysis on comprehensive reports and independent country case studies, especially by interdisciplinary organizations such as Freedom House and Citizen Lab, to draw a complete picture of this extensive campaign. I will then proceed to explore the Chechen case in greater detail, in line with Egloff & Shires' theory.

[8] On this typology of case studies (hypothesis-testing), *see* Levy (2008).

[9] Interestingly, Russia is part of the so-called "Seven Sisters" of cyber conflict – i.e., the most advanced and capable actors in the cyber domain – next to the U.S., U.K., China, Iran, Israel, and North Korea (Sanger, 2018).

To sum up, the independent variable is the logic of integration in the employment of OCCs, whilst the extended notion of violence – "intentional proximate harm to areas of human value" – configures the dependent variable. Accordingly, I'll employ deductive reasoning to test these scholars' plausibility probe, at the same time comparing both the narrow and broad definitions of (state) violence in their utility. In doing so, I will be able to assess the benefits, implications, and limitations of using this mode of analysis to study the violent effects of cyber operations.

1.3. Explanation of Key Concepts

In 1982, the science fiction writer William Gibson (2013) coined the term 'cyberspace' in his short story *Burning Chrome* (and later popularized it in his book *Neuromancer*), as a mass "electronic consensus-hallucination". Gibson envisioned that, as technology progressed, our imagination would enrich this otherwise non-existent space, reflecting our innate human tendency to give structure to the intangible. Presently, the internet embodies this consensual shared hallucination, with websites recreating real-world experiences like commerce, leisure, education, and social interactions (*See* Brantly, 2017). Put simply, 'cyber' implies digital interactions; hence, 'cyberspace' configures the sum of "networked systems of microprocessors, mainframes and basic computers that interact at the digital level" (Valeriano & Maness, 2015, p. 3). Nye (2011b) highlights the underlying political context, stating that "[t]he cyber domain includes the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and the political laws of sovereign justification and control" (p. 19).

Following this logic, very succinctly, Valeriano and Maness (2015) refer to 'cyber conflict' as the employment of computational technologies and capabilities for malicious and destructive aims, with the intention to impact or alter the relations among parties.[10] In this sense, 'cyberwar' configures an "escalation of cyber conflict to include physical destruction or death" (*Ibid*., p. 3). Conversely, other academics reckon that "[a] more useful definition of cyber war is hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence" (Nye, 2011b, pp. 20–21; *See* Clark & Knake, 2010). Nonetheless, the terms 'cyberwar' and 'cyber conflict' are often used interchangeably in strategic studies literature. A key distinction in cyber conflict studies, which I will carry into my work, is that cyberwar

[10] Here, Valeriano and Maness (2015) refer to these cyber conflict 'parties' specifically as "states" (p. 3). Although my research is focused on the role of states in this type of conflicts and their uses of cyber capabilities, I reckon that non-state parties currently also have the power to weaponize these technologies in conflict scenarios.

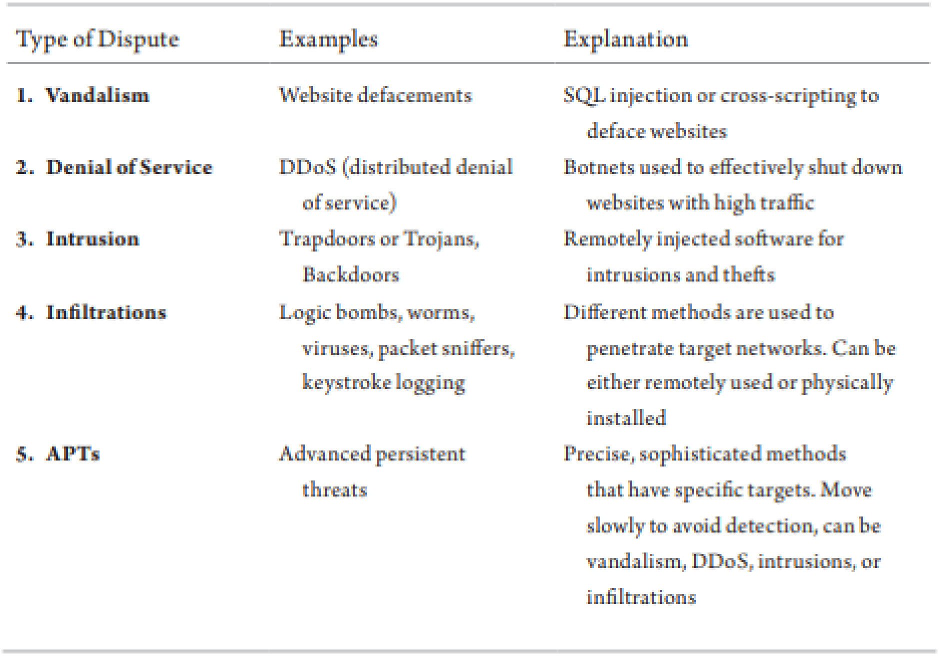
constitutes a state of armed conflict in which OCOs (defined *infra*) are employed to seek military objectives, whereas cyber conflict portrays a situation in which this OCCs are used below the threshold of 'armed attack' (I will expand on this discussion below) (Egloff & Shires, 2023; *See* Kello, 2017). For the purpose of this dissertation, I regard cyber conflict as an aggressive foreign security tactic used between states.

In line with Egloff & Shires (2022), I define offensive cyber capabilities as "the combination of people, technologies, and organizational attributes that jointly enable offensive cyber operations: the adversarial manipulation of digital services or networks."[11] (p. 1). These capabilities encompass various technological aspects such as the infrastructure required for surveillance and overseeing operations, methods for intrusion, tools obtained from open sources, etc. In addition, they comprise skilled staff for the development and implementation of these technological assets, as well as the organizational capacity to effectively manage, coordinate, and acquire the necessary permissions and legal authorizations (*Ibid.*; Egloff & Shires, 2023). In essence, the term 'OCCs' comprehends what is commonly known as 'cyber weapons', while also emphasizing the technological, administerial, logistic, and human investment needed for cyber operations.

As described by the Tallinn Manual on the International Law Applicable to Cyber Operations (hereafter, "Tallinn Manual"), cyber operations generally configure "[t]he employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyber space" (Schmitt, 2017, p. 564). These types of operations focus on capabilities related to information, aligning with the information warfare aspects of psychological operations, military deception, operational security, electronic warfare, and diverse forms of intelligence gathering (*Ibid.*). It follows that offensive cyber operations are powerful instruments of statecraft (Demchak, 2011). In its turn, a 'cyber weapon' represents "a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings" (Rid & McBurney, 2012, p. 6). Importantly, cyber weaponry greatly varies in type, target, usage, and employment (Valeriano & Maness, 2015). In this regard, Valeriano and Maness (2015) outline four fundamental methods used in cyber conflicts, as demonstrated below in Fig. 4[12] – through a crescent order of complexity:

[11] In this logic, 'adversarial' basically means against the victim's or target's interests (*See* Egloff & Shires, 2023).

[12] Advanced persistent threats (APTs) introduce an additional dimension to the realm of cyber techniques and can manifest themselves in any of the four methods outlined (Sanger, 2018; *See* Fig. 4)). Examples of APTs like the Stuxnet worm illustrate their personalized nature and deliberate, gradual pace to evade detection. These tactics



Type of Dispute	Examples	Explanation
1. Vandalism	Website defacements	SQL injection or cross-scripting to deface websites
2. Denial of Service	DDoS (distributed denial of service)	Botnets used to effectively shut down websites with high traffic
3. Intrusion	Trapdoors or Trojans, Backdoors	Remotely injected software for intrusions and thefts
4. Infiltrations	Logic bombs, worms, viruses, packet sniffers, keystroke logging	Different methods are used to penetrate target networks. Can be either remotely used or physically installed
5. APTs	Advanced persistent threats	Precise, sophisticated methods that have specific targets. Move slowly to avoid detection, can be vandalism, DDoS, intrusions, or infiltrations

Figure 4: Fundamental methods used in cyber disputes

Source: Valeriano & Maness (2015, p. 85)

At its core, the emergence of the modern state is linked to the establishment of the state's monopoly on violence – i.e., the notion that the state has the right to use and authorize the use of (physical) force (Weber, 1919/2015). Notwithstanding the empirical fragmentation associated with the political violence field, which hampers its comprehensive study, some social scientists have advocated for a broader take on state violence, "ranging from direct political violence and genocide to the redefinition of state violence as the neoliberal exit of the state from the provision of social services and the covert use of new technologies of citizen surveillance" (Torres, 2018, p. 381). Indeed, it can manifest itself in various forms, including armed conflicts, police brutality, extrajudicial murders, or systemic oppression. Hence, in simple terms, state violence refers to the branch of political violence focused exclusively on the state and its structures. For this work, I define state violence as violence[13] enacted, sponsored, or permitted by state actors, both in interstate and repressive scenarios.[14] That said, I will now delve into the close relation between state violence and technological advancements.

typically exhibit heightened maliciousness and unparalleled sophistication, almost invariably originating from state actors, and targeting specific entities with dreading precision (Valeriano & Maness, 2015).

[13] The concept of violence that I adopted is already extensively defined *supra.*

[14] I use the terms "interstate" and "repressive" as different categories of state violence, with the former denoting violence between states and the latter denoting violence by a state against its own citizens. Importantly, these categories become less distinct in real-world scenarios, as explored later.

II. TECHNOLOGY & STATE VIOLENCE

> "The merging of industry, technology and the means of waging war has been one of the most momentous features of processes of industrialization as a whole."
>
> - A. Giddens in *The Nation State and Violence* (1985, p. 3)

2.1. Evolution and Theory

States have a long history of violence. Even though technology is not a prerequisite for violence, it does enable a wide range of violent effects. Curiously, the kind of technologies that currently raise the most significant security concerns are also the ones that hold the greatest potential for benefiting humanity (Valeriano & Maness, 2015). These prospects and concerns stem from the inherent dual nature of the technological progress. As noted by defense policy analyst Andrew Krepinevich (1994), "[a]ll the military revolutions of the last two centuries are in a real sense spinoffs from the Industrial and Scientific Revolutions that have been central, defining processes of modern Western history". Nowadays, new technologies have the ability to generate widespread empowerment, enabling individuals and small groups to defy conventional sources of authority such as states and institutions. These tools have become increasingly affordable and accessible, transcending geographical and physical barriers. Consequently, they have ushered in a world characterized by a multitude of threats that can emerge from any individual, group, or state. In this new paradigm, every entity must consider the possibility that others, be they individuals, groups, or states, pose a potential security risk (*See* Beck, 2009; Wittes & Blum, 2016).

According to Herrera (2007), technological advances are not created exogenously to the international political system. In fact, their transformative features are not simple consequences of their material characteristics, but they are modeled by constrains and trends within the international arena. For instance, the railroad was introduced as a military tool, one that came to deeply alter the relationship between space and time, and it was key to the emergence of Germany as a war power (*Ibid.*). The invention of the atomic bomb, in its turn, entirely revolutionized the conflicts that followed, as the image of certain mutual destruction resulted in a reformulation of war doctrines and deterrence strategies. Likewise, cyber operations cannot be taken devoid of their international and historical contexts, as their evolution is connected to how future technologies will be leveraged and employed (Valeriano & Maness, 2015).

Whereas state violence can manifest itself in very distinct ways, it is instrumental by nature – to achieve political objectives (Arendt, 1970; Clausewitz's, 1832/1984). It should be noted, however, that the study of violent human conflict is largely fragmented across a wide range of different disciplines and subfields. Thus, as the various forms of political violence are not demarked analytically, similar or overlapping events can be approached simultaneously through different angles and conflicting methods. This fragmentation represents the main difficulty in the development of this research field (Chenoweth *et al.*, 2019). Consequently, political violence configures a multidimensional, remarkably vast, and ill-defined concept. Moreover, this field of study tends to set a strict division between periods of marked political violence and intervals of seeming peace, internally or internationally, even if these intervals are maintained by high-levels of state-initiated violence. This logic, in essence, ignores the fact that "diverse types of political violence coexist on a broad continuum, as fundamentally non-peaceful alternatives to each other" (*Ibid*., p 13).

Additionally, Wittes and Blum (2016) defend that military revolutions cover four basic elements: technological change, systems' development, operational innovation, and organizational adaptation. Nonetheless, the incorporation of technological change into political systems and structures is seldom analyzed by International Relations (IR) scholars (Herrera, 2007). Conversely, academics in the field of science and technology have demonstrated how new multifaceted means of state violence are emerging "due to intricate interplays between individual innovations, scientific breakthroughs, technological inventions, strategic paradigm shifts, and broader cultural waves" (Egloff & Shires, 2021, p. 130). Hence, "[a]s modern society leans ever more heavily on the Internet for commerce, communications and the management of its vital infrastructures, its fragility becomes an ever-greater concern" (Bowden, 2011). To McGraw (2013), "our reliance on these systems is a major factor making cyber war inevitable, even if we take into account (properly) narrow definitions of cyberwar. The cyber environment is target rich and easy to attack." (p. 109). As these authors highlighted, this growing interconnectivity that enhances efficiency and control, on the other hand, also facilitates new forms of crime, espionage, sabotage, terrorism, and warfare (Gartzke, 2016).

Importantly, history also demonstrates that societies take their time to normatively adjust and properly respond to major technological disruptions (Segal & Goldstein, 2022). Indeed, it took approximately three decades after the atomic bombs were used in Japan for the international community to draft jointly agreements on nuclear weapons. Therefore, norms and legal restrictions on cyber technology are bound to develop slowly, in a complex equilibrium between states' self-interests and international coordination (*Ibid.*). Nevertheless, even during the peak of the Cold War, the two sides of the conflict worked together to outline common basic rules and approaches.

The absence of effective regulations presents a tempting vector for both state and non-state actors seeking to cause disruptions or sow chaos on society. Most worryingly, the cover of anonymity, characteristic of cyberspace's structure, enables perpetrators to hide behind a high degree of deniability to evade considerable consequences (Lupovici, 2016; Polard *et al.*, 2018; Canetti *et al.,* 2023). As Hadji-Janev and Aleksoski (2013) warned, the proliferation of cyberattacks in number and scale makes it a plausible scenario that a major cyberattack may one day cripple the critical infrastructure of a state, in a manner similar to that of a mass destruction attack. Still, over the last decades, the majority of OCOs constituted attacks that, whilst violating the national sovereignty of states, systematically remained below the threshold of a conventional armed attack (and so, were met with virtually no reprisals). Consequently, many contend that future cyberattacks will mainly be used for political advantage, espionage, and international statecraft, with the most harmful attacks leading to the slow degradation the society's confidence in social, political, and economic institutions (Polard *et al.*, 2018).

Critically, the concept of 'use of force' should not be equated with violence. Nonetheless, numerous legal experts have attempted to examine whether a cyberattack can be correlated with this legal term – i.e., equal to an "act of aggression"[15] (Sleat, 2017; Gorwa & Smeets, 2019). Likewise, while most studies on OCCs highlight their (de)escalatory potential, they fail to comprehend that those dynamics do not directly lead to a decrease in violence (Egloff & Shires, 2022). Central to this question lies the apparent lack of a suitable definition of violence, particularly one that is not constrained to pre-digital, somatic conceptions of harm. On this topic, Brantly (2017) asserted that, like black powder that once amplified the projectile's lethal range, "an increasingly pervasive substrate of cyberspace will expand the lethal potential of hacking for violent ends" (p. 88). With the exponential growth in scale and scope of cyberattacks in recent years, questions whether cyber incidents could raise to the legal threshold of an 'armed attack' (for the purpose of Article 51 of the Additional Protocol I to the Geneva Conventions) have continuously puzzled researchers.

2.2. Just War Theory and Cyber Violence

Generally, traditional definitions resume the concept of 'violence' to the "behavior involving physical force intended to hurt, damage, or kill someone or something" (Oxford University Press, 2002). The display of violence in the largest scale is war – a state of

[15] UN General Assembly Resolution 3314, Definition of Aggression, A/RES/3314 (14 December 1974), article 1 states that: "Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition".

"armed fighting between two or more countries or groups" (Cambridge University Press, n.d.). In Clausewitz's (1832/1984) famous remark: "war is simply the continuation of policy with other means" (p. 28). Nonetheless, while states have constantly turned to sublethal harms to undermine rivals, technological developments have boosted the usage and efficacy of these methods, especially when applied against open societies (Barret, 2017). In the last decades, nation-states have been refining their methods of inflicting harm on adversaries, in a race to adjust to the new digital era. Consequently, cyber threats have claimed a prominent role in states' most acute security concerns. Similar to physical violence, cyber violence protracted by state actors has a clear instrumental value and it can constitute both kinetic and non-kinetic, threatened and applied forms of violence (Brantly, 2017).

The semantic conception of violence as a (mostly) physical concern is, of course, historically relevant. Nevertheless, moving into the new digital age has crippled its utility when understanding and explaining new events and conducts. Thus, even though this concept is deeply rooted in historical phenomena and theories, it's time it evolves accordingly to meet the new paradigm. As Brantly (2017) explains: "[cyberspace] is violent both in its ability to affect physical violence through first, second and third order effects, but also in its ability violently alter the reality of the world in which we exist in the present" (p. 75). So, to grasp the complexity it entails, one must analyze the violence incorporated into hacking, the emerging of offensive cyber teams throughout the world, and the society's evolution towards a "consensual hallucination"[16] in which our lives progressively depend on (*Ibid., See* Gibson, 2013). This, in turn, opens a new basis for comprehending a wide range of normative and political concepts in relation to the cyber world.

In his article entitled "Just Cyber War?: *Casus belli*, information ethics, and the human perspective", Matt Sleat (2017) constructed an interesting argument surrounding information ethics and the Just War Theory (JWT). The main questions addressed by him are twofold: (i) whether a cyberattack can constitute an actual *casus belli*[17]; and (ii) if the just war doctrine still offers a suitable foundation to ethically examine issues raised by cyberattacks. Centrally, whilst the just war theory is concerned with violent acts in the physical realm against human entities, cyberattacks are mainly conceived as non-violent acts committed in the cyber domain against

[16] In the words of William Gibson (2013), cyberspace depicts a "consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts … A graphical representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters, and constellations of data. Like city lights, receding".

[17] This term represents "[a]n act or situation provoking or justifying war. The phrase is Latin, and comes from *casus* 'case', and *belli* 'of war'" (Oxford University Press, 2006). It is covered by the *jus ad bellum* doctrine.

non-physical entities (e.g., computer software, virtual assets, or databases) (*Ibid.*). Contrarily to skeptical theorists like Arquilla (1999), who believe that the event of cyberwar leaves "just war theory in tatters" (p. 394), Sleat (2017) explains that the digital era does not render the JWT entirely obsolete. Accordingly, he sets out to prove that, off those ontological conceptions that are found unadaptable with this doctrine – i.e., their *non-physicality*, their *non-human* targets, their *non-violent* nature – only the latter presents a substantial theoretical challenge (*Ibid.*, emphasis in original). To counter this difficulty, the author conceptualizes the types of harm provoked by cyber operations in the sense of those affecting "vital human interests through degrading the functionality of computer systems necessary to a country's critical infrastructure" (*Ibid.*, p. 6).

Interestingly, Egloff and Shires (2022) conceive of violence in a similar manner to Sleat's conception of 'aggressivity'. In fact, the latter recognizes that the main struggle arises from assessing whether a cyberattack can be deemed aggressive or not. So, while Sleat (2017) does not define aggressivity, this scholar does compare the (non-physically) aggressive potential of a cyberattack with that of a chemical weapon – which he renders very aggressive in nature. It follows that, in order to evaluate the degree of aggressivity present (or not) in a cyber incident, it is necessary to examine the exact extend of the perpetrated harm, which is deeply rooted in perceptions "about the nature and relative importance of a large and complex set of specifically human needs, interests, values and purposes" (*Ibid.*, p. 19). In this regard, the author seems to lean closer towards Egloff and Shires' (2023) concept of "areas of human value".

Finally, while Sleat (2017) believes that it is unlikely that a cyberattack may constitute a just cause for war in the future, he does concede that it can lead to harmful effects equivalent to the kind of violence that JWT refers to. Indeed, he contends that nowadays' cyberattacks can be seen as potentially aggressive (or violent) "in morally significant ways" (p. 26). What Sleat means by that, however, is not explicit. Still, it is clear that the violence/aggressiveness of a cyberattack lies within the extent of the disruption, particularly in how much it negatively impacts the vital interests of citizens, whether directly or indirectly. These considerations will, afterwards, inform whether a computer network attack constitutes a *casus belli* in its own right (*Ibid.*). Nevertheless, in line with authors like Valeriano and Maness (2015), this scholar maintains that the global security landscape is characterized today by a series of "low level cyber skirmishes between states" (Sleat, 2017, p. 34).

Fundamentally, 'cyber violence' definitions are part of larger theoretical debates on the expansion of words beyond their core definitions (Brantly, 2017). There are, of course, risks associated with this conceptual expansion. For one, the extension of the concept of violence beyond physical harm may lead to the dilution of the analytical focus on the (already too fragmented) political violence field, as Chenoweth *et al*. (2019) argued. Moreover, if generally adopted, this expanded concept could potentially be manipulated for ideological or political purposes. For instance, a repressive regime could refer to this definition to justify harsher (and unproportional) countermeasures against the opposition's digital campaign, claiming that it is undermining national unity (Egloff and Shires, 2021).[18]

In addition, if this notion were to alter the *jus ad bellum* doctrine, more specifically, the definition of 'armed attack', there could be an increase of OCOs being deemed as use of force in comparison to the old criteria (*Ibid*.). Nonetheless, as Egloff as Shires (2021) pointed out: "although an expanded definition of violence implies more sub-threshold activity is violent (and potentially a use of force), it is highly unlikely to move the threshold itself" (p. 146). Likewise, the *jus in bello* doctrine – or International Humanitarian Law (IHL) – could benefit from an expanded conception that comprehensively addresses the full spectrum of harmful consequences of cyberattacks. In this topic, the ICRC asserts that "an operation designed to disable a computer or a computer network during an armed conflict constitutes an attack as defined in IHL whether or not the object is disabled through destruction or in any other way" (Gisel *et al*., 2020, p. 313) Alternatively, according to a limited interpretation, non-destructive operations that were harmful in a logical sense would still fall outside the scope of the law.

In conclusion, while some scholars have attempted to adapt conventional concepts to the cyber sphere, I confirmed that most (traditional) definitions of state violence fail to account for a variety of (non-physical) harms. By limiting this study to the physical realm, we tend to overlook effects associated with a wide array of manifestations of political violence. In the same tone, ICRC experts claim that adopting an expanded definition of violence "constitutes one of the most critical debates for the protection of civilians against the effects of cyber operations" (Gisel *et al*., 2020, p. 314). Indeed, technology and digital weapons enable not only international actors to reach their tactical and strategical goals, but also to profoundly impair the lives of individuals and communities around the world with apparent impunity. In this regard, recent studies denote that instances of acute psychological harm and extensive community repression can, in certain cases, be just as damaging as physical violence acts (Woodlock *et al*. 2019; Egloff and Shires, 2022; Shandler *et al*., 2023).

[18] Still, states' justifications for the use of violence fall beyond the scope of this dissertation.

2.3. The Psychology of Cyber Terror

Similar to violence, harm is a concept that has been extensively studied in a variety of research fields, from philosophy to psychology, politics or law. Oversimplified definitions of harm generally revolve around damage, injury, or hurt of some kind (*See* Last, 2007). Additionally, it often entails connotations of permanence, which are rather easily discarded in the cyber world. Nonetheless, this concept has received substantially less theoretical attention in the area of cybersecurity (Agrafiotis *et al*., 2018; *See* Gorwa & Smeets, 2019). Ominously, as a growing number of cyber threats continues to challenge the current security landscape, their harmful effects remain somewhat unclear or understudied. As a matter of fact, during my research, I came across a staggering lack of metrics, frameworks, and empirical studies examining the broader impacts of malicious cyberattacks on people and communities alike.

Few academics have attempted to overthrow the notion that cyberattacks are mostly harmless irritants, or just a threat to information security (Gartzke & Lindsay, 2015). Relevantly, Shandler *et al*. (2023) set out to prove that apparently insignificant cyberattacks can entail considerable damage by "traumatizing civilians, triggering profound psychological harm, undermining human security, and exacerbating cycles of violence." (p. 2). In this sense, measuring the severity of cyberattacks by applying the metric of psychological stress is aligned with the argument that even non-physically damaging cyber interactions can be deemed violent. It follows that, whilst first-order outcomes – like system disruption and degradation, access denial, or data theft – are still worrying, the sole focus on visible or direct impacts conceals more insidious (long-term) psychological or societal effects (*Ibid*.). To illustrate this view, Shandler *et al*. (2023) explain that regarding a ransomware attack on a hospital network as ineffective, due to the lack of physical damage resulting from the attack, fails to account for the great psychological distress it likely prompted in its victims.

Foremost, these authors claim that the cumulative weigh of trivial individual cyberattacks can eventually pose a massive toll on society (*Ibid*.). It may be true that, thus far, the most prominent cyberattacks have failed to measure up to the 'doomsday prophecies' of the alarmist rhetoric. Yet, in recent times, we have registered a proficient decline of confidence in public authorities and their capacity to protect people from these novel threats (Shandler & Gomez, 2022). Notably, Beck (2009) labeled it the new "era of insecurity", in which our manufactured uncertainties – risks spurred from the economic and technological progress of the last decades

– are not only intangible to our senses (i.e., incalculable) but also fundamentally inescapable.[19] Consequently, our perceived vulnerability to cyber harms, also reflected in increasingly high levels of anxiety across the world, induces citizens and companies to pressure governments, demanding sticker cybersecurity laws often at the expense of their privacy and civil rights.

Furthermore, Shandler *et al.* (2023) suggested that the sum of characteristics of cyberspace – i.e., "complexity, universal interconnectivity, and attributional ambiguity" – seem to worsen the emotional effects experienced by cyberattack victims (p. 5). Indeed, the immensely complex nature of the cyber sphere can be associated with overall confusion and uncertainty, consequently triggering emotions like fear, powerlessness, and anxiety in the public (McDermott, 2019). New research also demonstrates how people with limited digital knowledge reveal amplified dread[20] when faced with a cyberattack (Gomez & Villar, 2018). Moreover, the pervasive and borderless nature of digital interconnectivity opens the way for malicious cyber incursions into peoples' lives and privacy. A cyber intrusion could be carried out by anyone from anywhere in the world and the attacker can effectively hide behind the cover of online anonymity. Accordingly, it is a particularly difficult task to uncover the identity of a cyber offender (*See* Kello, 2013; Nye, 2017). This uncertainty, once again, only heightens the victims' threat perception[21], thus contributing to the deterioration of individual and collective security.

Significantly, their research study has shown that both cyber violence and conventional violence can lead to the same elevated level of psychological distress (Shandler *et al.*, 2023). Here, psychological distress – the dependent variable – comprises a sum of emotions, such as anger, anxiety, and threat perception. It is worth noting that psychological distress has been often linked with proneness to negative behaviors like alcohol or substances' abuse, impoverishment, and depression (*See* Schiff *et al.*, 2006). Appropriately, this research work consisted of an internal meta-analysis that combined an extensive array of surveys and studies made in this still insipient literature. Some of these simulated realistic exposure to both traditional and cyber violence committed by unknown attackers. In this regard, their conclusion is particularly remarkable, as it demonstrated that the psychological trauma and severe stress

[19] In his conception of 'Risk Society', in accordance to Beck, Pathe Duarte (2015) refers to the growing environmental, social, political, and economical risks that evade the control and anticipation of today's societies, being that part of the uncertainty and of the impossibility of control are essential characteristics of today's world (p. 452).

[20] 'Dread' is defined by the authors as "the apprehension of the negative consequences of an uncertain activity" or of an impending catastrophe (Gomez & Villar, 2018, p. 64).

[21]'Threat perception' is defined as "the cognitive appraisal of the danger posed by a class of threat" (Shandler *et al.*, 2023, p. 8).

caused by kinetic acts of political violence can be compared to the level of distress triggered by crippling cyberattacks (Shandler *et al*., 2023).

In another study on cyberpsychology, Gross *et al*. (2016) reasoned that, depending on the identity of the victims and the attackers, the psychological consequences of cyberattacks could rival those of traditional terrorism. Although there is no current consensual definition of terrorism – and such discussion lays beyond the scope of this research work – it is widely accepted that it reflects deliberated and premeditated acts of violence intended to instill extreme fear and terrorize the population beyond the immediate victims of the attacks (Blakeley, 2012). There has been considerable opposition within the field of IR to the idea that states can also commit terrorist acts, despite the fact that the majority of state violence aims to generate terror and leads to significantly higher casualties when compared to non-state terrorism (Gross *et al*., 2016). In essence, this distinction is founded on realist theories on the historical creation of states and the Weberian monopoly on the legitimate use of force (*See* Weber, 1919/2015). Accordingly, Denning (2007) defended that, "to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear". Notwithstanding the lack of physical consequences so far, cyberterrorism[22] has developed the potential to cause similar (lethal) consequences to those of conventional terrorism (*See Ibid*.).

In line with the previous results, Gross *et al*. (2016) and Backhaus *et al*. (2020) observed that, even though no casualties or physical injuries were involved, acts of cyber terror can mirror kinetic forms in the anxiety, fear, panic, anger, and the extreme conducts they incite in the population. Certainly, physical destruction is not the main goal of terrorism, but the feelings and behaviors it generates on a wider audience. Still, whereas most studies focus on the dangers that cyberterrorism poses to critical infrastructures and national security, their impacts on human security remain vaguely studied (*Ibid*.). According to Tadjbakhsh (2014), 'human security' highlights the required conditions for a dynamic and thriving civil society. It means that people should be able to live free from a climate of constant fear and insecurity. This is an essential condition for society to develop a prosperous public speech and free information flow, democratic institutions, and respect for human rights (Gross *et al*., 2016). Ultimately, it is possible to trace a parallel between high levels of psychological anguish and dramatic shifts in public opinion, political radicalization, and possible military escalation (Shandler *et al*., 2023).

[22] This concept refers to "the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear" (Denning, 2007, p. viii).

In a 2021 survey from Gallup, cyber threats (specifically, cyberterrorism) were rated by the American public as the most serious menace faced by the country (Brenan, 2021). Remarkably, this perception surpassed concerns about Russian belligerence, the COVID-19 pandemic, or Iran's nuclear weapons program. These results steadily demonstrate a pervasive sense of threat and fear regarding cyberattacks, with respondents ranking them as equally or more terrifying than international terrorism, global pandemics, militarism, proliferation of nuclear weapons, and other threats. In fact, this growing fear surrounding cyber threats has remained consistent across multiple years of survey data (Shandler *et al.*, 2023). Another report uncovered that 65% of all Estonians reckon cyber incidents to be the biggest threat to their nation, and 55% regard foreign interference as a threat to the country's sovereignty (Saar Poll, 2013, p. 4). Most analysts advocate that, albeit the 2007 DDoS attacks paralyzed Estonia's government services and brought the country to the edge of its nerves, they did little to cripple Estonia in any serious or long-lasting sense. Yet, as these numbers suggest, the psychological impact following this large-scale attack is visible, specifically due to the high sense of vulnerability it incited on the population.

Finally, these results raise substantial questions concerning their vast legal, ethical, and security implications. Recognizing the potential for cyberattacks to cause widespread chaos and long-lasting repercussions, regardless of whether they result in direct physical harm to essential infrastructure, calls for a reassessment of our approaches to comprehend and address these dangers. Crucially, physical destruction does not represent the only factor concerning legal harm. The creators of the Tallinn Manual also contended that serious injuries may be completely psychological, thus it's "[r]easonable to extend the definition [of attack] to serious illness and severe mental suffering that are tantamount to injury. In particular, note that Article 51(2) of Additional Protocol I (1977) prohibits 'acts or threats of violence the primary purpose of which is to spread terror among the civilian population'. Since terror is a psychological condition resulting in mental suffering, inclusion of such suffering in this Rule [defining a cyber-attack] is supportable through analogy" (Schmitt, 2013, p. 108).

Likewise, the International Committee of the Red Cross (ICRC) highlights the importance of considering severe mental suffering in assessing the proportionality of harm caused by conflicts. In this sense, these experts argue that psychological injuries, such as post-traumatic stress disorder (PTSD), have significant and long-term impacts on individuals and, thereby, should be considered when evaluating incidental harm in conflicts (*See* Gisel, 2018). In this sense, Shandler *et al.* (2023) maintain that this perspective should also be applied to cyberwarfare, where the question of whether a cyberattack has caused enough psychological harm to warrant an armed response arise. However, defining and measuring severe mental suffering presents legal and empirical challenges, as its effects might manifest over long periods of time. In addition, they often require sophisticated diagnostic techniques mostly inaccessible in conflict or oppression scenarios (*Ibid.*).

Quantifying these terms in IHL has proven to be particularly difficult, as attempts to introduce concrete criteria have faced significant resistance (*Ibid.*). Nonetheless, acknowledging the levels of psychological harm caused by OCOs is long overdue. While the Tallinn Manual suggests that inconvenience, stress, or fear do not qualify as collateral damage, it fails to present any empirical data to support this assertion (Gisel, 2018).[23] In contrast, some experts argue that serious mental injury, even if it falls short of PTSD, can still cause significant, long-lasting harm to individuals and society as a whole (*Ibid.*). Critically, these research studies provide evidence that cyberattacks can cause severe psychological distress comparable to conventional attacks. What is more, this conclusion aligns with the evolving understanding that state terrorism can undermine civil society by exploiting fear, sowing insecurity, and cementing distrust.

Notwithstanding the emergence of ever more innovative exploitation tactics of the global information infrastructure, some experts believe that there are also strong deterrence forces at play in the cyber domain, which effectively limit the intensity of that exploitation (Gartzke, 2013; Valeriano & Maness, 2015). Hence, I turn to the question: do these strong deterrence forces actively limit the level of harm provoked by offensive cyber operations?; or do they still cause extensive harm to individuals and communities worldwide? That being said, I will now focus on the theoretical reviewing of cyber conflict literature, followed by an analysis of prominent interstate cyberattacks in modern history – the cyberattacks in Georgia in 2008 and the NotPetya attack in 2017. As established *supra*, my examination will be informed by the conceptual grounding and model of analysis laid out by Florian J. Egloff and James Shires.

[23] The Tallinn Manual states that in contrast to PTSD, "inconvenience, irritation, stress or fear … or a decline in civilian morale" do not qualify as collateral damage (Schmitt, 2013, p. 160). In its turn, ICRC experts hold that "inconvenience, stress or fear incidentally caused by attacks are not relevant for an assessment under the principle of proportionality" (Gisel, 2018, p. 35).

III. OCCs & INTERSTATE VIOLENCE

> "Cyberwarfare is far more than a mere instrumental thing, comparable to, say, 'gun warfare', or 'tank warfare'. It is closer to things like 'psychwarfare', or even 'armed combat'. Perhaps mostly, it is much like 'insurrectionary war'."
>
> - A. Marques Guedes (2010a, p. 828)

3.1. Theories of Cyber Conflict

According to Joseph S. Nye (2011b), cyber conflict comprises three areas: governments, organizations, and individuals. The central focus of this assessment, in terms of perpetrator agents, is on government-to-government cyber combat. As established *supra*, the current consensus is that cyberattacks have the effect of reducing political violence, as they enable states, groups, and individuals to engage in forms of aggression that fall short of full-fledged war (*See* Rid, 2013). By employing weaponized computer code and computer-based operations, targeted attacks can be carried out on an adversary's technical systems without directly causing physical harm to people or casualties. Accordingly, these informational means of fighting, contrasting with traditional forms of warfare, don't systematically put soldiers' and civilians' lives at risk (Vijaykumar, 2021).

To Smeets (2018), "unlike weapons of mass destruction, cyber weapons are an integral part of the commander's arsenal in conducting force-on-force and asymmetric warfare and will be used in concert with kinetic weapons to soften up the adversary's defenses" (p. 98). This notion is in line with Demchak's (2011) concept of "cybered conflict" – i.e., a conventional conflict that includes (but it's not confined to) OCOs. Still, in a rare quantitative examination of the relationship between (physically) violent conflicts and offensive cyber operations, Kostyuk and Zhukov (2017) uncovered that such operations have a rather superficial influence on battlefield dynamics. These authors, of course, relied on a narrow and simplistic definition of violence.

In 2011, the United States proclaimed that a cyberattack can be equated to an act of war, thereby punishable by conventional military force (The White House, 2011). The Tallinn Manual later instituted that "a cyber operation that seriously injures or kills a number of people or that causes significant damage to, or destruction of, property would satisfy the scale and effect requirements [of armed attacks]" (Schmitt, 2017, p. 341). These declarations represented a defining moment that introduced a new direction in the interpretation of cyber incidents in the international arena (Valeriano & Maness, 2015). Controversially, the former asserted that even non-kinetic attacks or threats to the US national security could be responded to by physical counterattacks.

With both domains increasingly merging, Clarke and Knake (2010) predicted a fundamental change in international relations and, ultimately, in the global power balance. Now, this perspective appears to be in line with the abovementioned doctrine of "cyber-hype". Given their potential for global disturbance and escalatory effects, according to alarmists, "[c]yberwar may actually increase the likelihood of the more traditional combat with explosives, bullets and missiles" (*Ibid.*, p. 32). Hence, as of now, many believe that cyber conflict exists in a difficult equilibrium, in a 'gray area' between peace and war, which can tilt and escalate at any moment (Nye, 2016; Smeets, 2018; Sanger, 2018).

Valeriano and Maness (2015) sought to counter this prediction with empirical research. They contend that old realist paradigms, like those developed by Machiavelli and Hobbs, centered on power politics and deterrence strategies are ill-applied to emergent technology and cyber interactions. In their book called *Cyber War Versus Cyber Realities*, the authors refute the idea that cyber weapons are revolutionizing the system, thereby reasoning that cyber conflicts will most likely remain scarce, low-level, and of limited effects in the foreseeing future. This is because cyber interactions do not immediately correlate with power, technology, or resources. Instead, they take part in a broader function in active foreign policy disputes, where low-severity cyber clashes represent standard relations between states (*Ibid.*). Importantly, in their research, the authors uncovered that traditional security dynamics – threat articulation, channeled response, and subsequent escalation by the opponent – are not so easily discernible in the cyber realm (neither deterrence nor compellence)[24] (*Ibid.*).

In turn, these researchers concluded that the cyber domain displays distinctive dynamics. The underlying normative system has limited escalatory reactions by establishing restraining forces of its own.[25] Accordingly, Valeriano and Maness' (2015) theory of cyber restrain rests on four processes: (i) the nature of the cyberweapon and its reproducibility; (ii) the blowback potential; (iii) the potential for collateral damage in the cyber sphere; (iv) the potential for causing harm to civilians (pp. 4-5). These factors help explain why debilitating cyberattacks on states' critical assets will remain relatively rare or absent in the future. Foremost, the high potential for civilian harm, the uncertain nature of these weapons, the possible collateral

[24] In line with Cioffi-Revilla (2009), "compellence is therefore about inducing behavior that has not yet manifested, whereas deterrence is about preventing some undesirable future behavior" (p. 126).

[25] Critically, 'cyber restrain' is not to be confused with 'cyber deterrence'. Cyber restraint is, accordingly, a form of operations derived from the deterrence theory but not dependent on it (Valeriano & Maness, 2015).

damage, and predictable weak payoffs appear to be holding back escalatory threats (Gartzke, 2013). Centrally, the lack of an operational script for states to follow in such a scenario discourages offensive actions and pushbacks, particularly given their ability to trigger disproportionate consequences (Valeriano & Maness, 2015). Besides, the majority of states doesn't possess the means to effectively launch massive devastating operations on their rivals.

Critically, these authors assert that the concept of cyber deterrence is essentially faulty, as it misapplies a logical system constructed in one area (nuclear) to an entirely different realm (cyber). The uncertainty and uncontrollability surrounding the use of cyberweapons make it a generally impracticable option for states to retaliate. Moreover, for a cyber operation to be credible (a central feature of the deterrence theory), the national cyber capabilities must be made public, which is also unreasonable in this milieu (*Ibid.*). Additionally, a display of power or brute force is counterproductive in this regard, not only considering states' interest in keeping the full extent of their capabilities confidential, but also given that further (unpredictable) escalation could happen. Consequently, a simple cost-benefit calculous foresees a restrictive and careful tendency in the employment of OCOs in the near future (*Ibid.*). Indeed, even though certain cyberweapons could potentially threaten to cause catastrophic reverberations, the majority of cyber tactics and interactions has so far been constrained to targeted espionage or deception campaigns, aimed at exploiting or exposing some vulnerability in the victim (Gartzke, 2013).

Another important argument is the evidence of regionalism in contemporary cyber disputes, which is presented as counterintuitive due to the borderless nature of cyberspace (Valeriano & Maness, 2015). These scholars found that cyber capabilities are most often used for regional interactions, thus defying the notion that this domain is inherently global and so detached from states' physical constrains. Notwithstanding the high probability for a cyber conflict to become global, this is not forcefully the case most often (*Ibid.*). Now, this contradicts the assumption that "there are no geographic limits" in cyberspace (Singer & Friedman, 2014, p. 73). Instead, the local character of most OCOs relates to states' regional clashes. Therefore, simple power projection doesn't justify cyber interactions, since there are other regional dynamics in motion. Indeed, cyber operations cannot be analyzed devoid of their historical contexts. The exceptions are the hegemonic powers, against which cyber campaigns are unleashed beyond territorial matters (Valeriano & Maness, 2015).

Unlike the nuclear deterrence theory, cyber deterrence appears to feature not an attempt to avert a single catastrophic event, but a sequence of efforts to shape behaviors along a range of potential attacks (Nye, 2016). Importantly, Maurer (2018) reasoned that the "threshold is lower for hacking than for most conventional military capabilities" (p. 9). As OCOs introduce more uncertainty and volatility into the system, this perfect forum for low-level, widespread, and (particularly) psychological threats directed at enemy populations becomes ever more unstable. In this regard, "even if there is no act of cyber war in a strict sense, many cyber-attacks that have happened might be regarded as quasi-cyber war" (Jianqun, & Longdi, 2014, p. 11). Here, it is worth mentioning that the use of proxies is a recurrent practice, particularly in this 'gray zone' of quasi-war. Due to the principle of plausible deniability, using proxies to project coercive power through cyberspace figures as a relatively attractive option for states. Essentially, this is because technology enables new coercive effects below the threshold of the use of force (Nye, 2016; Maurer, 2018).

3.2. States and Cyber Proxies

Throughout history, states have turned to proxies to wield power and conduct their illicit activities. In truth, the emergence and legitimatization of the modern nation-state itself is linked to its established authority and control over coercive capabilities, including those carried out by proxies, militias, or private contractors (*See* Weber, 1919/2015). Presently, however, numerous states could be more accurately described as intermediaries than as dominant actors with full control over their national security (Bobbitt, 2003). In recent decades, the concept of 'nation-state' is continuously transforming into what has been referred to as "market-state", characterized by a growing trend of privatization that is both widespread and systematic (*Ibid.*). The perceived lack of cyber knowledge and effective capacity within governments worldwide is contributing to the growing reliance on external entities. In reality, many countries are expanding their internal and external security approaches to utilize non-state actors as a means to exert coercive influence in the realm of cyberspace (*Ibid.*).

The author of the book *Cyber Mercenaries*, asserted that "[t]he Internet enables a new spectrum of harmful effects that, in turn, introduce a new set of escalatory dynamics" (Maurer, 2018, p. 154). This escalatory risk is, in part, associated with the uncertainty of the forces at play and the attribution problems in this domain, but also with the unintentional impacts of the use of proxies. Schelling (2008) addressed this diffusion of risk and graduate erosion of control as "salami tactics" [26] (p. 66). According to the political scientist Branislav L. Slantchev (2005),

[26] To illustrate this tactic, the author describes the following situation: "Tell a child not to go in the water and he'll sit on the bank and submerge his bare feet; he is not yet "in" the water. Acquiesce, and he'll stand up; no more of him is in the water than before. Think it over, and he'll start wading, not going any deeper; take a moment to decide whether this is different, and he'll go a little deeper, arguing that since he goes back and forth it all averages out. Pretty soon we are calling to him not to swim out of sight, wondering whatever happened to all our discipline" (Schelling, 2008, pp. 66–67).

this concept configures "a strategy that takes steps that are small enough not to activate the threatened action, yet that bring the player closer to his goal" (p. 4). Consequently, as discussed above, states have a shared self-interest in managing their proxy relationships tightly (*See* Valeriano & Maness, 2015). Still, lessons taken from this current activity suggest that, in practice, state actors can never fully control or influence proxy relationships (Maurer, 2018).

Even though proxy relationships vary across regions and states, according to Maurer (2018), the majority falls within three categories: delegation, orchestration, and sanctioning. In brief, the delegation type refers to a relationship purely governed by contracts, in which the state agent delegates authority to a non-state actor to act on its behalf (e.g., private contractors, mercenaries, etc.). Orchestration, in its turn, describes the act of engaging intermediary actors voluntarily by offering them ideational and material assistance, thus using their involvement to address target actors and achieve specific political objectives. Hence, orchestration differs from delegation due to the correlation of ideological interests between intermediary and orchestrator, hereby fundamental to the affiliation (*See* Abbott *et al*., 2015).[27] In other words, while delegation is essentially hierarchical and can be translated into "state-sponsored" (which implies more control), orchestration involves network relationships and "state-supporting" activities below the threshold of effective control, such as funding, weapons supplying, or sharing intelligence (Maurer, 2018, pp. 45-46).

Finally, sanctioning draws on the concept of 'passive support', as found in counterterrorism scholarship. In this sense, the state demonstrates passive support for a non-state actor when it consciously decides to allow the actor's actions to continue against a third party, even though it possesses the capability to intervene (*See* Byman, 2012).[28] This permission or tolerance can also take the form of posterior endorsement, for instance, by sheltering the proxy from subsequent prosecution. According to this scholar, a state may turn "a blind eye" over the agents' illicit actions for a number of reasons, like general domestic support, the unthreatening nature of the proxy, the low cost of inaction, the inability to act, or indirect gains for the state (*Ibid.*). Following this reasoning, the cyberattacks on Estonia in 2007 reveal an instance of at least passive support from the Russian state to non-state actors.

According to Maurer (2018), countries of the former Soviet Union pose the best examples for the nature and evolution of cyber proxies, in particular, in sanctioning relationships. After the collapse of the USSR and the ensuing institutional and financial meltdown, corrupt state

[27] This author widened and adapted Abbott *et al.*'s (2015) definition of 'orchestration' to cyber proxy relationships.
[28] The author concedes that his definition is built on Daniel Byman's book *Passive Sponsors of Terrorism* (*See* Byman, 2012).

agents had the incentives to recruit those who possessed the technical skills to successfully carry out cyber heists. Security and intelligence agencies have also become interested in the newfound opportunities presented by OCCs. Hence, this convergence of economic difficulties, limited accountability, and substantial rewards has fostered an environment where malicious activities were allowed with minimal controls (*Ibid.*). In reality, the state's tolerance of cybercriminal activities fuses with individuals' exploitation of their own positions within the state for personal benefits in complex a myriad of ways (*Ibid.*). Essentially, forming a proxy relationship configures a way to escape detention and legal repercussions. As Oleg Gordievsky, a former KGB officer, revealed "[t]here are organised groups of hackers tied to the FSB and pro-Chechen sites have been hacked into by such groups... One man I know, who was caught committing a cybercrime, was given the choice of either prison or cooperation with the FSB and he went along" (Alvey, 2001, pp. 52-53).

Finally, in today's state-centric international system, cyber proxies hold a vital importance in the conduction of malicious cyber activity. In basic terms, such relationships are established in countries worldwide due to the abundance of non-state actors possessing capabilities that can be advantageous to the state. Whilst the configuration of proxy relationships may vary, these modalities – delegation, orchestration, sanctioning – play a crucial role in the conduct of offensive computer network operations. Overall, Maurer (2018) defends that the type of relationship is more important than the individual agents that comprise it, since the dynamics involved will invariably dictate the risk they pose to the system. Appropriately, this academic links the definition of cyber proxies to "offensive action", in what he reckons to be the direction of the discussions "about the future of war, whether war necessarily involves physical effects, and the meaning of violence and coercion" (*Ibid.*, p. 8).

Now, having reviewed relevant theories in cyber conflict scholarship, I will turn to the analysis of the selected case studies. To recapitulate, I set out to examine paradigm-shifting cases in modern state disputes through the lenses of the broad conception of violence, to evaluate whether these cases constitute violent uses of OCCs. To do so, I will utilize the CCDCOE database (particularly, the interactive cyber law toolkit), together with the Council on Foreign Affairs (CFA) database (the Cyber Operations tracker) and review the related material. Pertinently, I will assess news articles, official reports, and case studies, so as to draw a holistic picture of these offensive cyber operations. I will focus on, *inter alia*, their innovative features, the methods deployed, the perpetrators' intent, the use of cyber proxies, the wider geopolitical context, and their main impacts (principally, those that resulted in harm towards the three areas of human value). Lastly, I will compare both definitions of violence in order to determine which is better suited to study the violent nature of these emerging weapons.

3.3. Case Studies:

3.3.1. Invasion of Georgia (2008)

On 7 August 2008, following years of ever-mounting tensions and belligerent provocations, Georgia initiated a large-scale military operation against the separatist region of South Ossetia, where Russian peacekeepers were stationed at the time. Moscow swiftly reacted by deploying the Russian Federal Army to both South Ossetia and Abkhazia (another pro-Russia separatist region in Georgia). Heavy fighting erupted as the Russian Air Force conducted airstrikes on Georgian positions and cities, leaving utter destruction and death in its wake. The Russian Navy enforced a blockade and landed naval infantry on the Abkhazian coast, thereby assuming control over Georgia's coastline on the Black Sea. In total, this conflict was prolonged for five days until a ceasefire was accorded, on August 12th, with mediation conducted by the former French President Nicolas Sarkozy and the EU. Centrally, this interstate war represented the first time in history that cyberwarfare was used as a tool in military action, thus embodying an important preview of this new form of hybrid warfare (Geers, 2008). Properly, I will focus my analysis on the cyber dimension of the Russo-Georgia war.

To contextualize, this conflict was the result of a much larger conjunction of geopolitical dynamics at play within the international system. After decades of suppression and mass terror, Georgia's conquered its independence from Russia in 1991. The transition to a post-soviet state contributed to the further alienation of the political-territorial entities of South Ossetia and Abkhazia, where fighting between Georgian and separatist forces (backed by Moscow) broke out between 1991-1992 and 1992-1994, respectively. These clashes ended with Georgia losing control over large parts of both territories and the subsequent implementation of ceasefires and peacekeeping responsibilities, accorded by the two leaders – Shevardnadze and Yeltsin – and supported by UN and OSCE missions.[29] Following the Rose Revolution, in 2003, tensions with Russia escalated again. Meanwhile, the election of Georgian President Saakashvili and his strong foreign policy turn towards the West coincided with the rise of President Vladimir Putin, Russia's renewed aggressiveness over its near-abroad, NATO's eastward enlargement, and the convergence of international interests in the Caucasus area, particularly associated with

[29] Russian forces undertook 14 peacekeeping responsibilities both in South Ossetia and later in Abkhazia. An agreement concluded in June 1992 in Sochi, between Eduard Shevardnadze and Boris Yeltsin, established the Joint Peacekeeping Forces (JPKF) for South Ossetia (Tagliavini, 2009).

energetic and security considerations (Tagliavini, 2009).[30] The sum of these factors created the perfect storm.

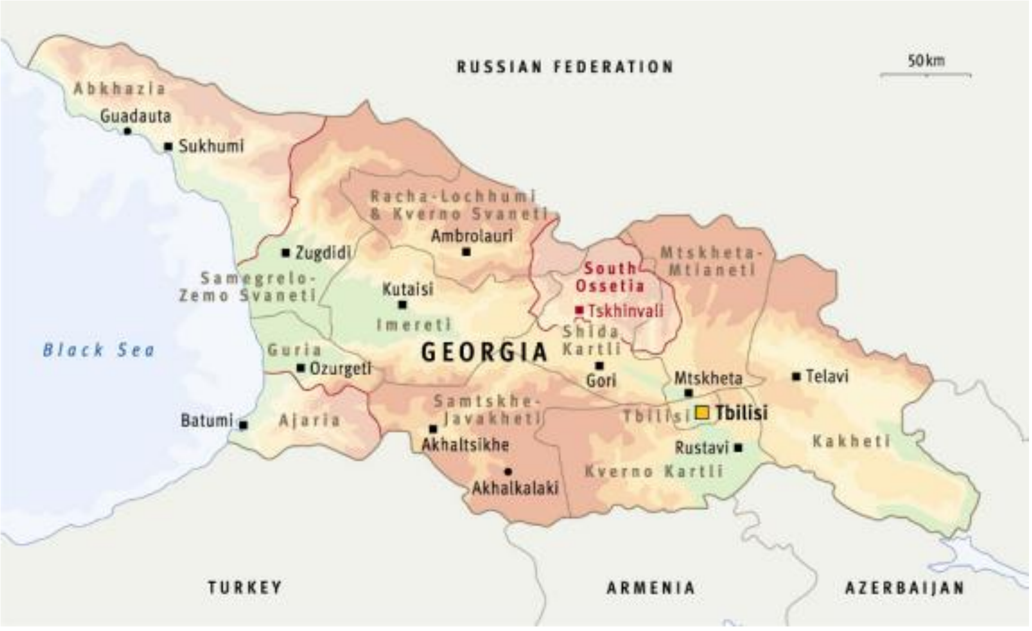


Figure 5: Map of Georgia (2009)

Source: Tagliavini (2009, p. 4).

In comparison to most conventional wars, this particular conflict was relatively small in scale, with limited involvement of military forces and a short duration period. Some might argue that it constituted a regular confrontation or campaign within a wider, long-term geopolitical cold war between the warring parties, characterized by intermittent outbursts of violence ranging from minor to major intensity (Hollis, 2011). Indeed, superficially, it appears to be solely one of many lasting 'cold wars' fought on the periphery of Russia, with occasional instances of formal military conflicts. Nevertheless, a closer examination of the cyber domain operations conducted by both sides reveals that this perception is somewhat deceptive and unfounded. Historically, the Russo-Georgian conflict can be regarded as a major precedent-setting event, as it established a new form of modern (hybrid) warfare and conveyed a set of important lessons for future conflicts of this kind (*Ibid.*; Carr, 2009; Marques Guedes, 2009).

[30] The Independent International Fact-Finding Mission on the Conflict in Georgia (IIFFMCG) was created by the Council Decision 2008/901/CFSP of 2 December 2008 concerning an independent international fact-finding mission on the conflict in Georgia, with a core team of three members led by Swiss Ambassador Heidi Tagliavini (*See* Tagliavini, 2009).

Firstly, as I referred to *supra*, this conflict represented the first case in history where an extensively prepared "swarm" attack on the cyber domain coincided with major combat actions in other domains of warfare (Marques Guedes, 2009, p.38).[31] According to Holsti (2011), Georgia was attacked in four fronts: land, sea, air, and cyberspace. As it appears, the network attack was premeditated, synchronized, and highly effective. A Georgian governmental update report from 10 November 2008 revealed that a "large number of Georgia's Internet servers were seized and placed under external control from late Thursday, 7 August, whereas Russia's invasion of Georgia officially commenced on Friday, 8 August. Also, much of Georgia's traffic and access was taken under unauthorized external control at the same time that this first large scale attack occurred" (Government of Georgia, 2008, p. 3). The targeted websites[32] were thoroughly selected, as if the intent was to hinder the communication and internal/external coordination capabilities of the Georgian state with its international allies (Marques Guedes, 2009).

Consequently, "as tanks and troops were crossing the border and bombers were flying sorties, Georgian citizens could not access web sites for information and instructions" (Oltsik, 2009). Hence, tactically, the employment of OCCs in this conflict seems to fall within the category of supportive measures, as they were used in tandem with kinetic means to improve the overall efficacy and power of the military assault. Significantly, more than a generalized DDoS attack on Georgian networks, investigators from *Project Grey Goose*[33] learned that the hackers "disabled the sites using a built-in feature of MySQL, a software suite widely used by Web sites to manage back-end databases" (Government of Georgia, 2008, p. 31). Accordingly, in the previous year, they had "posted online instructions for exploiting the 'benchmark' feature to inject millions of junk queries into a targeted database, such that the Web servers behind the site become so tied up with bogus instructions that they effectively cease to function" (*Ibid.*, emphasis in original). In general, the main methods involved website defacements, mass email spamming, and malicious payloads on Internet applications (SQL injections). As Jeffrey Carr

[31] In this regard, however, Marques Guedes (2009) alludes to Charles Billo and Welton Chang recount that "[i]n 2002, Chechen rebels claimed that two of their Web sites, kavkaz.org and chechenpress.com, crashed under hack attacks by the Russian FSB security service. The website crashes were reportedly timed to occur concurrently or shortly after Russian Special Forces troops stormed the Moscow Theater in which the rebels had taken hostages". (Billo & Chang, 2004).

[32] These included, *inter alia*, "the U.S. and U.K. Embassies in Tbilisi, Georgian Parliament, Georgian Supreme Court, Ministry of Foreign Affairs, various news agencies and other media resources, the Central Election Commission, and many others" (Government of Georgia, 2008, p. 5-6).

[33] *Project Grey Goose* consists of a volunteer open-source intelligence initiative comprised by more than 100 security experts from tech giants like Microsoft and Oracle, former members of the Defense Intelligence Agency, Lexis-Nexis, the Department of Homeland Security and defense contractor SAIC, among others. It was originally launched on August 22nd, 2008, to examine Russian cyberwar against Georgian websites.

(2009), one of *Project Grey Goose* members, explained, this method reflects “moderate technical sophistication, but more importantly, it shows planning, organization, targeted reconnaissance, and evolution of attacks” (p. 141).

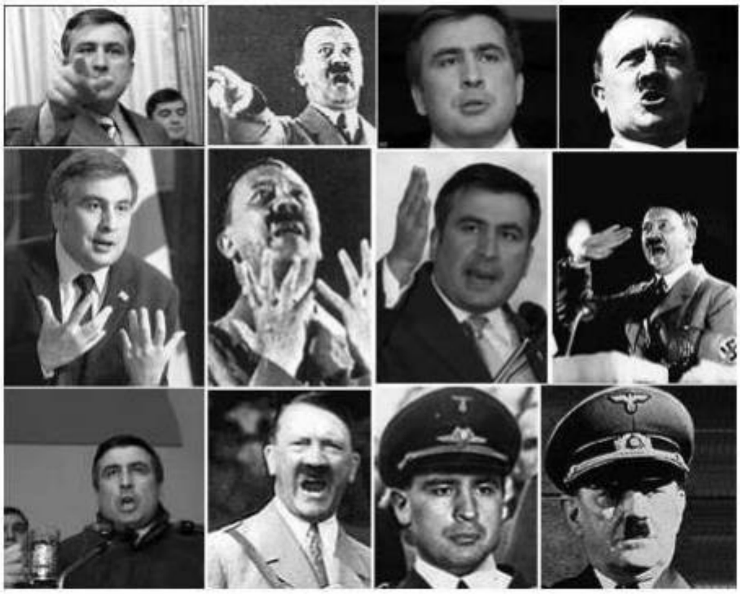


Figure 6: Screenshot of the defacement attack on President Mikheil Saakashvili's website

Source: Government of Georgia (2008, p. 4) [34]

Although no direct link was successfully established between the perpetrators and Russian governmental officials, the degree of premeditation and synchronization of the attacks denotes, at least, some tacit level of collaboration. According to these investigators, the Russian online forum where the cyberattacks were coordinated “appeared to have been prepped with target lists and details about Georgian Web site vulnerabilities well before the two countries engaged in a brief but deadly ground, sea and air war” (*Ibid.*, p. 30). In this sense, Carr contended that “the level of advance preparation and reconnaissance suggests that Russian hackers were given information for the assault by officials within the Russian government and or military” (*Ibid.*, p. 31). Indeed, numerous sources appoint the Russian Business Network (RBN), a Russian organized crime group operating then from St. Petersburg, as the central orchestrator behind the cyberattacks on Georgia in 2008 (*See Ibid.*, Popescu & Secrieru, 2018). This organization,

[34] Portraying the Georgian leader as Hitler not only demoralized the Georgian people but also served to rally support among Russians for attacking their perceived enemy. These actions fall under the category of psychological operations (PSYOPS) and are typically carried out by military personnel due to their demoralizing effects (Hagen, 2012).

which was extinct shortly after this particular campaign, is thought to have been affiliated with the Russian security services (*Ibid.*).

In truth, the Russian state's endorsement of these attacks is not such a farfetched possibility, given that it has passively supported previously coordinated cyberattacks on other states, like in Estonia in 2007.[35] Given the tight nexus between governmental structures and criminals that arose after the fall of the Soviet Union, numerous specialists maintain that the OCOs against Georgian targets "were carried out by Russian criminals but orchestrated by the Russian government" (Maurer, 2018, p. 101). In this sense, there's no current consensus on whether the attacks were a product of a sanctioning relationship or if they comprised a "blitz-orchestration"[36] of cyber proxies (*Ibid.*; Deibert *et al*., 2012). In line with Maurer (2018), I tend to agree with the latter scenario, particularly when considering the low virulence of the attacks and the likelihood that intelligence transfer occurred between Russian state agencies and cybercriminals (*See* Government of Georgia, 2008; Marques Guedes, 2009). In any case, while it is only probable that these hackers had received information that the invasion would be launched when it did, it is plainly obvious that Russia was aware of these incursions, which the government did nothing to prevent or prosecute. To Marques Guedes (2009), this trend has become an established pattern.

Crucially, these cyberattacks temporarily halted the Georgian government's ability to communicate with its military forces and citizens. The unavailability of information during a conflict can have severe psychological effects that can deeply demoralize or disorient people and the decision-making process (Deibert *et al*., 2012). Indeed, this disruption sowed panic among the population, herewith speculations that the invaders were going to take the capital Tbilisi. In the meantime, Russia was enforcing its narrative online, while also averting Georgia's connection with foreign governments (White, 2018).

The peace agreement was finally signed on August 15th, following President Medvedev's statement that the operation's objectives had been accomplished (*Ibid.*). In the aftermath of the conflict, Georgian cities and villages had been completely destroyed and savagely pillaged, with tons of thousands of displaced people subsisting in dire conditions. The generalized trauma and severe post-traumatic stress that resulted from the hostilities is extensively addressed in the EU's Independent International Fact-Finding Mission (IIFFMCG) and Human

[35] "Examples of the state-sponsored use of cyberattacks prior to 2008 include espionage (e.g., Titan Rain, Moonlight Maze), support to precision military raids (e.g., Operation Orchard), sabotage (e.g., Stuxnet, the planning for which is estimated to have begun in 2007), and coercion (e.g., Estonia)." (White, 2018, p. 1).

[36] Maurer (2018) refers to the term "blitz-orchestration", due to the swift and ephemeral mobilization of non-state actors that took place, which culminated with the projection of coercive (cyber) power (p. 46, 101-2).

Rights Watch (HRW) reports (*See* Tagliavini, 2009). The September 2008 report revealed that "[i]nterviews with displaced persons and others affected by the conflict make clear that many remain deeply affected and traumatized by their experiences during the conflict. Many were caught in conflict zones where they witnessed deaths, ill-treatment, and experienced human rights violations. Many lost their homes and possessions" (*Ibid*., p. 7).

Now, as established *supra*, one cannot separate the consequences of the information operation from those of the entire military campaign. Whether Russia actively orchestrated or passively supported the cyber blockade, it is clear that these cyberattacks effectively disrupted Georgia's internal and external communications in a critical moment of the invasion. Consequently, widespread disorientation and helplessness took over Georgian troops and the general population, which further difficulted any chances of countering or escaping the incoming violence. Moreover, the Georgian government was deprived of important information sources and external support. In this regard, an US-CCU Special Report states that "[t]he inability of Georgia to keep these websites up and running was instantly damaging to national morale" (Bumgarner & Borg, 2009, p. 5). Besides delaying any international response, these attacks "were designed to make it difficult to organize an effective response to the Russian presence" (*Ibid.*). In fact, the Estonia attacks of 2007 had already proven that a cyber campaign could provoke "serious economic and psychological disruptions in a country without provoking any serious international response" (*Ibid*., p. 7).

Here, it is worth referring to Christopher J. Finlay's (2018) conception of violence, founded on his 'Double-Intent Theory'. He defends that "[v]iolence is defined, on this account, first by a double intention: on the one hand to inflict harm and, on the other, to narrow the window of opportunity within which its victim can respond, to whatever extent is necessary for success and possible" (*Ibid*., p. 364). In this sense, there was a violent intent herewith. Likewise, this offensive cyber campaign is deemed violent within Egloff and Shires' definition of violence, as it intentionally and directly caused harm to key areas of human value – bodily, psychological, and communal. Foremost, the "primary objective of the cyber campaign was to support the Russian invasion of Georgia" (Bumgarner & Borg, 2009, p. 6). Additionally, the degree and scale of the disruption caused could be partly linked to the Georgian people's confusion and (possibly fatal) exposure to their attackers, as well as to the government's inability to intervene or mount any sound and coordinated defense on time. The resulting death, torture, and psychological toll on civilians is well documented in the subsequent reports. Afterwards, the HRW (2009) declared that "Russian forces failed to observe the obligations to do everything feasible to verify that the objects to be attacked were military objectives (and not civilians or civilian objects) and to take all feasible precautions to minimise harm to civilians" (p. 87).

All in all, there's still some debate on whether the cyber front had a substantial role in the general war effort. Whilst Deibert *et al.* (2012, p. 4) claimed that it conveyed "a significant, if not decisive, role in the conflict", White (2018, p. 1) defended that "[t]he cyberattacks had little effect on conventional forces and were not decisive to the outcome". In fact, the chaos that spurred from the cyber campaign could have been much worst. For one, Tbilisi's information systems were then quite "primitive" (Marques Guedes, 2009, p. 38). Numerous networks weren't connected to the Internet; thus, they could not be targeted. In addition, Georgia's government ordered the immediate shut-down of many of its servers, whose content migrated to external ones (*Ibid.*). Critically, the cyber attackers did not target critical infrastructures, such as power stations or oil-delivery facilities, but only those that could cause a relative "inconvenience", therefore conveying more of a threatening message (Bumgarner & Borg, 2009, p. 4). This strategy resembles Russia's previous conduct towards Georgia's vital strategic asset – the Baku-Ceyhan oil pipeline – which held great interest for Western powers. Russia carried out bombings around the pipeline without actually striking it, which served as a clear indication that they possessed the ability to do so if desired. Following this reasoning, the cyber campaign aligns with a broader Russian strategy, as analyzed by Bumgarner and Borg (2009).

In conclusion, according to Geers (2008), the Georgian cyberattacks have enabled an important shift in military thinking. This cyber expert foresaw that henceforth every political conflict would have a "cyber dimension", which mirrors Demchak's concept of "cybered conflict" (*Ibid.*; *See* Demchak, 2011). Several important lessons spur from this conflict. Firstly, in Hollis' (2011) words, we've witnessed "the emergence of synchronized cyberspace domain actions as an intelligence indicator for strategic, operational, and tactical level military operations" (p. 2). Secondly, there was a reinforcement of Russia's understanding of cyberspace as "a tool for holistic psychological manipulation and information warfare", specifically given its ability to successfully shape the international narrative at a decisive time (White, 2018, pp. 1-2). Lastly, these events brought attention to the involvement of non-state third parties (in this case, cyber proxies) in modern conflicts. Notably, Marques Guedes (2009) points out the legal complexities resulting from the emergence of what he termed "[virtual] coalitions of the spontaneously willing"[37] (p. 103).

[37] With this concept, the author sheds some light on the rise and nature of these sporadic 'warlike alliances' of hackers (or 'hacktivists') in the virtual civil society, which are formed and dissembled with the causes that spur them. He denotes that this phenomenon constitutes a paradigm shift in our conception of political alliances,

Finally, with this analysis, I assessed the consequences of the Russian cyberattacks on Georgian networks during the Russo-Georgian conflict of 2008. In particular, I set out to uncover whether the cyber incursion on this nation-state could be considered violent in the extended sense. I learned that, although no casualties or destruction resulted from cyberattacks alone, these still damaged areas of human value. The psychological impact is particularly evident, as the disruption of critical communication channels for both the affected population and the international community heightened feelings of fear and vulnerability and contributed to the public mismanagement of the crisis. On the contrary, as Egloff and Shires (2022; 2023) predicted, the traditional definition of violence cannot properly address the full human cost of this operation. Moving on, I will now examine whether this conclusion holds in the NotPetya case. Crucially, like the Russian OCO on Georgia, this cyberattack (almost a decade later) unlocked a new kind of state-sponsored cyberwarfare.

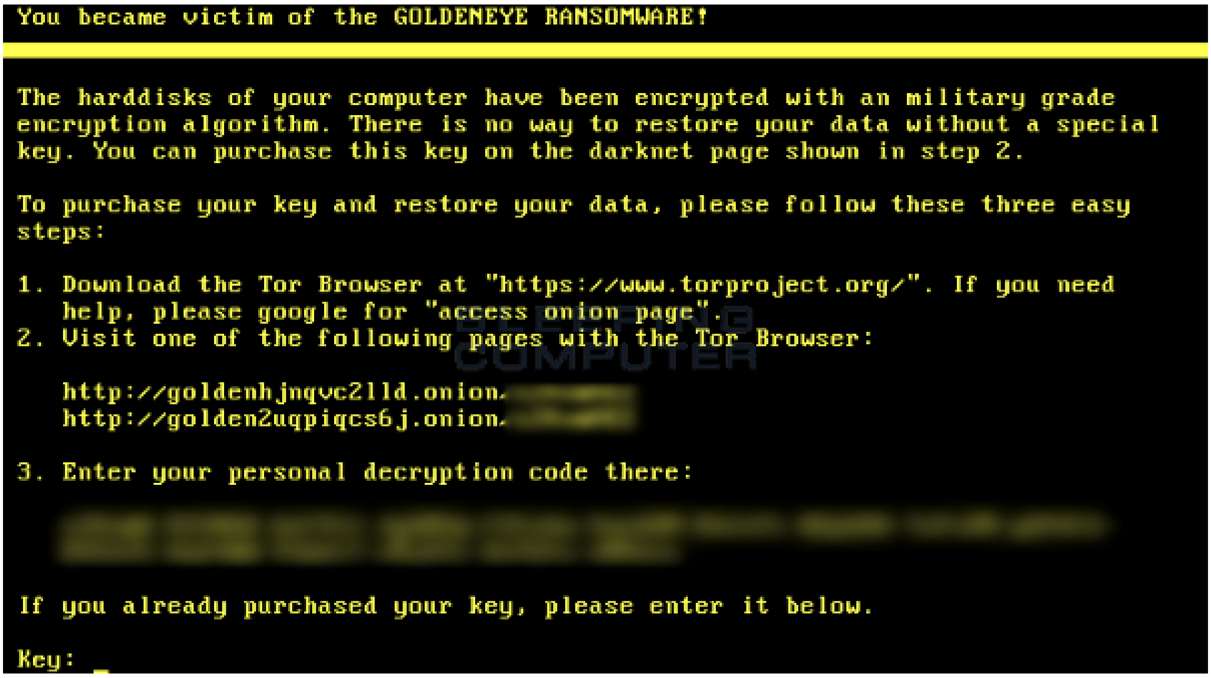
3.3.2. NotPetya malware attack (2017)

On 27 June 2017, the NotPetya malware was launched by Russia via the Ukrainian tax and accounting software, seeking to erase the greatest number of systems within the Ukrainian critical infrastructure, from national healthcare to electrical infrastructure (Stevens, 2017). Unwillingly or not, the worm ended up spreading viciously to a vast range of major multinational companies and institutions across the globe. The code employed by the hackers was carefully devised to disseminate automatically, swiftly, and indiscriminately. Ultimately, some refer to it as the most devastating cyberattack in history (Greenberg, 2018). Craig Williams, an executive from Cisco's Talos department (one of the first security firms to reverse-engineer the attack) disclosed to WIRED that: "[t]o date, it was simply the fastest-propagating piece of malware we've ever seen" (*Ibid.*). The estimated costs of the entire malware attack surpassed 10 billion USD worldwide, in the form of lost data, ruined equipment, irrecoverable revenues, etc. (*Ibid.*). Together with the North Korean WannaCry, this cyberattack ushered in a new era of indiscriminate and massively expanding cyber threats (Douzet & Gery, 2021).

To offer some perspective, the previous largest cyberattack in history, the WannaCry attack (of the same year) is believed to have caused financial damages ranging between 4 and 8 billion USD (Greenberg, 2018). In fact, NotPetya revealed some recognizable characteristics belonging to the WannaCry malware, as well as from its 2016 predecessor, the Petya

particularly on what they resemble, their possible impacts, and what limits to institute on their collective actions (*See* Marques Mendes, 2009).

ransomware – which encrypted files and demanded digital currency payments for their decryption. Notwithstanding, NotPetya’s messages requesting a ransom (*see* Fig. 7) were but a cover for its true intent – to destroy data on networks supporting a wide range of services, given that there was no real decryption-for-payment opportunity (*Ibid.*). These services included six power corporations, two airports, at least four hospitals just in Kyiv, over twenty-two Ukrainian banks, most ministries and federal agencies, and one nuclear power plant (Chernobyl) (Greenberg, 2018). Afterwards, the Information Systems Security Partners (ISSP) estimated that the attack permanently destroyed 10% of all computers in the country (Sologub, 2019).



```
You became victim of the GOLDENEYE RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://goldenhjnqvc2lld.onion/[redacted]
   http://golden2uqpiqcs6j.onion/[redacted]

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it below.

Key: _
```

Figure 7: Message after infection by NotPetya (aka GoldenEye) disguised as ransomware attack

Source: Esage (2016)

In the international setting, major corporations, such as FedEx, Maersk, Merck, Saint-Gobain, Mondelez International, and others, took up millions of dollars in losses. For instance, Maersk, an important UK-based shipping company (which handles close to one-fifth of the world’s shipping), revealed that it suffered financial costs estimated at approximately 250 million USD to 300 million USD – those figures are nonetheless believed to have been significantly downplayed (Greenberg, 2018). Nevertheless, the company's complete vulnerability during the halt of operations illustrates the actual disruption caused by the NotPetya cyberattack. Swiftly and simultaneously, all of Maersk's internet-connected devices, including "45.000 workstations, 4.000 servers, routers, VoIP phones, physical access settings, and other infrastructure", were infiltrated (*Ibid.*). With its over 70 ports worldwide and hundreds of ships, the multinational corporation found itself powerless in the face of this widely destructive virus. Ironically, the automated worm has even affected the Russian state oil company Rosneft.

This malware is the product of two Windows exploits working together. One was EternalBlue, a digital key that exploited a vulnerability in a Windows protocol, granting hackers remote control over unpatched machines. Originally, this penetration tool was developed by the US National Security Agency (NSA). However, it was later leaked in an extremely detrimental breach of the agency's highly classified documents in 2017, and finally refined by the Russian military intelligence agency (mainly known by its old acronym GRU), which subsequently launched it on Ukraine (Nakashima, 2018).[38] The other tool was Mimikatz, which was initially developed to demonstrate that Windows stored user passwords in the computer's memory. By using Mimikatz, hackers could extract these passwords from the system's RAM and use them to gain unauthorized access to other machines that shared the same credentials. This combination allowed for an automated attack to propagate like wildfire across networks, particularly on those with multiuser computers (Greenberg, 2018).

By incorporating both the EternalBlue exploit and a modified version of Mimikatz into the malware's design, the attackers ensured that this virus could spread autonomously, even infecting machines running updated versions of Windows (Greenberg, 2019b). This approach transformed NotPetya into a self-propagating worm, utilizing trusted networks instead of the Internet to bypass security measures typically effective against ransomware attacks (NCSC, 2018). The presence of the altered Mimikatz and EternalBlue within the malware's code suggests that it was not intended to selectively target its victims. Instead, its primary objective was to propagate as extensively and as rapidly as possible. By combining automated credential theft and vulnerability exploitation, this viral attack became uniquely capable of achieving the widest scale propagation ever seen in the history of cyberattacks (*Ibid.*). After successive waves

[38] After a thorough investigation, the CIA concluded with "high confidence" in November 2017, that the Kremlin's military intelligence agency known as GRU created the NotPetya malware, as revealed by *The Washington Post* article (Nakashima, 2018). In accordance with classified reports cited by U.S. intelligence officials, the hackers worked for the military spy service's GTsST (or the Main Center for Special Technology). This unit is reckoned to be highly involved in the GRU's cyber program, including the enabling of influence operations (*Ibid.*). Therefore, I denote a delegation relationship between the Russian state and its cyber proxy, in line with Maurer's classification (*See* Maurer, 2018).

of coordinated, malicious cyberattacks on the country, ISSP reasons that “Ukraine became a testing ground for global cyber warfare” (Sologub, 2019; *See* Greenberg, 2018).

According to Robert Hannigan, the former director of Britain's GCHQ intelligence agency, this incident demonstrated an escalation of Russia's aggressive actions in the digital realm against Ukraine, reflecting a broader strategy of "hybrid warfare" that combines conventional military methods with OCCs to attain regional dominance (Nakashima, 2018). To Jake Williams, founder of the cybersecurity firm Rendition Infosec, the main aim was "the disruption of Ukraine's financial system", at the same time sowing discredit on the whole Ukrainian system and businesses; thus, generating a shared feeling of vulnerability and directly harming the community (*Ibid.*; Egloff & Shires, 2022). Hence, in the strategic sense, the deployment of this cyberweapon seems to have been supportive of a much larger and prolonged destabilization campaign conducted by Moscow, in the context of the illegal annexation of Crimea and the Donbas region. Tactically, however, this attack fits into the complementary logic of integration, mainly due to its unprecedented magnitude (irreplicable through conventional weapons) (Egloff & Shires, 2022).

Curiously, the attackers appear to have been trying out this new cyberweapon, as if testing its real efficacy was the actual goal of the operation (Sologub, 2019). Notwithstanding its indiscriminate and global impact, no intent to cripple the Ukrainian infrastructure, physically or deeply, was recorded. Indeed, complementary uses tend to remain in an experimental phase (Egloff & Shires, 2022). Plus, similar to the previous case study, a certain restrain can be denoted from these state-sponsored cyber clashes (*See* Valeriano & Maness, 2018). In fact, no cyber incursions of NotPetya’s dimension have been attempted since then. Yet, this isn’t necessarily good news. As the CEO of ISSP Roman Sologub (2019) explains, a well-planed and targeted cyberattack takes between six to twelve months to be completed in all its stages (e.g., penetration, reconnaissance, exploration, data encryption, etc.), with the initial phases being mostly undetectable to their victims. That said, the final shutdown on June 27th was but a “clean-up stage” of a much wider and sophisticated OCO, with the hackers erasing all the evidence of their actions and the information they accessed and gathered over time (*Ibid*.).

In line with Sanger (2018), viral attacks of this nature can be regarded as prototypical for the future of cyber disputes, with their primary goal being to generate widespread chaos and fear in the adversary. Recent studies reveal that the WannaCry ransomware attack not only infected more than 200.000 computers in at least 150 countries, but also prompted a significant disruption on the social level (Benson & McAlaney, 2020, p. 86). Indeed, the threat was so pervasive that led to the closing of firms and organizations, workforce layoffs, halted production in some fields, and left many businesses struggling to recover afterwards (*Ibid*.). Critically, this virus spread to the UK's National Health Service (NHS), which resulted in cancelled operations, suspended treatments, and diverted ambulances (The Independent, 2017; BBC News, 2017b). This disruption spurred emergency governmental reactions: the UK summoned an emergency Cobra meeting; and the US coordinated a response by assisting in the international search for the culprits (*Ibid*.). Both states, together with Australia, Estonia, Denmark, Lithuania, and Ukraine, all formally accused North Korea of being behind this massive attack. However, the international response was apparently restrained to a 'public shaming campaign' (Korte, 2017; NCSC, 2018).

Most importantly, WannaCry brough with it the realization that cyberattacks could now result in deaths (especially, given the apparent unpreparedness of the NHS) (Benson & McAlaney, 2020; *See* Fisher *et al*., 2017). Consequently, the population experienced feelings of "worry, anguish, disbelief, and a sense of helplessness", accompanied by a dreading sense of loss of control (*Ibid*., p. 87). The NotPetya attack, albeit only disguised as ransomware, can be considered an improved version of WannaCry, this time with more pervasive intentions and no incorporated 'kill switch' (Sanger, 2018). That said, even though there are no official studies or surveys measuring the emotional or psychological impact following this massive attack, the NotPetya operation can still be deemed violent in the extended sense. This becomes particularly evident when considering the wider offensive cyber campaign mounted against Ukraine, at least since 2014 (Przetacznik & Tarpova, 2022). Over the past years, the country's public energy, media, financial, business, and non-profit sectors have suffered the most with Russia's cyber onslaught. Relentlessly, these attacks ranged from denial of access to basic services to data theft and deletion, defacements, disinformation campaigns, pervasive surveillance, DDoS, and so forth (*Ibid*.).

The cyber assault intensified against the build-up to the 2022 full-scale invasion of Ukraine. In mid-February, a DDoS attack shutdown the websites of various government departments, banks, and media stations for some hours, which led several states to blame Russia for wreaking "panic and confusion among Ukrainians" (*Ibid*., p. 3). It follows that NotPetya's aggressiveness should not be reduced to a non-violent tool deployed by the Russian Federation (as the proponents of the narrow definition would argue). Instead, it must be approached in the context of this extensive and devastating campaign against Ukrainian sovereignty and its people. Significantly, the 2017 viral shutdown purposedly happened in the eve of Ukraine's

Constitution Day.[39] Indeed, some argue that this destructive cyberattack could be termed an act of cyberwar (Greenberg, 2018). As Volodymyr Omelyan, the Ukrainian minister of infrastructure, put it: "[i]t was a massive bombing of all our systems" and "[t]he government was dead" (*Ibid*.).

Finally, the NotPetya malware, along with its precursor WannaCry, compelled governments to contemplate the characteristics and ethical implications of automated cyberattacks falling below the threshold of armed conflict (Kaminska, 2021). These attacks stood out due to the enormous financial and operational harm they caused, as well as their indiscriminate spreading. In reality, this perspective overlooks the substantial psychological and communal charge provoked by the continued and damaging assault on Ukraine's population and national identity. Nonetheless, OCOs of this kind – termed "operations against computer data" – are incorporated in the states' arsenal for psychological operations and propaganda dissemination directed at the civilian population (Schmitt, 2018, p. 16). Ominously, as they don´t reach to the (violent) level of an actual 'use of force', massive and indiscriminate cyberattacks of this type are not covered by the principles of proportionality and discrimination envisioned by IHL (Kaminska, 2021).

All in all, together with the Georgian cyberattacks, these instances bring up important gaps in International Law. Although very different in context, method, and completion, the two cases caused extensive damage and encountered no significant legal reprisals from the international community (besides symbolic condemnation on public channels). In wider terms, they can both be regarded as part of Russia's historical clashes with states that threaten its influence over the post-Soviet space. Historically, Moscow has relied heavily on subversion tactics and informational means to prepare the battlefield before direct intervention (e.g., by spreading propaganda, exploiting vulnerabilities, inciting local revolts, jamming communications, etc.), as demonstrated in Georgia and Ukraine (Galeotti, 2018).[40] Interestingly, the NotPetya incident (as a complementary use of OCCs) denotes a much higher degree of sophistication and pervasiveness in comparison to the Georgian (supportive) cyber campaign. Nonetheless, the latter portrays a seemingly more aggressive operation, as it was directly associated with open hostilities.

[39] June 28th, a national holiday, celebrates the date of the adoption of the new constitution in the Ukrainian parliament — also known as 'Verkhovna Rada' – in 1996. Greenberg (2018) argued that the selected date was strategic, by configuring an attempt to have as few people as possible in the offices at the time of the attack.

[40] This strategy aligns with George F. Kennan's (1948) notion of political warfare: "the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures … and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states."

Now, Russia has come to exemplify the intricate and concerning utilization of these tools not only to counter its state rivals, but also against its own population. In a landscape where illiberal regimes are increasingly harnessing digital advancements to assert control, Russia's strategic deployment of digital technologies stands out. As I will assess, the Russian government has demonstrated a sophisticated ability to manipulate the digital realm in ways that stifle dissent, curtail civil liberties, and silence opposition through intricate surveillance apparatuses, targeted online censorship, and disinformation campaigns. In the following chapter, I will delve into the distinct tactics and implications associated with states growing use of these technologies for political repression purposes, herewith shedding light on the ethical and human rights considerations that arise in the intersection of technology and governance.

IV. OCCs & POLITICAL REPRESSION

> "If it turns out the Internet help to stifle dissent, amplify existing inequalities in terms of accessing to the media, undermine representative democracy, promote mob mentality, erode privacy, make us less informed, it is not obvious how exactly its promotion is also supposed to assist in the promotion of democracy."
>
> - E. Morozov in *The Net Dilusion* (2011)

4.1. Contextualization

Throughout history, significant technological and communication breakthroughs have brought about societal transformations and political unrest (Feldstein, 2021). Innovations such as the printing press, telegraph, radio, and now the Internet have expanded people’s access to information and allowed them to reach broader audiences. Paradoxically, these advances have also contributed to the rise of centralized and totalitarian states. Today, authoritarian regimes are increasingly leveraging digital tools to bolster their oppressive agendas, fundamentally reshaping the dynamics of state coercion (*Ibid.*). This aligns with Deibert *et al.*’s (2011) concept of "access contested", which highlights the escalating struggle for dominance and control over power and influence in cyberspace (p. 21). Here, it is crucial to recognize that governments are no longer solely reactive to digital demonstrations but have also been adopting new tools to strengthen their grip on power. While some governments may have reasonable motives for utilizing contact-tracing apps or location-monitoring technology (for instance, to combat infections during global pandemics), there have been increasing reports of privacy infringements and human rights violations associated with these technologies around the world.

State actors have long tried to prevent, restrain, and control popular protests and, most recently, civic movements online. One significant flaw in the argument surrounding "liberation technology"[41] was our inability to acknowledge the central role of states in determining Internet infrastructure (*Ibid*.). According to Lührmann and Lindberg (2019), the actual consensus is that we have now entered the "third wave of autocratization". Nowadays, the number of democracies is supplanted by the number of autocratic states, with an estimated 54% of the world's population living under an authoritarian regime, and 35% going through a process of autocratization – i.e., the regression in the verification of political rights and freedoms – observed in states such as the U.S., Hungary, Poland, India, Brazil, and Turkey (Lührmann *et al*., 2020, pp. 6, 16). In fact, these technological advancements allow states to circumvent old challenges associated with traditional propaganda and psychological warfare by greatly expanding their scope and efficacy, while also permitting more targeted actions towards adversaries and a greater degree of anonymity. Therefore, emergent technologies have empowered both democratic and autocratic states to counter regime threats and advance their own agendas.

In essence, political repression occurs when state authorities aim at preventing dissident beliefs and/or activities which they deem as imperiling to political order (Goldstein, 2001). This concept comprises the actual or threatened use of force within or outside the territory of a state against individuals or organizations (Feldstein, 2021). In line with Steven Feldstein (2021), the author of *The Rise of Digital Repression*, I define digital repression (often used interchangeably with other terms such as 'digital authoritarianism' or 'algorithmic repression') as "the use of information and communications technology to surveil, coerce, or manipulate individuals or groups in order to deter specific activities or beliefs that challenge the state" (p. 25). Clearly, these practices not only improve public actors' capacity to conduct traditional repressive campaigns, but they also manifest themselves in various ways beyond the overt use of violence or forced internet shutdowns. Most frequently, digital repression strategies involve subtler techniques of monitoring and targeting political defectors or adversaries. In this sense, emerging digital methods are expanding the range of repressive tactics available to states.

[41] The role of emergent Information and Communication Technologies (ICTs) can be framed by opposing theories. As explained by Deibert *et al.* (2011), "cyberspace has emerged as a leading sphere of contestation between largely democratic forces seeking to use the Internet and related "liberation technologies" to expand and enhance freedom, knowledge, and connectivity and autocratic states eager to stifle that potential" (p. xv). Accordingly, 'liberation technology' is any form of ICTs that can expand political, social, and economic freedom. This argument is extensively analyzed in Evgeny Morozov's book – *The Net Dilusion* (*See* Morozov, 2011).

A more recent phenomenon is the increasing prevalence of social manipulation and disinformation strategies sponsored by governments. Deibert *et al.* (2011) referred to this novel reality as "third generation controls", in which governments go beyond censorship or content filtering to employing propaganda, surveillance, and counterinformation technics in order to undermine and discredit their adversaries. Following this reasoning, Nyst and Monaco (2018) argued that government involvement encompasses different scenarios ranging from public authorities directly executing actions of social manipulation ("state-executed"), and launching attacks coordinated with proxies and third parties ("state-coordinated"), to indirectly instigating attacks ("state-fueled"), or signaling the state's endorsement of anti-opposition trolling narratives without actual engagement ("state-endorsed") (pp. 17-23). Similar to the abovementioned Maurer's model, this classification outlines the spectrum of government roles in manipulating public opinion, involving direct implementation, coordination, indirect provocation, and sanctioning (*See* Maurer, 2018).

Importantly, Feldstein (2021) explains that, although digital technologies pose a transformative effect on political repression, their impact is highly contingent on the state's capabilities and regime type. Accordingly, while autocracies employ these methods profusely and intensively, democracies (especially, illiberal types) conduct digital repressive measures as well. It should be noted, though, that the absence of certain political rights or liberal institutions in hybrid regimes does not irradicate the costs of resorting to repression, as coercion runs the risk of undermining their leaders' apparent legitimacy (domestically and internationally) and chance of staying in power (*Ibid.*). Hence, the same reasoning applies to the use of digital techniques. Naturally, autocracies are more inclined than democracies to utilize digital tools to strengthen their regime's control and authority (*Ibid.*). However, as I will delve into later, this principle applies more prominently to certain digital tactics than others.

The type of threat faced by the regime is also relevant in this context. Whilst mounting a strong coercive apparatus[42] has always been a priority for autocrats, public institutions designed to counter external threats are fundamentally distinct from those aimed at suppressing internal challenges (Greitens, 2016). Theoretically, the former generally represent "fragmented and exclusive" institutions, built to prioritize loyalty to the leader and expected to employ higher levels of (indiscriminate) violence[43], whereas the latter constitute mainly "unitary and

[42] The terms 'coercive apparatus' or 'coercive institutions' are defined by Greitens (2016) as the "cluster of organizations collectively responsible for domestic intelligence and internal security" (p. 21).

[43] Regarding the argument's generality, Greitens (2016) refrains from applying her theory to other (considered more violent) communist regimes, such as North Korea or China. Hence, the author suggests that her argument is

inclusive" organizations, usually owning enhanced intelligence capabilities (including OCCs), which reduces the likelihood of resorting to violence (*Ibid.*, p. 12). In other words, countering coups calls for fragmented and exclusive institutions, while managing popular turmoil is best achieved by forming a unitary and inclusive security apparatus. Autocratic leaders negotiate this organizational tradeoff by designing their coercive institutions to address their main perceived threat at the time (*Ibid.*).

In this topic, Way and Levitsky (2006) categorize two fundamental forms of coercive state capacity: high-intensity and low-intensity coercion. The first type refers to clear acts of violence such as extrajudicial assassinations or the aggressive suppression of popular protests. In contrast, low-intensity coercion entails less evident but systematic actions aimed at monitoring, intimidating, and repressing opposition movements, like employing extensive surveillance networks, harassment and imprisonment of opposition members and their supporters, legal suits against the media, restricting career opportunities for those with opposing views, etc. Clearly, digital repression tactics are incorporated into this last category. Likewise, these scholars maintain that the state's capacity to implement low-intensity operations is dependent on its "scope and cohesion"[44], which requires capable and coordinated security forces and a robust and unified infrastructure (*Ibid.* p. 388).

Overall, strategies of digital repression offer unmatched abilities to monitor private communications, disrupt political mobilization, and influence public discussions. Therefore, states are compelled to resort to digital means of surveillance, given their ability to effortlessly intrude into people's private spheres (which is particularly evident in the number of states that purchase "lawful interception" spyware from companies like the NSO Group) (Deibert, 2014, p. 11; 2020). Other repressive and coercive methods include domestic censorship, the deletion of data belonging to opposition groups, or the intimidation and blackmailing of regime dissidents or political minorities. Critically, these are believed to be less intrusive or conspicuous when compared to traditional, more (physically) violent methods (such as physically raiding the opposition's headquarters) (Feldstein, 2021; Egloff & Shires, 2022). Consequently, governments that launch these types of covert OCOs face a reduced risk of compromising their legitimacy (by provoking public revolt), all while achieving their goals of political control.

best suited at explaining "everyday repression" instead of openly violent state campaigns (e.g.: the Cultural Revolution in China) (*Ibid.*, pp. 301-304). For more on this discussion, *see* Greitens (2016).

[44] According to the authors, 'scope' focuses on the extent of the government's reach, while 'cohesion' looks at how well the state's internal workings operate as a cohesive unit. These two factors are crucial determinants of a government's ability to exert control and implement policies effectively (Way & Levitsky, 2006).

Notwithstanding the increased ability to handle external problems, digital repression technics don't always succeed in deterring civic protests or promoting internal stability. This is mainly because most of these technics are double-edged. Indeed, whilst digital technologies provide governments with the means to monitor opposition, control the flow of information, and manipulate political narratives, they also offer civil society and opposition actors opportunities to unite and reduce obstacles to collective action. These tools enable leaderless coordination, the chance to counter government narratives, and to capture live instances of state brutality; thus, generating critical opinion shifts (as occurred in the Arab Spring revolutions, in 2011) (Feldstein, 2021). To sum up, digital repression constitutes a rather nuanced and complex term, covering a wide array of methods and tools that may vary widely across regime types, organizational frameworks, and international contexts. That said, I will dive into the main actors, types, and patterns concerning this growing phenomenon.

4.2. Actors and Patterns of Digital Repression

In his book, Feldstein (2021) separates digital repression techniques into five broad categories, namely: surveillance, censorship, social manipulation and disinformation, targeted persecution of online users, and Internet shutdowns (p. 25) (*See* Annex I). These practices differ from one another according to the distinctive set of tools that they incorporate. However, the use of one technic can often intersect with others. For instance, surveillance and the target persecution of defectors regularly go hand in hand. Moreover, various types of repression depend on certain technological applications that operate in tandem with legal, policy, and regulatory measures, as I will explain *infra* (*Ibid.*). Pertinently, in this section, I will scrutinize their main characteristics in an effort to understand these methods' pervasiveness and actual effects on modern societies and people's lives.

First, surveillance refers to the collection of information through the "identification, tracking, monitoring, or the analysis of individual data or systems" (*Ibid.*, p. 26). Historically, the emergence of surveillance methods is closely intertwined with the advent of modern nation-states (Giddens, 1985). In fact, the very possibility of authoritarian rule depends upon the state's ability to successfully penetrate (and control) everyday activities of its population. Besides, high-level surveillance involving the use of strengthened policing rapidly tends to dissolve into oppression and terror (*Ibid.*). Over the last two decades, we've witnessed the rise of the 'new surveillance', which figures as a direct consequence of the accessibility of individual transitional data a metadata (Zuboff, 2019).[45] This was made possible by the emergence of novel technologies that enable global communications, political engagement, financial transactions, and so forth (*Ibid*., Marx, 2004). According to Feldstein's (2021) classification, these strategies can range from passive surveillance (e.g., undifferentiated phone tapping), to targeted surveillance (e.g., deployment of intrusion malware on specific targets), big-data and AI methods (e.g., public facial recognition systems), and surveillance laws and directives (pp. 27-30).

Notably, the COVID-19 pandemic accelerated governments' deployment of surveillance strategies worldwide. By March 2020, 43 mass surveillance initiatives were adopted in 27 countries; 120 contact tracing mobile apps were available in 71 countries; and 60 location tracking measures were introduced in 38 countries (Woodhams, 2020). Crucially, this research has found that 49% of digital health mobile apps "do not have dedicated privacy policies" (*Ibid*.). According to a December 2022 report, cybercrime laws were repurposed to censor critical voices and criminalize misinformation spreading about the coronavirus in states like Kenya and Saudi Arabia, while countries like Russia and the Philippines introduced new legislation to closely monitor, silence and prosecute such activities (ECNL *et al*., 2022). Democracies such as India and Canada have resorted to similar practices to confront the crisis. Most worryingly, evidence shows that these measures were increasingly normalized beyond the pandemic (*Ibid*.). Ultimately, even though states may have legitimate reasons for turning to digital surveillance in the name of security, IL standards require that these methods prove to be necessary, proportionate, and clearly regulated.

Censorship is another tool that has been historically employed by repressive regimes. The digital age has led to the development of exceptionally invasive methods of controlling information online. Accordingly, digital censorship encompasses state actions and regulations aimed at restricting access to information, for instance, by blocking certain social media platforms or websites, censoring specific content, or legally punishing critical online activity. Roberts (2018) divided the main censorship strategies used by governments into three non-exclusive categories: fear, friction, and flooding. The first tactic involves dissuading

[45] In this topic, it is noteworthy to mention Soshana Zuboff's book *The Age of Surveillance Capitalism*, where she warns about the underlying perils associated with the rise of commercial surveillance. The book describes how tech companies like Google and Facebook instrumentalize what Zuboff (2018) terms the "behavioral surplus" – i.e., behavioral data that surveillance capitalists accumulate when consumers use their services. In brief, this surplus is then used to capitalize on the prediction and influence of human behavior, given that "the surest way to predict behavior is to intervene at its source and shape it" (*Ibid*.). A prominent example is the case of Cambridge Analytica, a UK consulting firm that allegedly used this 'behavioral surplus' to sway the US election in 2016. Remarkably, this argument stresses not only the great power wielded by these tech giants, but also its chilling implications for democracies worldwide.

individuals or the media from creating or sharing specific types of content through the provision of punitive measures, whilst the second merely encompasses the raising of the costs of accessing certain information, without envisioning legal repercussions (e.g., bypassing blocked websites by installing a VPN). Lastly, flooding tactics presuppose the "coordinated production of information by an authority with the intent of competing with or distracting from information the authority would rather consumers not access" (*Ibid.*, p. 80).

Additionally, flooding is easier to disguise in the information age than before. In fact, the Internet provided a new venue for people (and bots) to spread messages at a very low-cost. One commonly used tactic by state authorities is the employment of "Twitter armies" to coordinate and promote an alternative, 'preferred version' of events (*Ibid.*, pp. 83-84). Now, this censorship tactic can also be understood under the social manipulation and disinformation category, as its primary purpose is to persuade, confuse, or distract (Feldstein, 2021). What is more, several countries have crafted closed-off national Internet networks to allow full control over the distributed content online. Two of the most remarkable examples are the "great firewall" in China and the "halal net" in Iran (*Ibid*., p. 31). Also, Russia has allegedly been running tests on the implementation of a national Internet, the so-called *RuNet*[46], technically disconnected from the global network. The successful consolidation of state control over the Internet can allow authoritarian regimes to strengthen their power and influence over the population (Sherman, 2021).

Like the previous categories, influence and disinformation tactics – already extensively used by repressive regimes over centuries – have now gained a new momentum with emerging technologies. In this context, Feldstein (2021) advances five key components: disinformation, flooding, trolling and harassment, automated methods (like bots and algorithms), and vandalism/defacement (p. 32). Disinformation[47] (also known as propaganda, fake news, information operations, etc.) involves the deliberate spreading of false, incorrect, or deceptive information with the purpose of causing noticeable and significant harm (*Ibid*.). Here, I refer

[46] *RuNet* has been used in reference to several different (technical) definitions of the "Russian internet". To some analysts, the term denotes the Russian-language section of the global internet, encompassing former Soviet republics with Russian-speaking populations and Russian online content, along with entities physically situated in Russia. Others, however, refer specifically to the digital and physical internet infrastructure within the Russia Federation's borders and the internet users within this geographical scope (Sherman, 2021). Here, I am referring to the latter, which has been gradually closing itself off from the global Internet.

[47] In the Russian context, the term disinformation (*dezinformatsiya*) is often used to encompass a number of other concepts: "strategic deception" (*strategicheskaya maskirovka*), "active measures" (*aktivnye meropriyatiya*), psychological operations, concealment and deniability. The overarching vector is the use of various information tools – with some analysts referring to it as the "information weapon" – to convey selective, incomplete, and/or distorted messages and influence the thinking of an adversary (Moore, 2019, pp. 4-6).

to 'social manipulation and disinformation' as state-backed methods that aim to influence narratives and beliefs, hence suppressing the truth, misleading the population, or sowing distrust in the adversary. As an example, long before the full-scale invasion of Ukraine in February 2022, the Kremlin had for years reiterated the narrative that NATO was threatening the country and had plans of invading Russia; thereby, portraying Ukraine and the Alliance as the actual aggressors in the following conflict (Klug & Baig, 2023). These methods have continued on a "steep rise" since 2018, and they are not reserved for autocracies alone (Feldstein, 2021, p. 86) (*See* Fig. 8).

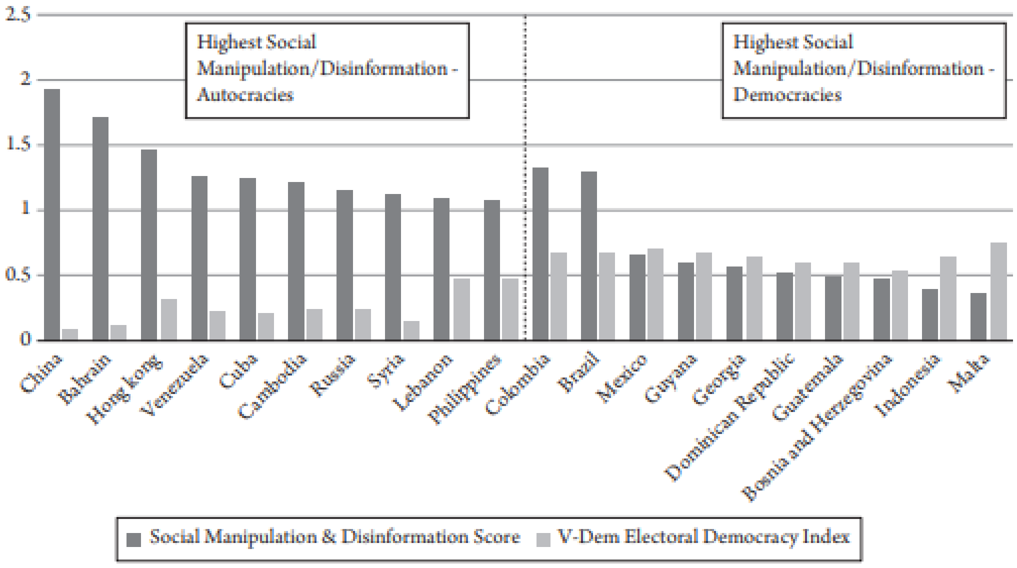


Figure 8: Comparison of the 'social manipulation and disinformation' indicators, in 2019

Source: Feldstein (2021, p. 85).[48]

The targeted persecution against Internet users typically involves targeted arrests, physical assaults, legal accusations, extended detentions, and violent suppression. In fact, authoritarian governments repeatedly target dissidents, journalists, human rights activists, and civil society groups. These agents infiltrate their networked devices, using a variety of sophisticated and persistent methods such as advanced malware campaigns or commercial spyware (Deibert,

[48] This index measures the principle of electoral or representative democracy, including whether elections were free and fair, as well as the prevalence of a free and independent media. The Democracy Indices by V-Dem are a dataset, released on an annual basis, that describes qualities of different governments published by V-Dem Institute.

2014). The latter appears to be particularly concerning, as the pervasive consequences spurring from these attacks may lead to irreparable harm to its victims (Feldstein, 2021). Nonetheless, this emerging market remains largely irregulated (*Ibid*.). Citizen Lab has uncovered that various governments and security services abuse these tools by hacking political opponents' platforms and human rights groups, both domestically and in other jurisdictions (Deibert, 2014). In this topic, Forensic Architecture[49] (2022) adds that the use of spyware is consistently entangled with a spectrum of physical violations, including break-ins, intimidation, assaults, arrests, lawsuits, and ultimately murders.[50]

Lastly, less technologically advanced states tend to resort to Internet shutdowns – i.e., the "intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information" (Olukotun, 2016). This tactic differentiates itself from other Internet restrictions (such as censorship), due to its time-bound feature that temporarily changes the state of the network. Accordingly, this phenomenon may vary in type (from 'bandwidth throttling'[51] to full Internet blackout) and scope (national, subnational, or solely comprising certain services/apps) (Feldestein, 2021). Data from the Shutdown Tracker Optimization Project (STOP) shows that Internet shutdowns have been dramatically increasing around the world (Dada & Micek, 2017).[52] Simultaneously, these incidents are now lasting longer, affecting more people, and increasingly being targeted at vulnerable groups. Countries like India, Myanmar, and Bangladesh use them to silence the voices of refugees and marginalized groups, whereas multiple nations in Africa often employ country-wide shutdowns in times of elections and political unrest (*Ibid.*).

Consequently, this reality is particularly critical in contexts where grave human rights violations are occurring. Now, this brings me back to the discussion on whether OCOs can be seen as violent in the broader sense. In a context of repression, Egloff and Shires (2022) contend

[49] Here, it is worth mentioning the Forensic Architecture Project – "Digital Violence: How the NSO Group enables State Terror", developed by Forensic Architecture and supported by Amnesty International and Citizen Lab. This project produces the most comprehensive database of incidents related to the NSO Group, in an interactive 3D platform. This research reveals that this company's Pegasus spyware is currently being distributed and used in at least 45 countries worldwide to infect and surveil the phones of activists, journalists, and human rights defenders (*See* Forensic Architecture, 2022).

[50] The famous case of the Saudi journalist and activist Jamal Khashoggi depicts an example of a regime-ordered extrajudicial killing, following an extensive campaign of digital and physical harassment and intimidation by the Saudi regime (Forensic Architecture, 2022). Khashoggi assassination occurred at the Saudi consulate in Istanbul, Turkey, at the hands of the bin Salman regime, sparking a global outcry (BBC News, 2018).

[51] Bandwidth throttling is the deliberate slowing of Internet traffic and mobile network connections (for instance, downgrading them to 2G) in order to disrupt communications and the regular flow of information.

[52] Data last updated in March 2023.

that complementary cyber capabilities offer additional repressive means to states, especially abroad. Unlike substitutive uses, such as the replacement of analog surveillance methods with digital ones, and supportive uses, which improve traditional repression tactics through adding digital technologies, complementary OCCs introduce novel methods of exerting extensive control and instilling terror in targeted populations (*Ibid*., *See* Deibert, 2014). As a pioneer in digital authoritarianism, China widely implements surveillance technologies, like cameras, sensors, facial recognition systems, and AI models, to create a pervasive atmosphere of fear and self-censorship. The most outrageous example is seen in the Xinjiang Region, where the Uighur minority (wrongly labeled as terrorists) are subject to constant monitoring and intimidation campaigns, while also targeting and harassing the diaspora communities. Hence, the region has been turning into what some have described as an "open-air prison" or a "digital Gulag" (Lamensch, 2021; *See* Furstenberg *et al*., 2021).

To conclude, digital technologies have made repression and control much more pervasive, efficient, and subtle (Lamensch, 2021). Michaelsen (2017) notes that digital surveillance and targeting activities are “facilitated by the increasing penetration of everyday life by the internet and social media, leading to a convergence of different social roles and activities on online platforms” (p. 466). It follows that the rise of digital repression practices around the globe is seriously threatening journalists, activists, regime critics, and civil society groups, both within and outside territorial jurisdictions. As I demonstrated, this complex phenomenon encompasses a wide range technics and tools, that are exploited by a growing number of states, albeit their use greatly varies according to regime type, threat perception, and technological sophistication. In truth, whereas authoritarian states turn to these repressive methods more extensively, democratic regimes do not fully refrain from using these tools. Plus, some states rely on less-advanced tactics, such as Internet shutdowns or hacking social media accounts, while others invest heavily in sophisticated surveillance networks, like ‘state of the art’ facial recognition systems or spyware programs.

At the same time, the impact of these technologies is contingent on state capabilities, organizational structure, and internal regulations. On this topic, Feldstein (2021) concluded that in countries with strong and capable institutions supporting extensive repression campaigns, and where checks on governmental power are weak, digital technology can drastically transform the regime's ability to accomplish its political objectives. However, in other scenarios where authorities lack the necessary capacity to effectively use digital tools, or in democratic settings with integrated safeguards, their impact is more restricted (*Ibid*.). Consequently, in states with robust coercive capabilities (such as coordinated security forces, a clear command structure, well-trained personnel, etc.), digital repression tools not only bolster existing oppression but can also revolutionize the state's capability to surveil political adversaries, suppress activist movements, and cause extensive harm on the population.

The case of Russia is particularly interesting, as this state has combined both old and new strategies (e.g., Soviet propaganda amplified by trolls using Twitter and Facebook and backed up by brute force) to create a brutal repressive machine. According to a 2021 special report from Freedom House, the Russian government engages in extremely aggressive transnational repression actions abroad, employing assassination as a prominent method and focusing on defectors and former insiders considered a risk to the regime's stability (Schenkkan & Linzer. 2021; *See* Gorokhovskaia *et al.*, 2023). Conversely, the government of Chechnya, an autonomous region in the North Caucasus, employs a slightly different, more vicious strategy. In my last case study, I will focus on (digital) transnational repression practices conducted by Russia, with an emphasis on the Chechen Republic, in an effort to understand the violent impacts of cyber technologies on individuals and communities. To do so, I will review the notion of "digital transnational repression", before turning to the analysis of the Russian, and more specifically Chechen, use of repressive methods abroad.

4.3. Case Study:

4.3.1. Digital Transnational Repression:

Even though the term 'transnational repression' is relatively recent, the practice itself is not new. In fact, it has long been a significant issue for diasporas with ties to authoritarian states, yet it has been systematically overlooked by academics (Furstenberg *et al*, 2021; Dukalskis *et al.*, 2022). Historical methods of spying, assassination, and retaliation against dissidents' families and associates have plagued emigrant communities for centuries. In reality, this phenomenon also dates back to the origins of nation-states, although it has gained more prominence with the growing establishment of bilateral and regional migration agreements, the global blurring of state borders in the late XX century, and, most recently, with the rise of Internet technologies (Tsourapas, 2021). Today, there are various notorious examples of transnational repression, from China's suppression of its Uyghur diaspora, Iran's state-controlled digital surveillance of exiled critics, Turkey's worldwide purge of those allegedly tied to the Gulen movement, and African states' sponsoring of violence against defectors, to the enforced disappearances of political émigrés in Central Asia (*Ibid.*; Furstenberg *et al*, 2021).

In contemporary times, with the rapidly increasing globalization, migration, and use of digital technologies, transnational repression has become a global and systematic phenomenon

(*Ibid.*). Authoritarian regimes have been increasingly adopting communication technologies to monitor and disrupt dissident networks, employing tactics like hacking, website defacement, malware planting, phishing, social media harassment, online threats, etc. (*See* Chope, 2023). Occasionally, instances where states violently repress their exiles abroad make headlines worldwide – e.g., the (abovementioned) brutal murder of journalist Jamal Khashoggi by Saudi operatives in Turkey in 2018; or the Belarusian dictator Lukashenko forcing a passenger plane to land in Belarus to detain a dissident journalist in 2021, using a false bomb threat (*Ibid*.; Dukalskis *et al*., 2022). Still, most dissidents from autocratic states and politically active communities in exile live in constant fear and are more often than not hidden from the public sphere.

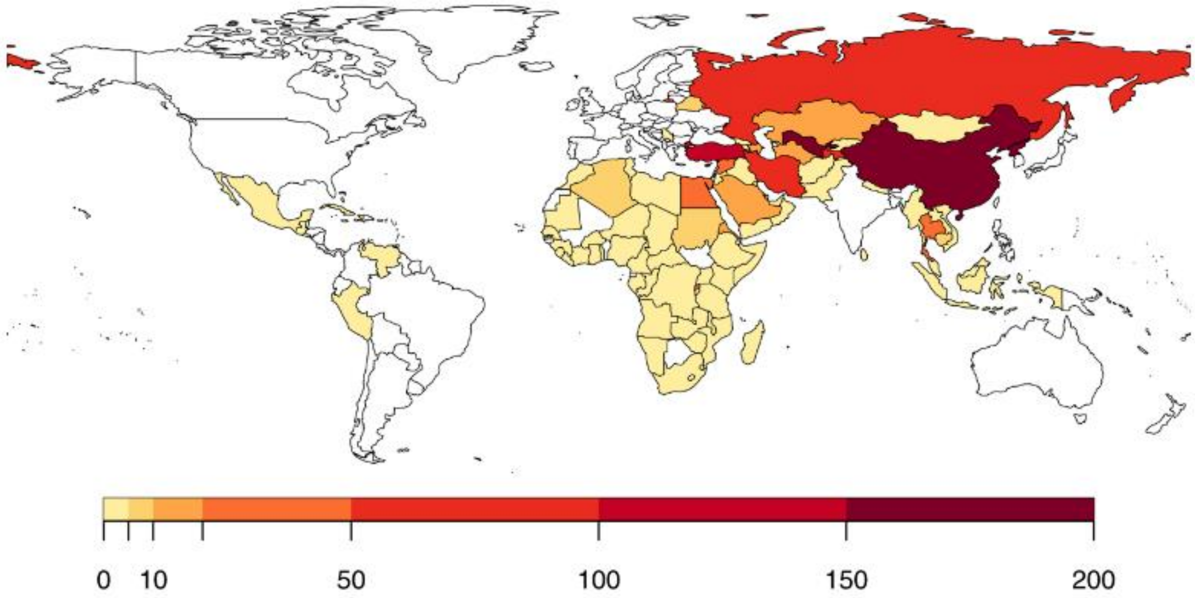


Figure 9: Perpetrators of transnational repression by number of cases (1991-2019)

Source: Dukalskis (2021, p. 73)

Most disturbingly, in certain countries, transnational repression has become an integral part of state policy (*Ibid*.). In a 2021 statistical study, Furstenberg *et al.* (2021) revealed that the most serious cases of extraterritorial repression are most probable to take place in the former Soviet republics (where many Central Asian exiles are found). This is mainly due to the legal channels and regional security agreements that rule procedures such as arrests and extraditions, like the Minsk Convention.[53] Even though this convention is meant to regulate extradition processes while also ensuring the rights of individuals, it nonetheless fails to account for the crucial principle of 'non-refoulement' – i.e., the international norm that establishes that refugees ought not to be sent back to a country where they may face mistreatment or harm (*Ibid*.). Another comparable agreement exists among members of the Shanghai Cooperation Organization (SCO). These instances illustrate situations where the process of extraditing individuals from one autocratic country to another is deemed legal and formalized through regional agreements, making it an institutionalized practice.

In a resolution of the Council of Europe, Chope (2023) notes that "[p]hysical transnational repression is only the tip of the iceberg" (p. 8). In fact, notwithstanding the numerous physical coercion cases, there are also wide-ranging tactics of 'everyday' transnational repression, such as digital threats, spyware, coercion through digital proxies, and the harassment of online users overseas. In this light, Citizen Lab has documented an increasing trend of using digital technologies to control, silence, and punish defectors across borders – a phenomenon commonly known as "digital transnational repression"[54] (*Ibid*.; Al-Jizawi *et al*., 2020, p. 5). Moreover, the misuse of interstate legal assistance mechanisms, like counterextremism, anti-money laundering, and anti-terror financing measures serves as another form of extraterritorial repression. These lead to severe consequences for targeted individuals, including asset freezing, financial exclusion, and so on. Critically, Lamensch (2021) warns that this phenomenon can be especially "subtle, pernicious and low-cost", as it easily evades matters of national jurisdiction and doesn't demand any physical dislocations to retain control over nationals abroad.

The most prolific perpetrators of this type of repression in 2022 were, according to Freedom House, the governments of China, Russia, Turkey, Egypt, and Tajikistan (Gorokhovskaia *et al.*, 2023, p. 27). Russia, in particular, has a long tradition of incurring in violent and often lethal retribution against its citizens abroad. In truth, this practice dates back to the early Soviet times, as Moscow tracked and pursued those who opposed to the Bolshevik regime and had emigrated

[53] The Minsk Convention (also known as the Convention on Legal Aid and Legal Relations in Civil, Family and Criminal Cases) was adopted in Minsk, on 22 January 1993. It was originally signed by Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russian Federation, Turkmenistan, Tajikistan, Ukraine, and Uzbekistan, thereby instituting a high degree of cooperation on criminal law between member states of the Commonwealth of Independent States (*See* Furstenberg *et al*., 2021).

[54] In accordance with Citizen Lab, I define "digital transnational repression" as the globalized practice "where states seek to exert pressure—using digital tools—on citizens living abroad in order to constrain, limit, or eliminate political or social action that threatens regime stability or social and cultural norms within the country" (Al-Jizawi *et al*., 2020, p. 5).

from Russia (the so-called “white Russian émigrés”[55]) (Tsourapas, 2021). After the fall of the Soviet Union, Russia has since been accused of perpetrating acts of violence against citizens who sought political asylum in Western nations. Two of the most famous cases were the poisonings of former-official Alexander Litvinenko, in London (2006), and Sergei Skripal and his daughter Yulia, in Salisbury (2018) (*Ibid.*). Today, Russia accounts for 7 of 26 assassinations or assassination attempts recorded globally, since 2014 (Schenkkan & Linzer, 2021, p. 27). This regime is also accountable for carrying out assaults, imprisonments, and illegal deportations in 8 different countries. Out of the 32 recorded instances of Russian transnational repression activities involving physical harm, a striking 20 cases reveal a Chechen link (*Ibid.*).

The targets chosen by the Kremlin include those who may have defected to NATO member states, collaborated with foreign intelligence and security agencies, or overall opposed Russia's interests or its secret services (Gorokhovskaia *et al.*, 2023). There are still numerous unexplained deaths of high-profile Russians in exile, their associates, and other potential targets connected to the Russian state. Despite clear evidence, such as the use of rare radioactive isotopes and nerve agents accessible only to the state or the actual detection of Russian operatives, the government still denies its involvement. Regardless of the growing international criticism, the Kremlin persists in using assassination as a method, thus sending a chilling warning to anyone engaged in political, intelligence, or business activities linked to the state (Schenkkan & Linzer, 2021).

Another common method is the misuse of the Interpol notice system as a weapon. Currently, Interpol is working urgently to strengthen supervision across 194 nations and reassess the vast number of ‘red notices’[56] that have accumulated over time (Apuzzo, 2019). The true extent of political interference in these notices, however, remains uncertain. The Russian state issues hundreds of names to Interpol in hope that at least some will stick; therefore, contributing to the harassment and detention of regime critics and defectors in other countries (Tsourapas, 2020; Gorokhovskaia *et al.*, 2023). Remarkably, Russia is accountable for 38% of all publicly issued red notices globally, in stark contrast to the United States at 4.3%

[55] This term (‘white Russian émigrés’, or ‘white émigrés’) refers to Russians who left the former Russian Empire following the events of the Russian Revolution (1917) and the Russian Civil War (1917–1923). They departed the region due to their opposition to the revolutionary Bolshevik political atmosphere in Russia. While many of these émigrés actively took part in or supported the White movement (in opposition to the ‘Red’ communists), the term is also used broadly to encompass those who left the country due to the shift in regimes.

[56] Put simply, the ‘red notices’ of Interpol represent a type of warrant in which police officers in one state ask their foreign counterparts to make an arrest. This notice system became a widely used tool by a growing number of governments worldwide (Apuzzo, 2019).

and China at 0.5% (Schenkkan & Linzer, 2021, p. 28). In fact, the government has widely used this tool to ensure the detection and deportation of citizens living overseas over long periods.

Besides high-intensity coercion tactics, like extrajudicial murders, Russia also engages in (and sponsors) low-intensity methods such as digital surveillance, online harassment, and advanced hacking campaigns (*Ibid.; See* Way and Levitsky, 2006). Notably, there are two major Kremlin-sponsored hacker groups: Fancy Bear and Cozy Bear, which employ similar tactics, benefit from substantial financial resources, sophisticated equipment, and a large network of employees who operate on a daily basis (Dobrokhotov, 2017). The accidently leaked 'target list' belonging to Fancy Bear provided significant proof of the state's close alignment with this organization (Satter *et al*., 2017). This extensive list focus on government opponents, journalists, and civil society figures spread across the globe, such as former-oil magnate Mikhail Khodorkovsky, Pussy Riot's Maria Alekhina, and famous activist Alexei Navalny (*Ibid*.). Russia, in its turn, fights these accusations with prevalent propaganda and disinformation campaigns.

Overall, Moscow employs a combination of methods to influence and control the Russian community abroad, focusing on essential pillars like the Russian Orthodox Church, Russian cultural institutions, and Russian-language media (Schenkkan & Linzer, 2021, p. 28). Ever since the fall of the Soviet Empire, the Russian government has strived to regain control over formal cultural institutions operating abroad, in particular the Orthodox Church. In a historical step, the Russian Orthodox Church Outside of Russia (ROCOR, also known as the 'Church Abroad'), established after the Bolshevik Revolution, was finally reunified with the Russian Orthodox Church, in 2007. Additionally, in 2008, the Federal Agency for the Commonwealth of Independent States Affairs, Compatriots Living Abroad, and International Humanitarian Cooperation (the *Rossotrudnichestvo*) was created to coordinate activities aimed at engaging with the diaspora and other official "soft power" initiatives. The Russian-language media also represents a key medium for manipulating and asserting influence over the post-Soviet space (*Ibid*.).

Furthermore, Russia's aggression war against Ukraine has exacerbated patterns of extraterritorial repression in Ukraine, Russia, Europe, and Central Asia (Gorokhovskaia *et al.*, 2023, p. 2). Thus far, the conflict has caused massive destruction, significant civilian casualties, human rights abuses, and the displacement of millions of Ukrainians and foreign citizens living in the country. In fact, Ukraine's visa-free entry system for citizens of 81 states, among other factors, made it a common choice for dissidents or others escaping authoritarian regimes (*Ibid*.). On the one hand, the invasion has put already targeted individuals in more vulnerable positions. On the other, the ongoing crackdown on rights and civil liberties in Russia over the last few years has been forcing people to leave the country, particularly anti-war activists and those fleeing forced military service[57] (HRW, 2022). Ultimately, these citizens could potentially turn into repression targets for the Kremlin, especially if they don't manage to secure asylum in other nations.

Curiously, as mentioned *supra*, the focus of the government's aggressive transnational repression efforts is on the coercion of particular individuals, and not on the control of the Russian emigrant community as a whole through violent means (Schenkkan & Linzer, 2021). On the contrary, Ramzan Kadyrov, the leader of the Chechen Republic, directs a total and brutal campaign of extraterritorial coercion against the Chechen diaspora (with the tacit endorsement from Moscow). This regime largely relies on digital platforms to collect information on Chechens in other countries (or even Russia), whose family members in the republic regularly face arrests and torture in order to silence dissenting voices abroad (CRD, 2016). Turning to the analysis of this specific campaign, I intend to probe how digital technologies contribute to (or enhance) the brutality of the regime against its people.

4.3.1.1. The Case of the Chechen Republic:

Within the spectrum of Russian transnational repression actions, the Chechen nexus holds a distinctive, more violent, connotation (*Ibid.*). This pattern started in 2009, with the killings of ex-military commander, Sulim Yamadayev, in Dubai, and of the former bodyguard of Kadyrov, Umar Israilov, in Austria (ICG, 2015; Council of Europe, 2023). Israilov had escaped and become a witness against the regime, holding evidence of a consistent practice of torture and executions involving the Chechen leader and his associates. Tragically, he was assassinated before he could testify in court. The Austrian police believed that this murder had been ordered by Kadyrov itself, as three Chechens were found guilty of accessory to murder (BBC News, 2011). In 2016, Abdulvakhid Edelgireyev, a prominent Chechen Islamist fighter affiliated with Al-Qaeda, was shot death in broad daylight, in Istanbul (Walker, 2016).[58] The prosecution of

[57] In an effort to create a comprehensive digital system of social control, the Russian government has implemented new legislation for drafting citizens into military service through online channels. Those who fail to comply with digital draft notices may receive severe penalties, including travel restrictions, financial limitations, and suspension of social benefits. This move reflects the state's larger ambition to establish a (totalitarian) state-controlled system of complete digital surveillance, coercion, and punishment, also known as the "Digital Gulag" (Stanovaya, 2023).

[58] In an article from the Guardian, Walker (2016) claims that this "murder is the latest in a pattern of audacious hits on key Chechen figures in the Turkish city over recent years". According to his sources, Turkish prosecutors believed that the Istanbul murders showed evidence of a more centralized Russian approach. At the time of the piece, the only suspect to be apprehended for any of the killings is an obscure figure who went by the nickname

Chechen dissidents continued and intensified in 2020 with the fatal stabbing of blogger Imran Aliyev, in Lille, and the assassination of Mamikhan Umarov, another critic of the regime, in Vienna (Schenkkan & Linzer, 2021; Council of Europe, 2023).

To contextualize, the Chechen diaspora emerged as a consequence of more than a century of Russian occupation, with significant growth during the two bloody wars for independence in the nineties. Following the defeat of the separatist movement in 2000, Akhmad Kadyrov governed the reintegrated republic under Russian rule until his assassination in 2004. Three years later, his son, Ramzan Kadyrov, was appointed his successor by President Vladimir Putin. Ramzan Kadyrov has since overseen a regime marked by extensive brutality, encompassing torture, extrajudicial killings, purges targeting the LGBTQIA+ community, and violent acts against journalists and human rights advocates (*Ibid.*; CRD, 2016). Albeit the relatively modest and rural population, Kadyrov's rule has adopted a rather intense personal character, close to that of a "personality cult" (ICG, 2015; Lokshina, 2016). The severity of repression has compelled numerous Chechens to seek refuge in Europe, driven by concerns about their safety both within Chechnya and in other parts of Russia.

Centrally, in contrast with the Kremlin's overall repression strategies abroad, the Chechen campaign of assassinations is built upon a foundation of comprehensive surveillance, digital intimidation, and coercion by proxy targeted at the entire Chechen diaspora (Schenkkan & Linzer, 2021). With growing numbers of Chechens overseas utilizing digital platforms such as Facebook or YouTube to express their opposition to Kadyrov's regime, the authorities realized that they could easily trace and gather information about opponents from publicly accessible sources. Subsequently, the government intimidates, detains, and occasionally subjects family members who are in Chechnya to serious coercion and torture, using them as leverage against dissidents living abroad. Additionally, the government has become adept of employing its own methods to either enlist or manipulate asylum seekers, turning them into operatives within the Chechen emigrant community (*Ibid.*). On the other hand, Chechen refugees have encountered mounting challenges in obtaining protection and asylum within Europe (Hauer, 2019). The two wars for independence, along with the insurgency against Russia (2000-2009), linked irrevocably Chechen militancy with international terrorism in the global imagination (Schenkkan & Linzer, 2021).[59]

"the Zone." This man was believed to be a Chechen citizen and to have been in contact with an FSB agent in respect to the murders.

[59] The involvement of Chechens and other North Caucasians in groups engaged in the Syrian civil war, including the Islamic State (IS) militant organization, further reinforced the view of Chechnya as a hub of terrorist activity (like in the abovementioned case of Edelgireyev) (Schenkkan & Linzer, 2021).

More recently, the regime's approach has shifted from reacting to events to taking proactive measures, transitioning from high-profile assassinations to the more routine practice of continuous surveillance (CRD, 2016). This strategy involves continuous monitoring of the diaspora through social media and telecommunications, orchestrated by the Chechen security services – which function as Kadyrov's autonomous force.[60] The surveilled targets may include relatives, acquaintances, and even extends to social media and blogs – platforms formerly used by the regime's opposition to express their views and organize. Kadyrov's government has enlisted teams of programmers and bloggers to monitor online activities, facilitated by the state institution known as the Security Council of the Chechen Republic, which is herewith responsible for tracing and directly punishing dissent (*Ibid*.).

Nonetheless, constant surveillance does not deter all Chechens. Those who opt to continue exposing the regime face meticulous scrutiny, physical harms, and potentially fatal costs devised by Kadyrov's forces. Their objective is to uncover compromising material ("kompromat") to shame critics on social media, resorting to fabrication if necessary (*Ibid*.). A case in point involves blogger Mikkail Malizaev, exiled in Germany. After condemning Kadyrov on Facebook, Malizaev witnessed immediate retaliation as his family in Chechnya was detained, abused, and coerced to demand his apology. Dissidents' family members can, in fact, face severe repercussions, including loss of benefits, property, or worse (Lokshina, 2016). Despite the pervasive threats, the blogger refused to return home and apologize. Those who do so risk beatings, televised humiliations, and uncertain fates, which often mean abduction, imprisonment, exclusion, or even murder (ICG, 2015; Hauer, 2019).[61] Years later, German immigration officers mandated Malizaev's wife and three kids to return to Chechnya, based on a failed asylum request (Malizaev didn't follow them due to his health condition at the time) (Hauer, 2019). The Chechen refugee was then forced to publicly apologize to Ramzan Kadyrov on YouTube. When he refused to use more groveling language in the video, Malizaev was physically beaten by two men in his house a few days later (*Ibid.*).

As a result, the Chechen emigrant community understands that any perceived actions against Kadyrov or the regime could lead to punishment for their relatives. This prompts

[60] The Chechen security services operate with a substantial degree of independence from the broader Russian federal security services, with their interaction mainly limited to training and sharing intelligence (CRD, 2016; *See* Marten, 2010). Still, some infamous cases like the abovementioned "Istanbul murders" denote a larger role from the central power in Moscow (*See* Walker, 2016).

[61] In the International Crisis Group (ICG) report, many interviewed Chechen residents identified public humiliation, along with collective punishment, as the two main factors leading to the pervasive fear within modern Chechen society (ICG, 2015; Lokshina, 2016). A Chechen citizen explained: "It's not even violence that is scary. They will disown you, publically humiliate you, make you a prostitute or a drug addict. You won't be able to live with dignity in this republic anymore. This is worse than death" (ICG, 2015, p. 35).

emigrants to preemptively cut off communication with friends and family back home (CRD, 2016). The widespread surveillance, including wiretapping and social media monitoring, means that even the innocent mentioning of critics or human rights defenders can compromise the anonymity of those at risk. Alongside opportunistic informants, the Chechen government dispatches its own agents, who often pose as refugees in Europe and spy on these communities to gauge political sentiments or scout for critics. Sometimes, these agents even reveal their true identities to remind people that they are not safe from political violence anywhere (*Ibid*.). What is more, these measures are taken jointly with the active manipulation of online media to depict dissident Chechens abroad as exceptions. In response to the public protests against the government that broke out in 2015 in various European cities, a simultaneous spur of videos featuring Chechens in Europe praising Kadyrov flooded the Internet (*Ibid*.).[62]

All in all, Kadyrov's totalitarian rule based on oppression and fear has managed to violently stifle dissent and maintain control, both domestically and abroad. The dissemination of videos of torture, humiliation, and brutal punishments by the security forces, aligned with the physical presence of militia men in diaspora spaces feeds into this climate of extreme and "pervading fear" that no one can escape from (Marty, 2010, p. 1). According to an International Crisis Group (ICG) report from 2015, popular fear had only become stronger, particularly following the pattern of assassinations that began in 2009 (and has intensified over the last few years) (*Ibid.; See* Council of Europe, 2023). To make things worse, there is a generalized assumption that pursuing legal remedies is simply useless, if not detrimental (ICG, 2015). Indeed, the Chechen leader remains untouched, despite all the human rights violations and international condemnation of his actions.

In one of the report's interviews, a Grozny resident said: "It was easier when federal troops were here; we knew where the enemy was, where danger came from" (*Ibid.*, p. 36). In fact, every respondent would turn off their phone and allow no voice recording during the interviews. This is especially concerning for Chechen refugees, who, thanks to modern technologies and digital platforms, are never totally out of reach. Now, in my view, this denotes a complementary logic, as digital-enabled repression allows this oppressive regime to go to great (and violent) lengths to spread its terror. In this sense, the Chechen government is able to maintain a massive and multifaced surveillance and intimidation campaign at entire communities overseas. As Kadyrov so eloquently put it: "I know all the webpages of all the

[62] In line with Feldstein's (2021), "flooding" can be both a technic used in censorship practices and as a social manipulation and disinformation tool.

young people who are residing in Europe, every Instagram and Facebook profile, every account of every social network, we are writing down your every word and putting them on record, we have all data on you, who you are, and what you are doing, we know everything. Nowadays, the modern age and technologies allow us all of that, we know everything and can find anyone, so do not make it worse for yourselves" (Caucasian Knot English, 2016).

To provide some perspective, since its rise to power in 2007, Ramzan Kadyrov has come to enjoy a crescent degree of autonomy over the Chechen Republic (Marten, 2010; Markedonov, 2015). His 'iron rule' has been met with an active endorsement from the Kremlin, particularly given the regime's role in the stabilization of this historically problematic region, ravaged by inter-ethnic disputes, separatist revolts, and Islamic terrorism (*Ibid.*). Indeed, securing the Northern Caucasus area remains of foremost strategic importance for Russia (Marques Guedes, 2010b). So, in reality, Kadyrov's Chechnya exists as a distinct entity within the Russian Federation, with a parallel policy and informal, yet well-trained, security units operating alongside official structures. It maintains a separate taxation system, its own legal framework, and, in practice, foreign relations (ICG, 2015). This so-called "outsourcing of sovereignty"[63], according to Marten (2010), is deemed necessary so that Putin can indirectly run Chechnya, while saving the "political and economic costs of a military occupation" (p. 5). At the same time, this trade-off might imply the allowance of certain (oppressive) "excesses" on Kadyrov's part, as Markedonov (2015) highlighted.[64]

In conclusion, we continue to witness the evolution and reconfiguration of state violence in scenarios of state rivalry and political repression. Whereas digital technologies have provided governments worldwide with means to engage their populations, assess public opinion, and adjust governance strategies, these very tools have also granted authoritarian and undemocratic regimes unparalleled abilities to maintain their hold on power. Most worryingly, as these technologies mature, it is expected that they will be used more profusely by states. Today, Russia is one of the most proficient adepts of the transnational nature of the Internet when it comes to repressive methods. This type of 'cyber repression' can be seen as particularly violent in the Chechen case, as I demonstrated in the last case study. Emerging technologies and communication channels are regarded by this regime as revolutionary means that allow Kadyrov to reach far beyond Chechnya's borders and violently coerce its people into

[63] Here, Marten (2010) draws on the classic definition of 'sovereignty', in accordance with Weber and his theory on the emergence of the 'legitimate monopoly on the use of force' (*See* Weber, 1919/2015).

[64] Interestingly, this 'fragmentation' of coercive power mirrors Greitens' theory of "fragmented and exclusive institutions", which lead to increased levels of violent repression (*See* Greitens, 2016).

submission. In contrast, analyzing these repressive practices using a purely physical lens would not account for the extensive psychological and communal violence that digital technologies directly enable on the Chechen population, not just in Russia but across the world.

V. CONCLUSION

5.1. Main conclusions and implications

> "The practice of violence, like all action, changes the world, but the most probable change is to a more violent world."
>
> - H. Arendt in *On Violence* (1970, p. 80)

The advent of Internet technologies has not only brought immense opportunities for both private and governmental entities but has also introduced significant disruptions to contemporary societies. These disruptions are further exacerbated by the increasing significance of ICTs in today's globalized world, amplifying the scope and consequences of such disturbances. The prevailing trend is evident: as digitalization becomes more prevalent, the susceptibility to vulnerabilities rises, exposing various domains of society, business, and governance to potential interference, manipulation, or harm. In the words of Brantly (2017), which approaches this question through an effects-oriented perspective, the "manipulation of code when directed towards a violent end can and does achieve violence" (p. 87). This scholar adds that the growing sophistication and widespread use of cyber capabilities inevitably lead to their weaponization by nation-states, given that the "pervasiveness of code can magnify the impact of non-armed force to include economic and political violence" (*Ibid.*, p. 88).

Nevertheless, in the last decades, the harmful consequences of such tools have been systematically unrecognized or underplayed by states, even though their impacts are being increasingly felt in all spheres of human activity. At the beginning of this dissertation, I set out to break with the current consensus that OCCs are basically non-violent alternatives to traditional means, by diving into the analysis of recent hostile uses of such technologies. To explore this hypothesis, I turned to Florian Egloff and James Shires' mode of analysis and applied it to pertinent cases. Focusing on the state, I carried the assumption that offensive cyber operations are always inserted into larger strategic decisions (which then turn into campaigns) made by state actors in relation to the offensive means that they have at their disposal. Likewise, even though I separated the terms 'interstate' and 'repressive' as differing types of state violence, I acknowledge that they often blur in real-world scenarios (*See* Chenoweth *et al.*, 2019). Thus, I applied the same criteria to thoroughly assess them.

Regarding my first question – ‘can uses of OCCs be deemed violent in the extended sense?’ – I uncovered that they do often cause harm to various areas of human value. This conclusion is informed by recent surveys (mentioned in Chapter II) and the three case studies I conducted. These surveys showed that the emotional distress prompted by hypothetical actions of cyber terror could be compared to those provoked by (kinetic) terrorist attacks. The following case studies confirmed that OCOs undertaken by state actors can result in extensive harm to individuals and populations worldwide. Very succinctly, the sustained cyber campaign and the disruption of communication systems at the beginning of the invasion of Georgia not only sowed chaos in the Georgian society but directly hampered the Georgian forces’ ability to protect their country and citizens. Moreover, the unmatched scale of the NotPetya attack caused vast social disruption worldwide and installed fear and distrust in Ukrainian society. What is more, the inherent violence in (and enabled by) the constant surveillance, digital intimidation, and targeted persecution of online dissent by Putin’s regime, both within and outside Russia, has become an established and disturbing trend.

Centrally, I learned that the narrow definition of violence fails to capture the wide range of non-physical harms brought by these evolving technologies. Analytically, I refrained from comparing both the narrow and extended conceptions of violence in terms of severity. Instead, I focused on assessing the analytical value of this notion when grasping the comprehensive array of impacts of employing OCCs against individuals and communities. Although measurements in state brutality fall beyond the scope of this work, I found that digital technologies greatly enable its increase in terms of range. In other words, while the level of intensity of violence remains unclear when compared to conventional methods, cyber means do entail more violence in extensiveness. That said, I believe that researchers and strategists ought to transcend somatic understandings of this concept as to include psychological violence, violence against communities, symbolic violence, among others. Accordingly, concerns about the escalatory dynamics of cyber conflicts should be refocused on violent escalation. This reasoning aligns with the normative aim of reducing cyber-related violence in IR by changing the political calculous on the deployment of OCOs.

With this, I turn to the second question: ‘is Egloff and Shires’ mode of analysis appropriate to examine violent uses of OCCs?’. To evaluate this, I looked into this model’s utility, clarity, and coherence. Overall, I maintain that the expanded definition provides a better conceptual base to study these effects in comparison to the traditional concept. Notwithstanding its obvious advantages, this framework reveals some significant flaws. Foremost, as I alluded to above, the authors failed to deliver a scale of severity. Yet, they stated that the most violent OCOs are "authoritarian practices of digital globalised repression, the indirect consequences of disrupted critical infrastructures, and digitally-enabled interpersonal coercion" (Egloff & Shires, 2021), without backing this claim with any empirical grounds. Similarly, these scholars reasoned that complementary uses of OCCs are the ones susceptible to entail more violence when contrasted to the other two types (supportive and substitutive). This is in part because, according to Egloff and Shires (2022), they are the least likely to be covered by existing legal frameworks. Once again, no quantitative data supports this claim. Consequently, their central thesis – that "OCCs relocate, rather than reduce, state violence" (Egloff & Shires, 2023, p. 131) – is theoretically unfounded.

Another issue with this definition is the notion of proximity. As mentioned above, authors like Kello (2013) are skeptical of the ability of informational means to be a proximate cause of harm. Conversely, others maintain that cyber tools are violent in their ability to inflict (not solely physical) damage through first, second and third-order effects (*See* Brantly, 2017; Egloff & Shires, 2022; Shandler *et al.*, 2023). In reality, I am confident that it is beyond their first-order consequences – e.g., data theft, denial of access, Internet blackouts, or disinformation – that their most acute and harmful impacts are found. The sources visited in this study confirmed that non-physically damaging cyberattacks can still perpetrate extensive harm by traumatizing individuals, aggravating cycles of violence, and corroding civil liberties (*See* Shandler *et al.*, 2023). That being said, it remains unclear how immediate in the causal chain an effect has to be in order for it to fall within this classification. Additionally, this vector of the framework excludes important angles such as the reliance on code to exacerbate instances of structural violence.[65]

Finally, I concede that the division between the three logics of integration adds analytical value to the discussion. In particular, the notion of complementary uses of OCCs – i.e., those that generate new forms of inflicting harm – conveys the debate towards the most innovative and complex (and therefore, threatening) types of cyber operations and their negative consequences. Indeed, their unique character makes them the most likely to require profound legal and policy adjustments moving forward (Egloff & Shires, 2022). This becomes particularly important when considering the current absence of international norms and conventions governing these rapidly emerging technologies. In the case of interstate disputes,

[65] As an example, biased algorithms can reinforce existing societal prejudices and inequalities, in processes like hiring, loaning, or accessing to information or basic services. Consequently, code can affect marginalized or targeted communities disproportionately, thus contributing to the aggravation of systemic violence. However, according to their authors, this category does not verify the framework's criteria of proximity and intention (*See* Egloff & Shires, 2023).

the fact that cyber operations are most often undertaken in a shady ‘gray area’ that falls short of armed attacks (historically conceptualized in terms of physical violence) further complicates their effective regulation. Nonetheless, states should be called to reassess their military and security doctrines so as to adjust to the profound transformations of the digital age. Crucially, our concepts should properly reflect these transformations. Hence, even though this model does not represent the most comprehensive (or even practical) solution, I regard it as a worthy step in the right direction.

All in all, this expanding understanding of harm reinforces the need for ethical scrutiny and policy frameworks that address the multifaceted effects of OCCs, ultimately guiding responsible behavior in the cyber realm. Nevertheless, as mentioned before, there are some drawbacks associated with the use of a broader definition of ‘violence’: analytical blurredness, political exploitation, or possible escalation. The lack of theoretical focus could be alleviated with the elaboration of concise metrics of analysis, which require further empirical and systematic research. In fact, I contend that clearer parameters, informed by real-life scenarios of cyber conflict and digital repression campaigns, would irrevocably improve their practical and normative value. In the words of Morozov (2011), “[w]e need policies informed by realistic assessments of the risks and dangers of the Internet”. Significantly, to the ICRC, the adoption of an expanded and widely accepted definition of violence is a crucial step in this process (Gisel *et al.*, 2020).

To summarize, I believe that the theoretical and strategical discourse surrounding the deployment of offensive cyber operations should evolve to encompass broader dimensions beyond the realm of physical violence. While the traditional focus on bodily harm remains crucial, it's equally important to acknowledge the psychological and communal harms inflicted on societies through the strategic use of OCCs. Contrarily to authors like Valeriano and Maness (2015), I reckoned that the ‘deterring forces’ at play in cyberspace are not preventing new forms of violence in this domain. Rather, their negative impacts are expected to worsen in scale and scope as these new weapons are developed and disseminated. As I revealed, these technologies have the potential to not only cause immediate physical damage but also to generate profound psychological distress and communal upheaval. Their effects currently reverberate through communities, eroding trust, exacerbating divisions, and sowing discord and fear among populations.

5.2. Research limitations and evaluation

When I began this research work, one of the first issues I encountered was the lack of quantitative research in the field. For that reason, I substituted an extensive empirical analysis of the main cyber operations in the last two decades with a more constrained qualitative analysis of two major events and one repression setting associated with one nation-state. As a result, the hypothesis-testing study that I conducted turned out more limited, and thus less significant, than I initially intended. To tackle this limitation, I focused on examining the initial questions using a multidisciplinary approach that touched upon a wide number of established fields, such as political studies, IR, cyber conflict studies, IL, philosophy and ethics, cyberpsychology, and so on. Consequently, I was able to construct a comprehensive theoretical study, test some of Egloff and Shires' assumptions, and infer valuable insights on the relation between state violence and emerging OCCs.

As I stressed above, another difficulty I faced early on was the lack of metrics provided by this mode of analysis. Its inherent vagueness presented an obstacle not only to the assessment of the violent uses of cyber technologies but also to the delimitation of my research universe. On the one hand, there is a surprising lack of OCOs catalogs to choose from; on the other, I struggled with the selection of the most productive (or elucidative) case studies. This problem of lack of demarcation became more noticeable in Chapter IV, where I was unable to create a reasonable criterion to situate the case study in a manner similar to the previous ones in Chapter III. This was mainly due to the lingering academic divisions between studies on interstate conflict and digital repression, which preclude a coherent evaluation of these increasingly blurring realities. Nonetheless, I strived to select notable and illustrative scenarios that were backed by reliable and interdisciplinary sources, thereby allowing me to conduct an informed analysis.

Lastly, my research clashed with the prominent idea that digital technologies are non-violent weapons. In turn, I asserted that the most evident expression of violence within the realm of cyberspace lies in offensive cyber capabilities, which involve the adversarial manipulation of digital systems and networks in context of international conflicts and global oppression. Indeed, nation-states remain a central source of violence in the global arena, as the development of new violent capabilities in the cyber domain raises important philosophical, strategic, and policy questions. Nevertheless, these actors are far from the only ones with access to these new powerful weapons. In fact, non-state actors such as private corporations, multinational tech firms, non-governmental organizations, and organized crime networks are becoming increasingly important players in today’s global shifts of power (*See* Nye, 2011b). Therefore, in future research, the use of OCCs by these actors must also be included in the discussion. In principle, the proposed framework provides a valuable direction for advancing this debate.

5.3. Future research

The endless reshaping of state violence persists in the Internet era. My comprehensive research study not only sheds light on the appreciation of OCOs as violent expressions (and on their pervasive consequences), but also contributes to the overdue reconceptualization of core concepts in our age, such as violence, harm, and war. As I demonstrated, including affective and community harms within the concept of violence challenges the conventional emphasis on physical harm, leading to a more nuanced understanding of the harm's variety. This perspective enhances both academic and policy discourse in the field. Moreover, in line with Egloff and Shires (2023), I believe that this model could potentially be expanded to other information-enabled technologies, so as to expose and tackle presently undetected forms of violence in international politics. However, extensive analytical research is still required in order to systematically compare the different logics of integration and assess their full theoretical value. In addition, more digital vectors of harm (e.g., structural violence) ought to be comprehensively addressed and added to this framework.

History shows that societal structures take time to adapt to and regulate paradigm-shifting technologies. In fact, it took almost three decades after the bombing of Hiroshima to develop agreements concerning nuclear weapons. As the level of disruption and destruction enabled by these technologies becomes ever more evident, specialists expect this domain to increasingly dominate states’ national security concerns. Nonetheless, norms governing the risks posed by cyber technology are likely to evolve slowly, not based on goodwill but on states’ self-interest in coordination, status, and restraint (Segal & Goldstein, 2022). This research study offers a fruitful conceptualization of violence; however, extensive research and empirical data are still needed moving forward. In the end, ″[t]he “open global internet” may be over, but self-interest in coordination and communication remains, even among adversaries” (*Ibid.*, p. 68).

Bibliography

Abbott, K. W., Genschel, P., Snidal, D. & Zangl, B. (Eds.) (2015). *International Organizations as Orchestrators*. Cambridge University Press.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

Al-Jizawi, N., Anstis, S., Barnett, S., Chan, S., Sen, A., & Deibert, R. (2020). Annotated Bibliography: Digital Transnational Repression. *Citizen Lab.* https://citizenlab.ca/wp-content/uploads/2021/05/Annotated-Bibliography-Digital-Transnational-Repression-May-2021.pdf

Alvey, R. (2001). Russian hackers for hire: the rise of the emercenary. Janes Intelligence Review, 13(7), 52-53.

Apuzzo, M. (2019). How Strongmen Turned Interpol into Their Personal Weapon. *The New York Times*. https://www.nytimes.com/2019/03/22/world/europe/interpol-most-wanted-red-notices.html

Arendt, H. (1970). *On violence*. Harcourt, Brace & World.

Arquilla, J. (1999). Ethics and Information Warfare. In Khalilzad, Z., LaTourrette, T., Mosher, D. E., Davis, L. M., Howell, D. R., & Raymond, B. (Eds.). *Strategic Appraisal: The Changing Role of Information in Warfare* (379-402). Rand Corporation.

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

Asal, V., Mauslein, J., Murdie, A., Young, J., Cousins, K., & Bronk, C. (2016). Repression, Education, and Politically Motivated Cyberattacks. *Journal of Global Security Studies, 1*(3), 235–247. https://doi.org/10.1093/jogss/ogw006

Backhaus, S., Gross, M. L., Waismel-Manor, I., Cohen, H., & Canetti, D. (2020). A Cyberterrorism Effect? Emotional Reactions to Lethal Attacks on Critical Infrastructure. *Cyberpsychology, Behavior, and Social Networking*, *23*(9), 595–603. https://doi.org/10.1089/cyber.2019.0692

Baron, I. Z., Havercroft, J., Kamola, I., Koomen, J., Murphy, J., & Prichard, A. (2019). Liberal Pacification and the Phenomenology of Violence. *International Studies Quarterly, 63* (1), 199–212.

Barrett, E. (2017). On the Relationship Between the Ethics and the Law of War: Cyber Operations and Sublethal Harm. *Ethics & International Affairs*, *31*(4), 467–477. https://doi.org/10.1017/s0892679417000454

BBC News. (2011). Austrian court convicts Chechens over dissident’s death. https://www.bbc.com/news/world-europe-13621483

BBC News. (2017a). Cyber-Attack: US and UK Blame North Korea for WannaCry. www.bbc.com/news/world-us-canada-42407488.

BBC News. (2017b). NHS “robust” after cyber-attack. https://www.bbc.co.uk/news/uk-39909441

BBC News. (2018). Khashoggi death: Saudi Arabia says journalist was murdered. https://www.bbc.com/news/world-middle-east-45935823

Beck, U. (2009). *World at Risk*. Polity.

Benson, V., & McAlaney, J. (2020). *Emerging Cyber Threats and Cognitive Vulnerabilities*. Academic Press.

Betz, D., & Stevens, T. (2011). Cyberspace and the State: Towards a Strategy for Cyber-Power. *Adelphi Series, 51*(424), 75-98. https://doi.org/10.1080/19445571.2011.636956

Billo, C. & Chang, W. (2004). *Cyberwarfare. An Analysis of the Means and Motivations of Selected Nation-states*. Institute for Technology and Security Studies.

Blakeley, R. (2012). State Violence as State Terrorism. In Breen-Smyth, M. (Ed.). *The Ashgate research companion to political violence* (63-78). Ashgate https://www.researchgate.net/publication/264715825_State_Violence_as_State_Terrorism

Bobbitt, P. (2003). *The shield of Achilles: war, peace and the course of history*. Anchor Books.

Bowden, M. (2011). Malware myopia. *Los Angeles Times.* https://www.latimes.com/opinion/la-xpm-2011-oct-23-la-oe-bowden-malware-20111023-story.html

Brantly, A. F. (2017). The Violence of Hacking: State Violence and Cyberspace. *The Cyber Defense Review, 2*(1), 73-92. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Violence%20of%20Hacking_Brantly.pdf?ver=2018-07-31-093713-703

Brenan, M. (2021). Cyberterrorism tops list of 11 potential threats to US. *GALLUP* [Survey]. https://news.gallup.com/poll/339974/cyberterrorism-tops-list-potential-threats.aspx.

Bufacchi, V. (2005). Two Concepts of Violence. *Political Studies Review, 3*(2), 193–204. https://doi.org/10.1111/j.1478-9299.2005.00023.x

Bumgarner, J., & Borg, S. (2009). *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008.* U.S. Cyber Consequences Unit [Report]. https://indianstrategicknowledgeonline.com/web/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

Bumiller, E., & Shanker, T. (2012). Panetta Warns of Dire Threat of Cyberattack on U.S. *The New York Times*. https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Byman, D. (2012). *Passive Sponsors of Terrorism*. Cambridge University Press.

Cambridge University Press. (n.d.). War. In *Cambridge Dictionary.* https://dictionary.cambridge.org/dictionary/english/war

Caucasian Knot English. (2016). *Kadyrov threatens emigrants from Chechnya* [Video]. YouTube. https://www.youtube.com/watch?v=q_BTt27mKEM

Cenciotti, D. (2013). Syria Never Stood a Chance Against Israel's Electronic Warfare. *Business Insider*. https://www.businessinsider.com/israeli-electronic-warfare-in-syria-2013-2

Chenoweth, E., English, R., Gofas, A., & Kalyvas, S. N. (2019). *The Oxford handbook of terrorism*. Oxford University Press.

Chope, C. (2023). Committee on Legal Affairs and Human Rights. *Transnational Repression as a Growing Threat to the Rule of Law and Human Rights*. Council of Europe. AS/Jur, 17. https://rm.coe.int/transnational-repression-as-a-growing-threat-to-the-rule-of-law-and-hu/1680ab5b07

Cioffi-Revilla, C. (2009). Modelling Deterrence in Cyberia. In Gori, U. (Ed.) *Modelling Cyber Security: Approaches, Methodology, Strategies* (125–131). IOS Press BV.

Civil Rights Defenders (CRD). (2016). *Chechnya - Repression Without Borders* [Report]. https://crd.org/wp-content/uploads/2018/06/Chechnya-Repression-Without-Borders.pdf

Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.

Clausewitz, C. (1984). *On War*. (Howard, M. & Paret, P., Trans.). Princeton University Press. (1832).

Dada, T., & Micek, P. (2017). Launching STOP: the #KeepItOn internet shutdown tracker. *Access Now*. https://www.accessnow.org/keepiton-shutdown-tracker/

Deibert, R. (2014). *Communities@ risk: Targeted digital threats against civil society*. Citizen Lab at the Munk School of Global Affairs. University of Toronto. [Policy Report]. https://hdl.handle.net/1807/80130

Deibert, R. J. (2020). *RESET: Reclaiming the Internet for Civil Society*. House of Anansi Press Ltd.

Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue 43*(1), 3–24. https://doi.org/10.1177/0967010611431079

Deibert, R., Palfrey, J., Zittrain, J., & Rohozinski, R. (2011). *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. MIT Press.

Demchak, C. (2011). *Wars of disruption and resilience: cybered conflict, power, and national security*. University Of Georgia Press.

Denning, D. E. (2007). "Cyberterrorism". Testimony before the Special Oversight Panel on Terrorism. Committee on Armed Services, U.S. House of Representatives. In Linden, E. (Ed.). *Focus on Terrorism* (Vol. 9, 71-76). Nova Science Publishers Inc.

Denning, D. E. (2012). Stuxnet: What Has Changed?. *Future Internet, 4*(3), 672–687. https://doi.org/10.3390/fi4030672

Dobrokhotov, R. (2017). Russia's soft warfare. *Al Jazeera*. https://www.aljazeera.com/opinions/2017/2/27/russias-soft-warfare

Douzet, F., & Gery, A. (2021). Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace. *Journal of Cyber Policy, 6*(1), 96–113. https://doi.org/10.1080/23738871.2021.1937253

Dukalskis A. (2021). *Making the World Safe for Dictatorship*. Oxford University Press.

Dukalskis, A., Furstenberg, S., Gorokhovskaia, Y., Heathershaw, J., Lemon, E. & Schenkkan, N. (2022). Transnational repression: data advances, comparisons, and challenges. *Political Research Exchange 4*(1). https://www.tandfonline.com/doi/full/10.1080/2474736X.2022.2104651

Egloff, F. J., & Shires, J. (2021). Making the Concept of Violence Central to the Study of Offensive Cyber Operations. Offensive Cyber Working Group. https://offensivecyber.org/2021/11/09/violence-offensive-cyber/

Egloff, F. J., & Shires, J. (2022). Offensive Cyber Capabilities and State Violence: Three Logics of Integration. *Journal of Global Security Studies, 7*(1). https://doi.org/10.1093/jogss/ogab028

Egloff, F. J., & Shires, J. (2023). The better angels of our digital nature? Offensive cyber capabilities and state violence. *European Journal of International Security, 8*(1), 130-149. https://doi.org/10.1017/eis.2021.20

Esage, A. (2016). Petya Ransomware Returns with GoldenEye Version, Continuing James Bond Theme. *Information Security Newspaper*. https://www.securitynewspaper.com/2016/12/07/petya-ransomware-returns-goldeneye-version-continuing-james-bond-theme/

Feldstein, S. (2021). *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*. Oxford University Press.

Segal, A., & Goldstein, G. (2022). *Confronting Reality in Cyberspace. Foreign Policy for a Fragmented Internet*. Independent Task Force [Report N. 80]. Council on Foreign Relations. https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf

Finlay, C. J. (2018). Just War, Cyber War, and the Concept of Violence. *Philosophy & Technology, 31*(3), 357–377. https://doi.org/10.1007/s13347-017-0299-6

Fisher, M., Therrien, A., Hand, J. & McCague, B. (2017). How cyber-attack is disrupting NHS. *BBC News*. https://www.bbc.com/news/live/39901370

Forensic Architecture (2021). Digital Violence: How the NSO Group enables State Terror. https://forensic-architecture.org/investigation/digital-violence-how-the-nso-group-enables-state-terror/

Fruhlinger, J. (2022). *Stuxnet explained: The first known cyberweapon*. *CSO Online*. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Furstenberg, S., Lemon, E., & Heathershaw, J. (2021). Spatialising state practices through transnational repression. *European Journal of International Security, 6*(3), 358–378. https://doi.org/10.1017/eis.2021.10

Galeotti, M. (2018). I'm Sorry for Creating the "Gerasimov Doctrine." *Foreign Policy Magazine*. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security 38*(2), 41–73. https://www.jstor.org/stable/24480930

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies, 24*(2), 316–348. https://doi.org/10.1080/09636412.2015.1038188

Gartzke, E., & Lindsay, J. R. (2017). Thermonuclear cyberwar. *Journal of Cybersecurity, 3*(1), 37–48. https://doi.org/10.1093/cybsec/tyw017

Geers, K. (2008). Cyberspace and the changing nature of warfare. *SC Media.* http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/554872/

Gibson, W. (2013). *Neuromancer*. Harper Voyager Publishers.

Gisel, L. (Ed.) (2018). *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities Under International Humanitarian Law: International Expert Meeting, 22-23 June 2016, Quebec*. ICRC [Report].

Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross, 102*(913), 287–334. https://doi.org/10.1017/s1816383120000387

Goldstein, R. J. (2001). *Political repression in modern America from 1870 to 1976*. University Of Illinois Press.

Gomez, M. A., & Villar, E. B. (2018). Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats. *Politics and Governance, 6*(2), 61-72. https://doi.org/10.17645/pag.v6i2.1279

Gorokhovskaia, Y., Schenkkan, N., & Vaughan, G. (2023). *Still Not Safe: Transnational Repression in 2022*. Freedom House [Report]. https://freedomhouse.org/sites/default/files/2023-04/FH_TransnationalRepression2023_0.pdf

Gorwa, R., & Smeets, M. (2019). Cyber Conflict in Political Science: A Review of Methods and Literature. In *Working Paper Prepared for the 2019 ISA Annual Convention* (1-24). https://doi.org/10.31235/osf.io/fc6sg

Government of Georgia (2008). *Russian Invasion of Georgia: Russian Cyberwar on Georgia* [Report]. Accessed via WayBack Machine, https://web.archive.org/web/20111117042929/http://mfa.gov.ge/files/556_10535_798405_Annex87_CyberAttacks.pdf

Greenberg, A. (2018). The Untold Story of NotPetya, The Most Devastating Cyberattack in History. *WIRED*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greenberg, A. (2019a). New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction. *WIRED*. https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/

Greenberg, A. (2019b). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Greitens, S. C. (2016). *Dictators and Their Secret Police: Coercive Institutions and State Violence*. Cambridge University Press.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists, 72*(5), 284–291. https://doi.org/10.1080/00963402.2016.1216502

Hadji-Janev, M., & Aleksoski, S. (2013). Use of Force in Self-Defense Against Cyber-Attacks and the Shockwaves in the Legal Community: One more Reason for Holistic Legal Approach to Cyberspace. *Mediterranean Journal of Social Sciences, 4*(14). https://doi.org/10.5901/mjss.2013.v4n14p115

Hagen, A. (2012). The Russo-Georgian War (2008): The Role of Cyber Attacks in the Conflict. *The Armed Forces Communications and Electronics Association.* https://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf

Hauer, N. (2019). 'If Someone Speaks the Truth, He Will Be Killed'. *The Atlantic*. https://www.theatlantic.com/international/archive/2019/12/chechnya-ramzan-kadyrov-vladimir-putin/603691/

Hern, A. & MacAskill, E. (2017). WannaCry Ransomware Attack “Linked to North Korea.” *The Guardian*. www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group.

Herrera, G. L. (2007). *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*. State University of New York Press.

Himma, K. E. (2007). *Internet security: hacking, counterhacking, and society*. Jones and Bartlett Publishers.

Hoisington, M. (2009). Cyberwarfare and the use of force giving rise to the right of self-defense. *Boston College International and Comparative Law Review, 32.* http://dx.doi.org/10.2139/ssrn.1542223

Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. *Small Wars Journal*. https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Holsti, K. J. (1964). The Concept of Power in the Study of International Relations. *Background, 7*(4), 179-194.

Human Rights Watch (HRW). (2009). *Up In Flames - Humanitarian Law Violations and Civilian Victims in the Conflict over South Ossetia*. [Report]. https://www.hrw.org/report/2009/01/23/flames/humanitarian-law-violations-and-civilian-victims-conflict-over-south

Human Rights Watch (HRW). (2022). *World Report 2022: Events of 2021*. The New York Times/Redux [Report]. https://www.hrw.org/sites/default/files/media_2022/01/World%20Report%202022%20web%20pdf_0.pdf

International Crisis Group (ICG). (2015). *Chechnya: The Inner Abroad*. [Europe Report n. 236]. https://icg-prod.s3.amazonaws.com/236-chechnya-the-inner-abroad.pdf

Jianqun, T., & Longdi, X. (2014). *Cyber War Preparedness, Cyberspace Arms Control and the United States*. China Institute of International Studies.

Kaminska, M., Broeders, D., & Cristiano, F. (2021). Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone. *13th International Conference on Cyber Conflict (CyCon), 59-72.* https://doi.org/10.23919/cycon51939.2021.9468290

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, *38*(2), 7–40. https://doi.org/10.1162/isec_a_00138

Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

Kennan, G. F. (1948). Policy Planning Staff Memorandum n. 269. *National Archives and Records Administration*. https://history.state.gov/historicaldocuments/frus1945-50Intel/d269

Kissinger, H. (2014). *World Order: Reflections on The Character Of Nations And The Course Of History*. Penguin Books Ltd.

Klug, T., & Baig, R. (2023). Fact check: Russia’s disinformation campaign targets NATO. *DW News*. https://www.dw.com/en/fact-check-russias-disinformation-campaign-targets-nato/a-64675398

Korte, G. (2017). *White House plan to “shame” North Korea shows complexities of responding to cyberattacks*. USA TODAY News.

https://eu.usatoday.com/story/news/politics/2017/12/19/white-house-strategy-punish-north-korea-wannacry-attack-were-going-shame-them/964116001/

Kostyuk, N., & Zhukov, Y. M. (2017). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution*, *63*(2), 317–347. https://doi.org/10.1177/0022002717737138

Krepinevich, A. F. (1994). Cavalry to Computer: The Pattern of Military Revolutions. *The National Interest*, *30*(37), 33-42. https://nationalinterest.org/article/cavalry-to-computer-the-pattern-of-military-revolutions-848

Lamensch, M. (2021). Authoritarianism Has Been Reinvented for the Digital Age. *Centre for International Governance Innovation.* https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/ .

Last, J. M. (2007). Harm. In A Dictionary of Public Health. *Oxford University Press*. https://www.oxfordreference.com/display/10.1093/acref/9780195160901.001.0001/acref-9780195160901-e-1867

Levy, J. S. (2008). Case Studies: Types, Designs, and Logics of Inference. *Conflict Management and Peace Science,* *25*(1), 1–18. https://journals.sagepub.com/doi/10.1080/07388940701860318.

Libicki, M. C. (2012). *Crisis and Escalation in Cyberspace*. RAND Corporation. https://doi.org/10.7249/mg1215

Libicki, M. C. (2016). *Cyberspace in peace and war*. Naval Institute Press.

Liff, A. P. (2012). Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies, 35*(3), 401–428. https://doi.org/10.1080/01402390.2012.663252

Lindsay, J. R. (2017). Restrained by design: the political economy of cybersecurity. *Digital Policy, Regulation and Governance*, *19*(6), 493–514. https://doi.org/10.1108/dprg-05-2017-0023

Lokshina, T. (2016). “*Like Walking a Minefield”: Vicious Crackdown on Critics in Russia’s Chechen Republic*. Human Rights Watch [Report]. https://www.hrw.org/report/2016/08/31/walking-minefield/vicious-crackdown-critics-russias-chechen-republic

Lupovici, A. (2016). The “Attribution Problem” and the Social Construction of “Violence”: Taking Cyber Deterrence Literature a Step Forward. *International Studies Perspectives*, 17 (3), 322–42. https://doi.org/10.1111/insp.12082

Markedonov, S. (2015). Outsourcing sovereignty from Russia to Chechnya. *OpenDemocracy*. https://www.opendemocracy.net/en/odr/outsourcing-sovereignty-from-russia-to-chechnya/

Marques Guedes, A. (2009). *A Guerra dos Cinco Dias [The Five Days War]*. Instituto de Estudos Superiores Militares.

Marques Guedes, A. (2010a). The New Geopolitical Coordinates Of Cyberspace - As Novas Coordenadas Geopolíticas Do Ciberespaço. *Revista Militar*, N. 2503/2504, 823 – 847.

Marques Guedes, A. (2010b). Russia and the West. An Interview of Armando Marques Guedes, conducted by Sergey Markedonov. *The Caucasus Times*.

Marten, K. (2010). Russia, Chechnya, and the Sovereign Kadyrov. *PONARS Eurasia,* (116).

Marty, D. (2010). Parliamentary Assembly. *Legal Remedies for human rights violations in the North-Caucasus region*. Council of Europe. RES 1738. https://pace.coe.int/pdf/60054d9cd5847b66952c743bbda99b68c80463c6d1b98952230a8376c0c01bb3/res.%201738.pdf

Marx, G. T. (2004). What's New about the "New Surveillance"? Classifying for Change and Continuity. *Knowledge, Technology & Policy, 17*(1), 18–37. https://doi.org/10.1007/BF02687074

Maurer, T. (2011). The Case for Cyberwarfare. *Foreign Policy*. https://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/

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

McDermott, R. (2019). Some emotional considerations in cyber conflict. *Journal of Cyber Policy, 4*(3), 309–325. https://doi.org/10.1080/23738871.2019.1701692

McGraw, G. (2013). Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*, *36*(1), 109–119. https://doi.org/10.1080/01402390.2012.742013

Michaelsen, M. (2017). Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran. *Surveillance & Society, 15*(3/4), 465–470. https://doi.org/10.24908/ss.v15i3/4.6635

Moore, C. (2019). *Russia And Disinformation: Maskirovka*. Centre for Research and Evidence on Security Threats [Report]. https://crestresearch.ac.uk/resources/russia-and-disinformation-maskirovka-full-report/

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs.

Nakashima, E. (2018). Russian Military was Behind "NotPetya" Cyberattack in Ukraine, CIA Concludes. *The Washington Post*. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

National Cyber Security Center (NCSC). (2018). Russian military "almost certainly" responsible for destructive 2017 cyber attack. https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

Nye, J. S. (2011a). Nuclear Lessons for Cyber Security?. *Strategic Studies Quarterly 5*(4), 18–38.

Nye, J. S. (2011b). *The future of power*. Public Affairs.

Nye, J. S. (2016). Deterrence and Dissuasion in Cyberspace. *Journal of Cyber Policy, 1*(2), 44–71. https://doi.org/10.1162/ISEC_a_00266

Nyst, C., & Monaco, N. (2018). *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*. Institute for the Future [Report]. https://legacy.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf

OECD (2019), Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies. *OECD Publishing*. https://doi.org/10.1787/02f0e5a0-en

Oltsik, J. (2009). Russian Cyber Attack on Georgia: Lessons Learned?. *CSO online.* https://www.csoonline.com/article/547308/cisco-subnet-russian-cyber-attack-on-georgia-lessons-learned.html

Olukotun, D. B. (2016). Internet shutdowns – an explainer. *DW Akademie*. https://akademie.dw.com/en/internet-shutdowns-an-explainer/a-36731481

Oxford University Press. (2002). Violence. In *The Oxford Essential Dictionary of the U.S* Military.https://www.oxfordreference.com/display/10.1093/acref/9780199891580.001.0001/acref-9780199891580-e-8876?rskey=Z0lFiE&result=4

Oxford University Press. (2006). Casus Belli. In *The Oxford Dictionary of Phrase and Fable.* https://www.oxfordreference.com/display/10.1093/acref/9780198609810.001.0001/acref-9780198609810-e-1349

Pathe Duarte, F. (2015). Sociedade de Risco [Risk Society]. In Gouveia, J. B., & Santos, S. (Eds.). *Enciclopédia de Direito e Segurança* (451-453). Almedina.

Pollard, N. A., Segal, A., & Devost, M. G. (2018). Trust War: Dangerous Trends in Cyber Conflict. *War on the Rocks.* https://warontherocks.com/2018/01/trust-war-dangerous-trends-cyber-conflict/

Press Trust India (PTI). (2015). World Facing ‘Bloodless’ Cyber War Threat: Modi. *The Hindu.* https://www.thehindu.com/news/national/world-facing-bloodless-cyber-war-threat-modi/article7375190.ece

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). 8 June 1977. ART. 51(2). https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-51

Przetacznik, J. & Tarpova, S. (2022). Russia's war on Ukraine: Timeline of cyber-attacks [Briefing]. *European Parliamentary Research Service (EPRS),* 1-7. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

Rid, T. (2017). *Rise of the machines: a cybernetic history*. W.W. Norton & Company.

Rid, T., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal, 157*(1), 6–13. https://doi.org/10.1080/03071847.2012.664354

Roberts, M. E. (2018). *Censored: Distraction and Diversion inside China’s Great Firewall*. Princeton University Pres.

Saar Poll. (2013). Public Opinion and National Defense. *Ministry of Defence of Estonia.* https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/public_opinion_and_national_defence_2013_oct.pdf

Sanger, D. E., & Mazzetti, M. (2016). U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict. *The New York Times*. https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html

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

Satter, R., Donn, J., & Myers, J. (2017). Russian hackers used a digital hit list to target nations, including the U.S. *PBS NewsHour*. https://www.pbs.org/newshour/world/russian-hackers-used-a-digital-hit-list-to-target-nations-including-the-u-s

Schelling, T. C. (2008). *Arms And Influence*. Yale University Press.

Schenkkan, N., & Linzer, I. (2021). *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression*. Freedom House [Report].

https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf

Schiff, M., Benbenishty, R., McKay, M., DeVoe, E., Liu, X., & Hasin, D. (2006). Exposure to Terrorism and Israeli Youths' Psychological Distress and Alcohol Use: An Exploratory Study. *American Journal on Addictions, 15*(3), 220–226. https://doi.org/10.1080/10550490600626200

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

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Schmitt, M. N. (2018). International Cyber Norms: Reflections on the Path Ahead. *Netherlands' Military Law Review, 111*(12). https://puc.overheid.nl/mrt/doc/PUC_248137_11/

Shandler, R., & Gomez, M. A. (2022). The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics*, 1–16. https://doi.org/10.1080/19331681.2022.2112796

Shandler, R., Gross, M. L., & Canetti, D. (2023). Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis. *Journal of Global Security Studies 8*(1). https://doi.org/10.1093/jogss/ogac042

Sherman, J. (2021). *Reassessing RuNet: Russian internet isolation and implications for Russian cyber behavior*. Atlantic Council [Report]. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior/

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar*. Oxford University Press. https://doi.org/10.1093/wentk/9780199918096.001.0001

Slantchev, B. L. (2005). Introduction to International Relations Lecture 8: Deterrence and Compellence. *Department of Political Science, University of California*. https://web.archive.org/web/20180209125507/http://slantchev.ucsd.edu/courses/ps12/08-deterrence-and-compellence.pdf

Sleat, M. (2017). Just cyber war?: Casus belli, information ethics, and the human perspective. *Review of International Studies,* 44(2), 324–342. https://doi.org/10.1017/s026021051700047x

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly, 12*(3), 90-113. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Smeets.pdf

Sologub, R. (2019). Two Years After NotPetya. Cyberattacks Don't Stop for a Moment. *ISSP Global.* https://www.issp.com/post/two-years-after-notpetya-cyberattacks-don-t-stop-for-a-moment

Stanovaya, T. (2023). Russia's New Conscription Law Brings the Digital Gulag Much, Much Closer. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/politika/89553

Stevens, T. (2015). *Cyber Security and the Politics of Time*. Cambridge University Press.

Tadjbakhsh, S. (2014). *Human security Twenty Years On*. Norwegian Peacebuilding Resource Centre (NOREF) [Expert Analysis]. https://www.files.ethz.ch/isn/181368/540cb240aa84ac7133bce008adcde01f.pdf

Tagliavini, H. (2009). *Report of the Independent International Fact-Finding Mission on the Conflict in Georgia.* Council of the European Union, Vol. I. https://www.echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf

The European Center for Not-for-Profit Law (ECNL), the International Network of Civil Liberties Organizations (INCLO) & Privacy International (PI). (2022). *Under Surveillance: (Mis)use of Technologies in Emergency Responses.* Privacy International Organization. https://privacyinternational.org/report/5003/under-surveillance-misuse-technologies-emergency-responses-global-lessons-covid-19

The White House (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* [Report]. https://apps.dtic.mil/sti/pdfs/ADA543951.pdf

Torres, G. (2018). State Violence. In Treviño, A. J. (Ed.). *The Cambridge Handbook of Social Problems* (381-398). Cambridge University Press.

Tsourapas, G. (2021). Global Autocracies: Strategies of Transnational Repression, Legitimation, and Co-Optation in World Politics. *International Studies Review, 23*(3), 616–644. https://doi.org/10.1093/isr/viaa061

U.S Department of Justice (2018). North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions. [Press Release]. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

United Nations Generally Assembly Resolution 3314. *Definition of Aggression*, A/RES/3314 (14 December 1974). Article 1 https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/PDF/NR073916.pdf?OpenElement

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: cyber conflict in the international system*. Oxford University Press.

Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.

Vijaykumar, D. (2021). Offensive Cyber Operations: A Double-Edged Sword. *Ethical Tech*. https://ethicaltech.duke.edu/2021/03/30/offensive-cyber-operations-a-double-edged-sword/

Walker, S. (2016). Murder in Istanbul: Kremlin’s hand suspected in shooting of Chechen. *The Guardian*. https://www.theguardian.com/world/2016/jan/10/murder-istanbul-chechen-kremlin-russia-abdulvakhid-edelgireyev

Way, L. A., & Levitsky, S. (2006). The Dynamics of Autocratic Coercion after the Cold War. *Communist and Post-Communist Studies, 39*(3), 387–410. https://doi.org/10.1016/j.postcomstud.2006.07.001

Weber, M. (2015). *Politics as Vocation* (Waters, T. & Waters, D., Trans.) Palgrave Macmillan. (1919).

White, S. P. (2018). Understanding Cyberwarfare Lessons from the Russia-Georgia War. *Modern War Institute*. https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf

Wittes, B., & Blum, G. (2016). *The Future of Violence - Robots and Germs, Hackers and Drones*. Amberley Publishing Ltd.

Woodhams, S. (2020). COVID-19 Digital Rights Tracker. *Top10VPN*. https://www.top10vpn.com/news/surveillance/covid19-digital-rights-tracker/ .

Woodlock, D., McKenzie, M., Western, D., & Harris, B. (2019). Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control. *Australian Social Work, 73*(3), 368–380. https://doi.org/10.1080/0312407x.2019.1607510

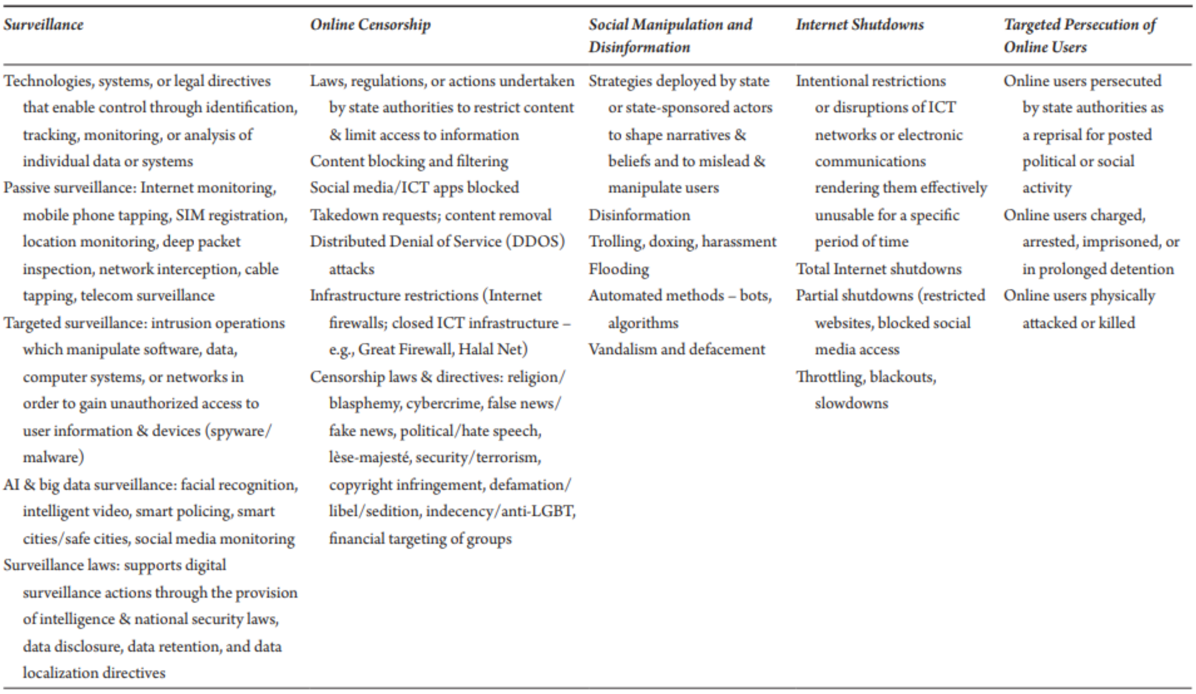
World Health Organization (WHO). (2022). WHO Violence Prevention Unit: approach, objectives and activities, 2022-2026. [Publication]. https://www.who.int/publications/m/item/who-violence-prevention-unit--approach--objectives-and-activities--2022-2026

Zuboff, S. (2018). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

ANNEXES

Annex I

EXPLANATION OF THE 5 TYPES OF DIGITAL REPRESSION

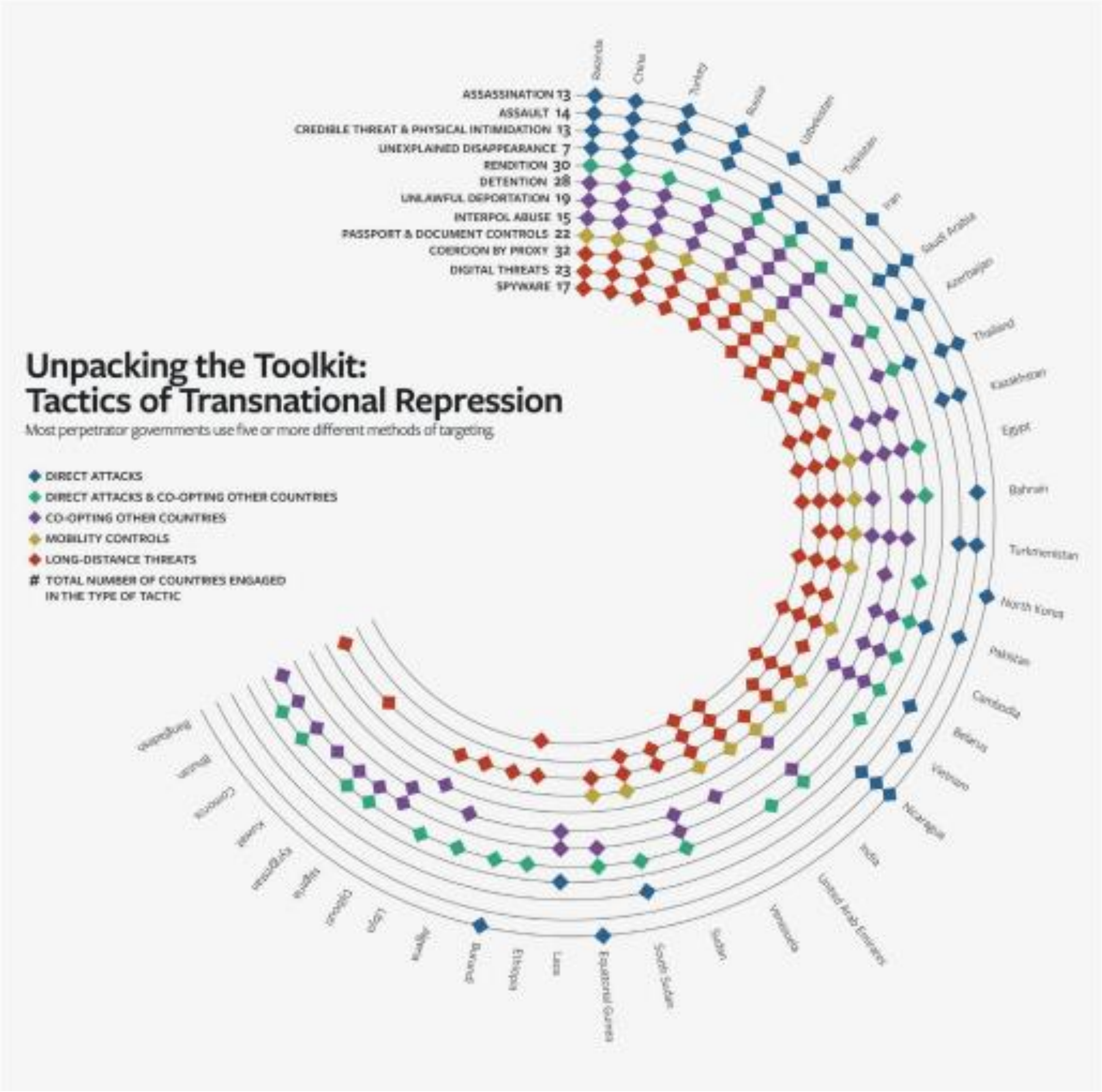


Surveillance	*Online Censorship*	*Social Manipulation and Disinformation*	*Internet Shutdowns*	*Targeted Persecution of Online Users*
Technologies, systems, or legal directives that enable control through identification, tracking, monitoring, or analysis of individual data or systems Passive surveillance: Internet monitoring, mobile phone tapping, SIM registration, location monitoring, deep packet inspection, network interception, cable tapping, telecom surveillance Targeted surveillance: intrusion operations which manipulate software, data, computer systems, or networks in order to gain unauthorized access to user information & devices (spyware/malware) AI & big data surveillance: facial recognition, intelligent video, smart policing, smart cities/safe cities, social media monitoring Surveillance laws: supports digital surveillance actions through the provision of intelligence & national security laws, data disclosure, data retention, and data localization directives	Laws, regulations, or actions undertaken by state authorities to restrict content & limit access to information Content blocking and filtering Social media/ICT apps blocked Takedown requests; content removal Distributed Denial of Service (DDOS) attacks Infrastructure restrictions (Internet firewalls; closed ICT infrastructure – e.g., Great Firewall, Halal Net) Censorship laws & directives: religion/blasphemy, cybercrime, false news/fake news, political/hate speech, lèse-majesté, security/terrorism, copyright infringement, defamation/libel/sedition, indecency/anti-LGBT, financial targeting of groups	Strategies deployed by state or state-sponsored actors to shape narratives & beliefs and to mislead & manipulate users Disinformation Trolling, doxing, harassment Flooding Automated methods – bots, algorithms Vandalism and defacement	Intentional restrictions or disruptions of ICT networks or electronic communications rendering them effectively unusable for a specific period of time Total Internet shutdowns Partial shutdowns (restricted websites, blocked social media access Throttling, blackouts, slowdowns	Online users persecuted by state authorities as a reprisal for posted political or social activity Online users charged, arrested, imprisoned, or in prolonged detention Online users physically attacked or killed

Source: Feldstein (2021, p. 26)

Annex II

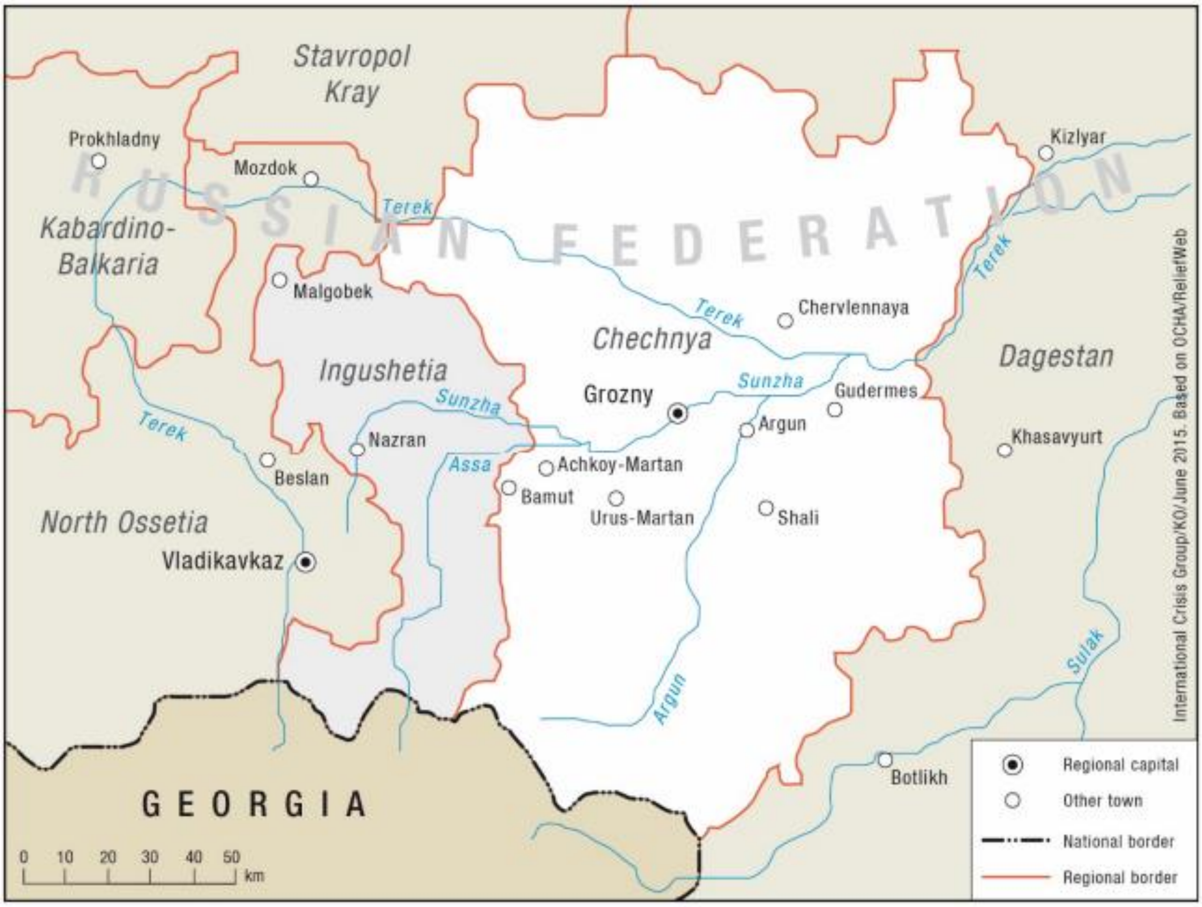
MAIN ACTORS AND TACTICS OF TRANSNATIONAL REPRESSION



Source: Gorokhovskaia *et al*. (2023, p. 4).

Annex III

MAP OF CHECHNYA



Source: ICG (2015, p. 40)

– End of Document –