Cyber Warfare & Influence Operations as Threats to Democratic Freedom

by David Popper

Submitted to
Central European University Undergraduate Studies Department

In partial fulfillment of the requirements for the degree of Bachelor of Culture, Politics and Society

Supervisor: Alexios Antypas

Budapest, Hungary 2025

Copyright Notice

Author's declaration

I, the undersigned, David Popper, declare herewith that the present thesis is exclusively my own work, based on my research and only such external information as properly credited in notes and bibliography. I declare that no unidentified and illegitimate use was made of the work of others, and no part of the thesis infringes on any person's or institution's copyright. I also declare that no part of the thesis has been submitted in this form to any other institution of higher education for an academic degree.

Budapest, 17 June 2025

David Popper

Signature

Abstract

This thesis critically examines the evolving role of cyber warfare (CW) and information operations (IOs) in shaping national security, political stability, and public trust. As cyberspace becomes a key battleground for both state and non-state actors, conventional models of warfare and deterrence prove increasingly inadequate. The research highlights how cyber capabilities are integrated into broader geopolitical strategies, often preceding or replacing traditional military action. It investigates the legal and ethical ambiguities surrounding state-sponsored cyberattacks and digital surveillance, especially the complicity of private companies in enabling authoritarian regimes through the unregulated trade of cyberweapons.

The thesis argues that existing international legal frameworks fail to address the borderless, asymmetric nature of cyber threats, allowing perpetrators to act with impunity. By comparing case studies, including attacks on critical infrastructure and democratic processes, the work underscores the urgent demand for globally coordinated norms and stronger regulatory mechanisms. Special attention is paid to the role of democracies in setting ethical standards, regulating private sector involvement, and communicating the tangible impacts of cyber threats to the public.

Ultimately, the thesis calls for a multidimensional response: demystifying public understanding of cyberattacks and developing implementable international agreements. Drawing from literature in international law, security studies, and digital governance, the study concludes that only through cooperation, transparency, education, and political will can democratic societies preserve control over cyberspace.

List of abbreviations:

CS = Cyber Space
CW = Cyber Warfare

CySec = Cyber Security

IO = Influence Operations

Table of Contents

CHAPTER I - Cyber Warfare and Influence Operations: Definitions and Methods...................... 1

1.1 Introduction 1

1.2 The Evolution of CW: Historical Context 3

1.3 Tactics and Methods of CW 4

1.4 Influence Operations (IOs) 5

1.5 Key Trends in CW during the Past 15 Years 8

1.6 Hybrid Warfare and Geopolitical Impact 9

1.7 Challenges in the Cyber Context 10

1.8 Analytical Frameworks: Rationalist, Legal, and Humanitarian Approaches 11

1.9 Evolving Literature and Critiques 12

Chapter II – Impact of CW and IOs on National Security, Political Stability, and Public Trust: Evaluating the Adequacy of Current International Legal Frameworks 14

2.1 CW's Impact on National Security 14

2.2 Legal Aspects of CW and the Tallinn Manual 14

2.3 State Responsibility and Cyber Due Diligence 15

2.4 Critiques and Future Directions 15

2.5 Deterrence in the Cyber Domain 16

2.6 Strategic Debate: CW’s Role in Modern Conflict 16

Chapter III – Strategies to Mitigate Damage from Cyber Threats 19

3.1 Offense-Dominant Nature of CW 19

3.2 Cyber Defense Strategies 20

3.3 Offensive Cyber Capabilities and Pegasus case-study 21

3.4 Role of Corporations, International Alliances and Education in Addressing Cyber Threats and Enhancing Cybersecurity Measures 23

Conclusion 27

Full bibliography 29

Appendix 32

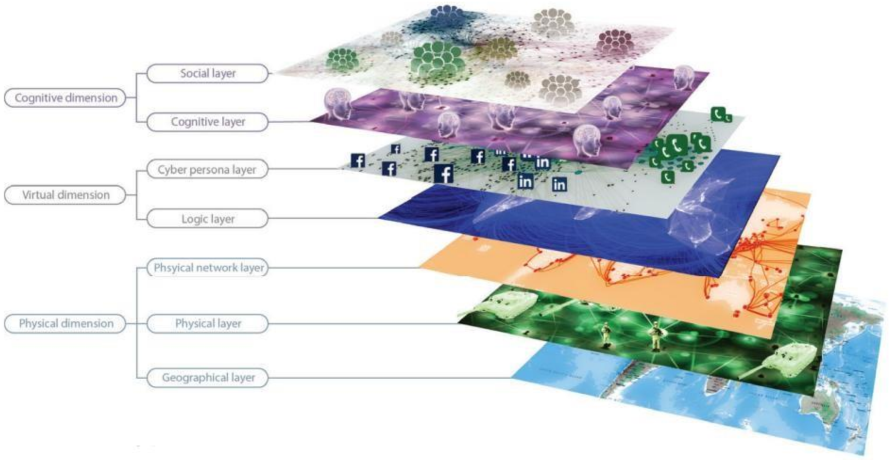
CHAPTER I - Cyber Warfare and Influence Operations: Definitions and Methods

1.1 Introduction

CW refers to state or state-sponsored conflicts conducted within CS, defined as "the global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (NIST, 2021), typically aimed at disrupting, damaging, or destroying governmental, military, or critical civilian infrastructure (Green, 2016, p. 8). It is distinct from cyberterrorism and cybercrime, although overlaps exist in tactics and methods. According to Even & Siman-Tov (2012, p.10) CW targets three primary layers of CS: the physical layer, which includes attacks on hardware infrastructure such as routers, servers, and data centers; the syntactic/logical layer, which exploits vulnerabilities in software and systems through malware, hacking, and network intrusions; and the semantic layer, which manipulates human perception through misinformation campaigns, phishing, and social engineering tactics. Each of these layers presents unique vulnerabilities and requires distinct defensive strategies.

Figure 1. Layers of CS

Source: van Haaster, J., 2019. On cyber: The utility of military cyber operations during armed conflict. Universiteit van Amsterdam, p.184. Figure 26



Although cyberattacks have become more well-known in the twenty-first century, their theoretical underpinnings date back many years. The strategic implications of digital technologies in military operations were examined in the early talks of information warfare in the late 20th century. Organizations such as the RAND Corporation, which studies the potential of cyber weapons, and articles such as Arquilla & Ronfeldt's (1993) groundbreaking "Cyberwar is coming!" laid the groundwork for the current discussion on cyber conflict. The latter contended that this "new type of warfare" would fundamentally alter interstate conflict from what has previously happened. Early electronic warfare, which utilized radio and radar interruptions, gave rise to modern CW. Cyber operations became a crucial part of national security plans as technology developed (Green, 2016, p. 7). Over time, CW has evolved from basic espionage to highly sophisticated operations capable of crippling financial systems, critical infrastructure, and government networks.

CS has been formally recognized as a crucial area for military and national security operations—often referred to as the "fifth domain" after land, sea, air, and space (Clarke & Knake, 2019).

In order to accomplish strategic goals, CW now plays a crucial part in hybrid warfare, which combines conventional military tactics with online operations. Cyberattacks can have more subtle effects like espionage and information manipulation, or more obvious ones like power grid outages. States progressively included cyber operations into their larger defense and intelligence plans as cyber capabilities improved.

1.2 The Evolution of CW: Historical Context

As stated by Rafi (2023, p.109), the development of CW can be traced through distinct phases. The early cyber espionage incidents starting with the 1986 Cuckoo's Egg case defined the realization phase which focused on intelligence collection and reconnaissance activities. The take-off phase brought more sophisticated cyberattacks into play when the 1999 Moonlight Maze operation targeted U.S. government networks. The modern militarization phase introduced cyberattacks, which could cause physical destruction, proving the escalating nature of cyber operations and that they had evolved from reconnaissance tools into offensive capabilities, producing significant geopolitical effects.

Several landmark incidents illustrate this rapid evolution of CW (Edelman, 2024, pp 34-36). The 2007 Estonia cyberattack, which Russia allegedly conducted, caused extensive damage to Estonia's digital infrastructure and financial sector, making it a notable nation-state cyber attack. The 2010 Stuxnet operation, which (allegedly) the U.S. and Israel jointly conducted against Iran's nuclear enrichment facilities, proved that CW could serve as a strategic statecraft instrument. The 2012 Shamoon attack on Saudi Aramco revealed the destructive capabilities of cyber operations through its destruction of essential data. The 2015 Ukrainian power grid attack, which Russian state actors conducted, demonstrated the real-world effects of CW by leaving hundreds of thousands without electricity. The 2022 Russian cyberattacks against Ukraine demonstrate how cyber operations have become integral to the traditional military strategy, thus merging digital warfare with physical combat. These incidents demonstrate both the offensive capabilities of CW and its function as a strategic deterrent and coercive instrument in international relations.

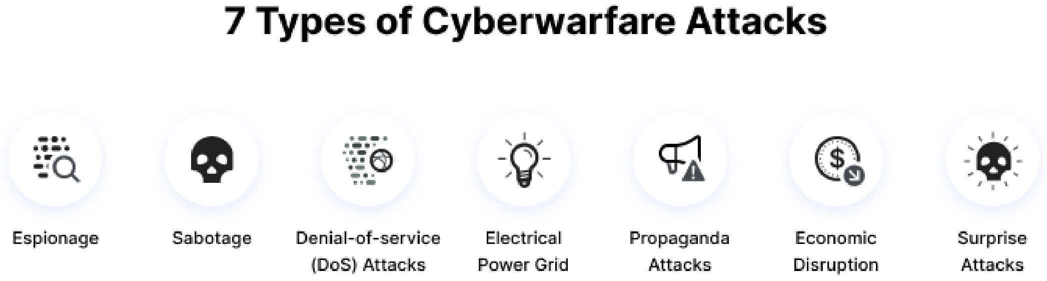
1.3 Tactics and Methods of CW

Modern CW includes various tactics, such as cyber espionage, cyber sabotage, cyber information warfare, and the use of ransomware and malware. Cyber espionage involves infiltrating networks to steal sensitive data, primarily targeting military, corporate, or national security infrastructures. These incidents are primarily focused on intelligence gathering, rather than causing direct harm, and may include reconnaissance efforts or data collection aimed at acquiring sensitive information without disruption or destruction. On the other hand, cyber sabotage seeks to directly damage or disable critical systems, with attacks like Stuxnet and Shamoon serving as prime examples. These attacks aim to destroy infrastructure and disrupt the functioning of key sectors (Slonopas, 2024).

Cyber information warfare involves disrupting or manipulating the flow of information to confuse or deceive both governments and citizens. This often includes social engineering tactics that influence public opinion, interfere with elections, or undermine trust in institutions. Social media platforms have amplified these efforts, enabling these campaigns to operate on a global scale (further discussed in the next section (1.4 IOs)).

Figure 2. 7 types of CW attacks

Sources: (7 types of Cyberwarfare attacks. (n.d.). Imperva. https://www.imperva.com/learn/wp-content/uploads/sites/13/2021/10/cyberwarfare.png



Ransomware and malware attacks lock critical data or systems until the victim pays a ransom, causing severe disruption, economic damage, or even harm to national security. Cyber attackers utilize a variety of methods to achieve their objectives, ranging from unauthorized access to networks to the deployment of viruses, malware, and sophisticated Distributed Denial of Service (DDoS) attacks that overload and incapacitate systems (Rafi, 2023, p. 112). These methods, which are designed by state-sponsored groups to create chaos, disrupt operations, and damage the reputation of targeted institutions, have further blurred the lines between criminal activity and political warfare.

Among the most dangerous and prevalent cyber threats is ransomware, which locks users out of their data and demands a ransom for its release. These attacks have become particularly destructive, as they target both private businesses and government entities, causing financial losses, damaging critical infrastructure, and disrupting public services. States such as North Korea and Iran have been reported to use ransomware attacks not only for financial gain but also as part of broader strategic goals, including spreading propaganda and exerting political influence (Slonopas, 2024). In these instances, cyberattacks act as tools to achieve multiple objectives simultaneously, making it harder to pinpoint motives and tactics. The increasing frequency and sophistication of ransomware attacks indicate a growing risk to both national security and economic stability.

1.4 Influence Operations (IOs)

IOs are another powerful tool used by states and non-state actors to shape public opinion, alter behaviors, or manipulate perceptions for strategic goals. These operations are aimed at creating a specific political or social narrative, and they can have far-reaching impacts on political decisions, elections, and public trust. Foreign influence efforts, information, and political warfare involve using all available means, except direct military action, to achieve national objectives through non-violent means like propaganda, subversion, and diplomacy.

An influence operation can be described as "the deployment of resources for cognitive ends that foster or change a targeted audience's behaviour" (Hollis, 2018, p. 36), directly or via changing the attitude (Pijpers, 2024, p. 6-7). In other words, these operations aim to alter the cognitive and psychological processes and attitudes of a target audience, often with the goal of furthering national interests. In the context of CS, IOs are particularly challenging, as they may involve subtle forms of interference, such as altering voters' perceptions without resorting to violence. This however, can involve methods like persuasion, manipulation, deception, and even coercion.

IOs have evolved significantly with the rise of online platforms, particularly social media, which allows for the amplification of messages and manipulation of public sentiment on a global scale. These operations can take various forms:

Disinformation Campaigns: Spreading false or misleading information to confuse, mislead, or sway public opinion. This is commonly seen during elections or in political crises.

Social Media Manipulation: Creating fake accounts or using automated bots to flood social media with messages that promote specific narratives or suppress opposition.

Psyops/Perception Management: Psychological operations that aim to influence the emotions, attitudes, and behaviors of target audiences, often used to destabilize or manipulate political environments.

While traditional military power (e.g., military forces and economic sanctions) is often used by states to project power, soft power—the use of cultural diplomacy, values, and information—has become a major component of statecraft and is characterized by persuasion, attraction, and non-coercive influence, contrasting with hard power tactics that rely on force or economic pressure (Nye, 2004, pp. 5–8, as cited in Bentzen, 2018, p.2).

In political science and international relations, the verb "to influence" refers to power dynamics between states, encompassing the ability to persuade others to align with one's desires or to prevent them from acting against those interests (Pijpers, 2024, p. 6.) Authoritarian regimes, which often lack strong soft power resources, frequently turn to cyber tactics to weaken democratic institutions and destabilize societies (Deibert, 2015, pp. 64–78).

IOs exploit the rapid, borderless nature of the internet, leveraging anonymity and low-cost communication channels to manipulate information and alter perceptions globally. CS offers unique advantages for IOs, such as the speed and anonymity of online interactions, as well as the lack of traditional authority structures (Center for Security Studies, 2019, p.13). This environment encourages more aggressive tactics, as the absence of clear hierarchies allows for a wider range of actors to engage in influencing behaviors.

From a legal perspective, the threat of force in international relations is governed by the principles of jus ad bellum, which dictate when states may lawfully resort to force as part of their foreign policy (Schmitt, 2017, p. 31). Despite their non-kinetic nature, these activities may still violate international legal principles, including state sovereignty and the prohibition against foreign intervention in domestic affairs (Schmitt, 2013, p. 45).

According to Pijpers (2024, p. 6), the rise of CS enables the targeting of highly specific social groups. This is partly due to the accessibility of their data through the internet and social media and partly because big data and data science tools allow for precise identification. Consequently, these groups can be reached with tailored messages delivered in familiar language and through their preferred communication platforms. While such micro-targeting methods can encourage participation in political or social discussions, they can also foster disengagement and deepen societal divisions. Or, as stated by Nimmo (2020, p. 4), "The most dangerous influence operations will be those that show the greatest ability to spread to many different communities, across many platforms, and into real-life discourse."

1.5 Key Trends in CW during the Past 15 Years

According to Edelmann (2024, pp. 40-52), in recent years the following trends became visible in CW:

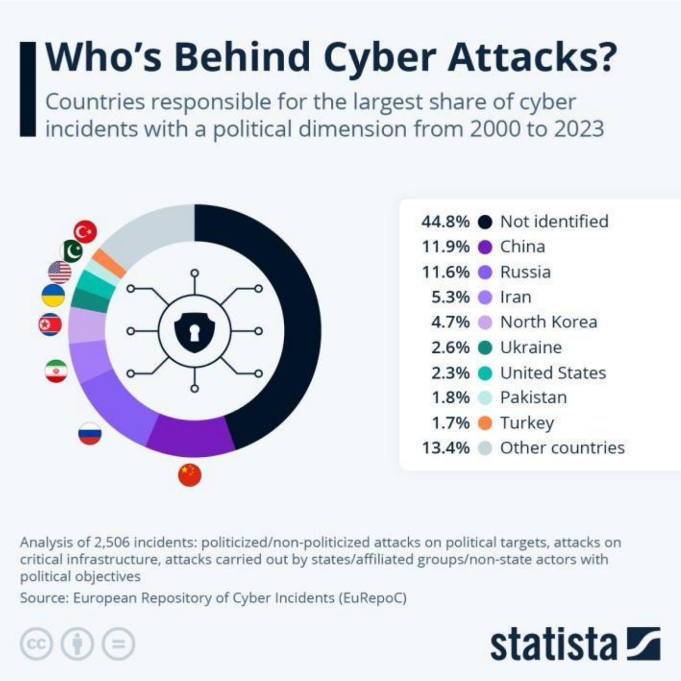
The Nature of CW: CW is sometimes misunderstood as a separate type of warfare that exists outside of conventional military strategy. Rather, cyber operations are usually included into more comprehensive military plans, supplementing or bolstering traditional methods. Cyber capabilities are used by states to thwart enemy operations or get ready for physical wars. Furthermore, weaker powers use cyberattacks to harm stronger opponents in asymmetric battles rather than directly confronting them militarily. Although acts of war are governed by current legal frameworks, the swift development of cyber capabilities calls into question the application of these laws, requiring explicit standards and guidelines in CS.

State Actors Dominate: Nation-states remain the primary perpetrators of cyberattacks, using cyber tools for espionage and coercion.

Attribution Challenges: While technology has improved the ability to identify cyberattack sources, attribution is often delayed, complicating state responses. Attribution issues arise on multiple levels, including technical identification of the perpetrators, legal accountability, and political considerations. While technical investigations can trace cyber intrusions, legal attribution is more complicated and requires evidence of harm or violations of international law, which may be ambiguous or difficult to establish in CS. Moreover, political factors often determine whether a state will publicly attribute an attack, with considerations about preserving covert actions or avoiding diplomatic fallout (Maurer, 2018, p. 104).

Figure 3. Attribution of cyberattacks from 2020 to 2023

Source: Fleck, A. (2024). Who’s Behind Cyber Attacks?. Statista. statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/.



Who’s Behind Cyber Attacks?

Countries responsible for the largest share of cyber incidents with a political dimension from 2000 to 2023

Analysis of 2,506 incidents: politicized/non-politicized attacks on political targets, attacks on critical infrastructure, attacks carried out by states/affiliated groups/non-state actors with political objectives

Source: European Repository of Cyber Incidents (EuRepoC)

The Role of Private Companies: Private entities are increasingly present in cysec, acting as both defenders and targets. Companies provide advanced cysec tools and services, often outpacing governmental responses. Additionally, private firms have assumed roles in attribution, challenging state monopoly and geopolitical implications.

1.6 Hybrid Warfare and Geopolitical Impact

CW and IOs are increasingly intertwined with traditional forms of military and geopolitical strategy, creating what is known as hybrid warfare. Hybrid warfare combines conventional military tactics with cyber and information warfare to achieve strategic objectives (NATO, 2024). For instance, Russia’s interference in the 2024 Moldovan presidential election through disinformation campaigns and cyberattacks is a prime example of hybrid warfare tactics, using both cyber means and IOs to achieve political gains (Harvey, 2025).

As the line between digital and physical warfare continues to blur, CW impacts not only individual nations but also the global economy. Attacks on one nation’s critical infrastructure can have ripple effects across international systems, such as financial markets, supply chains, and multinational companies. The interconnectedness of the global economy means that the consequences of a cyberattack in one country can extend far beyond its borders.

In response, many nations are building cyber defense capabilities and forming international partnerships to strengthen collective defense against cyber threats (Choucri, 2012, pp. 9-16). Countries are investing in advanced technologies and strategies to safeguard critical infrastructure, ensure national security, and maintain control over their digital sovereignty.

1.7 Challenges in the Cyber Context

Novelty and Rapid Change: Continuous technical innovation, which produces new vulnerabilities and adversary strategies, is what defines the cyber landscape. This ongoing change makes establishing standards and formulating policies more difficult. (Nye, 2016, pp. 10–12).

Data Scarcity: Since a large portion of the crucial information about cyberattacks is classified or confidential, there is little publicly available data on state behaviors in CS. Comprehensive examination and comprehension of state actions are hampered by this lack of transparency (Tsagourias & Buchan, 2015, pp. 55–56).

Despite these challenges, valuable sources of information exist, such as cysec reports from companies like CrowdStrike and FireEye, state cysec policies, and international agreements that provide guidelines for behavior in CS.

1.8 Analytical Frameworks: Rationalist, Legal, and Humanitarian Approaches

Understanding cyberattacks requires considering multiple theoretical and legal perspectives:

Rationalist Deterrence: This framework draws heavily from Cold War deterrence theory, applying it to the cyber domain. Deterrence in CS involves states calculating the potential costs of cyberattacks, often leveraging the threat of retaliatory measures to discourage adversaries. Deterrence also relies on the idea that mutual restraint in CS can prevent escalation and conflict (Edelman, 2024, pp. 90-93).

International Law: Interpretations of international law, particularly the UN Charter and rulings from the International Court of Justice (ICJ), provide a foundation for regulating state behavior in CS. However, the exact application of concepts like sovereignty and use of force to cyberattacks remains debated (Schmitt, 2013, pp 7-10).

Humanitarian Norms: Cyberattacks, especially those targeting civilians, are increasingly examined through the lens of international humanitarian law. Precedents set by treaties banning chemical weapons and landmines are used to explore how similar norms could govern cyberattacks on civilian infrastructure such as hospitals or power grids (Gisel et al, 2020, p.2) (Schmitt, 2013, pp. 139–145).

1.9 Evolving Literature and Critiques

Critiques of early literature noted a tendency to overgeneralize the term "cyber warfare." Scholars like Ben Buchanan and Joseph Nye have contributed to a more detailed understanding by emphasizing the need for responsible state behavior in CS and proposing frameworks for deterrence that extend beyond traditional military strategies (Buchanan, 2017, pp. 5–10; Nye, 2016, pp. 22–25).

Legal scholarship has also evolved, with significant contributions from authors like Oona Hathaway (Hathaway et al, 2011). In recent years, the field has expanded with publications from contributors like Michael Schmitt, notably the Tallinn Manuals (2013 and 2017), which seek to apply existing laws of armed conflict to cyber operations. These manuals have become central references for analyzing the application of international law to cyberattacks. Nevertheless, achieving legal consensus on cyber norms remains a significant challenge (Schmitt, 2013, pp. 9–10). Other criticisms of the field include the slow policy process and fragmented interpretations among military and government lawyers.

David E. Sanger's The Perfect Weapon (2018) examines how cyber capabilities have become central to modern statecraft, enabling nations to wage covert campaigns with strategic impact. It details high-profile operations like Stuxnet and Russian interference in U.S. elections, emphasizing the geopolitical consequences of unregulated cyber activity.

The late 2000s shifted the narrative to viewing cyberattacks primarily as national security threats, ignited by incidents such as the 2007 Estonia cyberattacks (Clarke & Knake, 2010, pp. 60–65). Influential works, including Richard Clarke and Robert Knake's Cyber War, highlighted the risks associated with state-sponsored cyberattacks, although they often lacked clear definitions and theoretical frameworks.

Their other book, The Fifth Domain (2019) offers a practical analysis of cysec policy, stressing that the digital realm has become the "fifth domain" of warfare. The authors advocate for stronger public-private cooperation and clearer cyber norms, highlighting how resilience—not just retaliation—is key to defense.

Investigative journalism also played a role in illuminating specific cyber incidents but frequently fell short of providing broader theoretical context. This gap in the literature prompted subsequent investigators to refine the language and frameworks used to analyze cyber conflicts, integrating insights from international relations and law. An influential work in this realm is Nicole Perlroth's This Is How They Tell Me the World Ends (2021), which investigates the opaque market for zero-day exploits and the rise of cyberweapons. Based on her professional reporting, the book reveals how a lack of regulation has allowed governments, hackers, and corporations to operate with impunity, raising ethical and security concerns.

Chapter II – Impact of CW and IOs on National Security, Political Stability, and Public Trust: Evaluating the Adequacy of Current International Legal Frameworks

2.1 CW's Impact on National Security

To reiterate the arguments made so far, CW has emerged as one of the most significant threats to national security and essential infrastructure in the current era. With society becoming increasingly reliant on online systems and networks for critical sectors like energy, finance, and government, the possible vulnerabilities to cyberattacks have multiplied. State and non-state actors now target these systems to disrupt services, steal sensitive data, and cause lasting damage to infrastructure. The potential consequences of these attacks are far-reaching, not just within the affected nation but also globally, given the interconnected nature of modern economies and communications. Cyberattacks can breach government systems and military networks, undermining state stability and national defense. In delicate times such as elections, cyberattacks can be particularly devastating as they target government networks, manipulate public opinion, spread misinformation, and disrupt communications. These tactics weaken public trust in democratic institutions and increase political polarization. Because cyberattacks are frequently undetectable, they pose a serious threat to public trust in the legitimacy of democratic processes.

2.2 Legal Aspects of CW and the Tallinn Manual

As the scale and scope of cyberattacks continue to grow, addressing the legal and ethical aspects of cyber warfare becomes increasingly crucial. Current international laws, such as Article 2(4) of the UN Charter, which prohibits the use of force against other states, do not provide clear guidance on how these laws apply to cyber operations (Hathaway and Crootof, 2012, p. 842).

The ambiguity of these laws creates challenges for states seeking to respond appropriately to cyberattacks. In particular, the principle of non-intervention, which prevents foreign interference in a state's internal affairs, is often difficult to enforce in CS (Schmitt, 2013, p. 46-47).

CW also blurs the line between jus ad bellum (laws governing the use of force) and jus in bello (laws governing conduct during conflict). Scholars continue to debate how these traditional frameworks apply to cyber aggression and whether cyberattacks can be considered "armed attacks" under international law. The Tallinn Manual, a leading guide on the laws of CW, suggests that traditional legal frameworks can apply to cyber activities, emphasizing state sovereignty and accountability (Schmitt, 2013, p. 25-43). However, the lack of consensus among nations on how to regulate cyber warfare leaves many legal issues unresolved.

2.3 State Responsibility and Cyber Due Diligence

One perspective that has gained traction is the concept of cyber due diligence which holds states accountable for preventing harmful cyber activities originating within their borders (Green, 2016, pp.118-120). This framework suggests that rather than focusing on attribution, states should be responsible for ensuring that cyberattacks do not emanate from their territory. However, this approach faces challenges in terms of enforcement, as proving the origin of cyberattacks remains difficult. Moreover, ensuring that states take adequate preventive measures may require significant international cooperation and transparency

2.4 Critiques and Future Directions

Advocating for restraint may unintentionally weaken the strategic stance of states that adhere to such norms, potentially destabilizing their security situation. However, Edelman argues that states generally practice restraint in CS, avoiding large-scale attacks likely due to deterrence or adherence to legal frameworks (Edelman, 2024, p. 59).

Critics of this approach suggest that focusing too much on large-scale cyber attacks overlooks the significant risks posed by "gray zone" activities, which can disrupt national security without crossing the threshold of war (Kello, 2017, p. 249). While some proponents of cyber operations argue they may reduce human suffering compared to traditional warfare, the long-term impacts of cyberattacks on society raise ethical concerns that should be addressed (Denning & Strawser, 2014 p. 5).

2.5 Deterrence in the Cyber Domain

A significant issue in cysec is the effectiveness of deterrence. Traditional models of deterrence, rooted in the notion of retaliation, may not apply effectively in CS due to the anonymity and attribution challenges of cyber operations. According to Edelman (2024, pp. 90-93.), the aforementioned theory of rationalist deterrence posits that states weigh the potential gains against losses before launching cyberattacks. While this approach has historical roots in Cold War deterrence, its application to cyber conflict is complicated by the unique characteristics of cyber operations. Furthermore, deterrence does not guarantee long-term stability, as evidenced by proxy conflicts arising from mutual deterrence during the Cold War. Misattribution or miscommunication in cyber conflict may also lead to unintended escalations.

2.6 Strategic Debate: CW's Role in Modern Conflict

The covert nature of CW complicates its strategic use. Cyber operations, such as those seen in the Estonia and Ukraine conflicts, often operate in the background of conventional military strategies, providing support but rarely serving as a decisive factor in achieving political or military objectives. In this sense, CW acts more as a "tool of mass disruption" rather than a weapon that can lead to conclusive victories or strategic outcomes, similarly to early air power, suggesting that while cyber operations can be highly disruptive, they are unlikely to replace traditional military force in achieving political goals (Green, 2016, p. 91).

Cyber incidents often lead to responses that do not escalate to traditional warfare. States may impose economic sanctions or pursue diplomatic avenues in retaliation for cyberattacks (Singer and Friedman, 2014, p. 167). This approach allows for maintaining international stability while addressing cyber threats. Criminal indictments against individuals or groups involved in cybercrimes serve as another non-kinetic response, balancing accountability with geopolitical considerations.

However, governments' ability to respond to these threats is often hindered by the anonymous nature of cyber operations, as attribution remains difficult—not only due to sophisticated techniques to hide their origins but also because many states deny involvement and instead attribute such acts of cyber aggression to independent or non-state actors (Green, 68-70).

In the context of international law, states are held accountable for activities occurring within their borders, similar to obligations related to counterterrorism. The framework proposed by Healey (2011) outlines different levels of state involvement, ranging from prohibited cyber activities to state-led operations.

Experts such as Ranum (2011) suggest that transparent attribution could help build credibility in cyber conflict scenarios. One proposal to address this issue includes using identification codes in data packets, although this solution has its limitations (Green, 2015, p.69).

The strategic significance of CW remains a matter of debate. Some experts view cyber warfare as a transformative force in modern conflict (Stone, 2013), fundamentally altering the nature of warfare, while others argue it is an exaggeration or merely a complement to traditional forms of warfare (Rid, 2013). Several key incidents provide critical insights into the evolving role of cyberattacks in warfare.

For example, the cyberattacks on Georgia (2008) demonstrated how cyber operations could be used to disrupt government functions and debilitate entire nations (Green, 2016, pp.18-20). The Stuxnet (2010) incident, in particular, represents a pivotal moment in the evolution of CW. The operation conducted by Unit 8200 within the Israeli army, which targeted Iran's nuclear infrastructure, highlighted the ability of cyber weapons to cause significant kinetic damage (Zetter, 2014, pp. 172–174). It demonstrated that cyber weapons could be designed not just for espionage or disruption but also for sabotage, capable of directly impairing the functionality of critical national infrastructure; in this case it damaged Iran's nuclear centrifuges and slowed its uranium enrichment activities (Zetter, 2014, pp. 175–178). This marked a significant shift, where cyber operations evolved from being largely informational to having the potential to cause physical harm, placing them on par with conventional military tools.

Chapter III – Strategies to Mitigate Damage from Cyber Threats

3.1 Offense-Dominant Nature of CW

CW presents unique challenges for both attackers and defenders. As claimed by Gartzke (2015, 343-347), cyber attackers must contend with cyber defenses and an evolving offense-defense cycle, but the offense generally holds the upper hand. Defenders face a daunting task, as they must safeguard vast networks that are inherently vulnerable and operated by fallible human users. Attackers often have the advantage since they need only one successful breach to impact large, vulnerable networks, while defenders must maintain constant vigilance (Karabacak et al, 2016 in Asbas, 2023, p. 134). This offense-defense imbalance is exacerbated by human errors and the inherent vulnerabilities of online systems, creating a perpetual struggle for those tasked with cysec.

This is a particularly relevant phenomenon in the case of zero-day vulnerabilities, which are a type of software attack tool that has never been used before and for which, therefore, no defense currently exists. A zero-day attack tool is an exploit that utilizes a previously unused vulnerability in software or hardware.

Another distinct characteristic of CW is the difficulty in distinguishing between legitimate and lawful combatants and civilian involvement in state-level conflicts (Sheldon, 2024). Unlike traditional warfare, where the identity of participants is more clear-cut, the low barriers to entry allow civilians with the requisite skills to participate in cyberattacks. Generally, cyberattacks are considered less expensive than other attack types (Karabacak et al, 2016 in Asbas, 2023, p. 134), since the technologies required are widely available and mostly open-source. Because of the wide accessibility, the amount of potential attackers multiplies, resulting in a large number of suspects.

Civilians can access software and tools that allow them to carry out cyberattacks against state agencies, NGOs and individual targets, potentially complicating their legal status under the international laws of armed conflict, such as the Geneva Conventions. For instance, cyber attacks against Estonia and Ukraine allegedly involved civilian participants (aka "hacktivists"), possibly motivated by nationalist sentiments. This ambiguity challenges the prosecution of CW cases and complicates defense measures. Hence, accountability issues are brought up by this phenomenon.

The anonymity provided by CS further interferes with defense efforts. Groups of attackers can mask their identity, location, and motives, making attribution harder and sometimes speculative. Again, the Estonia case illustrates this issue: despite suspicions of Russian involvement, solid evidence directly linking the Russian government is lacking (Sheldon, 2024). This anonymity hinders deterrence efforts, as uncertainty about the attacker's identity makes retaliation risky and increases the likelihood of targeting the wrong person or group .

3.2 Cyber Defense Strategies

In response to these threats, many nations are prioritizing cyber defense by establishing specialized military units and agencies. For instance, the United States has established the Twenty-fourth Air Force to defend Air Force networks, while the Navy has reformed its Tenth Fleet, or Fleet Cyber Command, for similar purposes (Lewis et al, 2011, pp. 21-22) . Both units work under U.S. Cyber Command and are responsible for overseeing all U.S. military cyber operations.

Similarly, the United Kingdom has set up the Cyber Security Operations Centre (CSOC) under the GCHQ, and France established its Network and Information Security Agency in 2009 to protect its digital infrastructure (Lewis et al, 2011, pp. 11-12, 20-21)

These structures focus on cysec essentials, including firewalls, encryption, network monitoring, and physical security, to defend critical infrastructure and maintain digital resilience.

3.3 Offensive Cyber Capabilities and Pegasus case-study

While most of the focus remains on cyber defense, the development of offensive cyber capabilities is also gaining attention According to Sheldon (2024), in Western countries, these offensive measures are typically regulated by law and primarily managed by intelligence agencies, such as the NSA in the United States and GCHQ in the United Kingdom. Although their use is often legally restricted, such capabilities continue to be developed within these frameworks. In contrast, countries like China and Russia appear to integrate offensive and defensive cyber capabilities more fluidly into their broader military and intelligence operations. In Russia, cyber activities are reportedly managed by institutions such as the Federal Security Service (FSB) and the Ministry of Defense (Connell & Vogler, 2017, pp. 7-8). Similarly, in China, entities such as the General Staff Department and various People's Liberation Army (PLA) militia units are believed to lead both defensive and offensive cyber operations, reflecting distinct approaches compared to Western models (Segal, 2016, pp. 93, 132).

The ethical implications of offensive cyber capabilities are demonstrated by controversies like the Pegasus spyware incident (Sheldon, 2024). Developed by the Israeli NSO Group, Pegasus was reportedly sold to government agencies under the pretense of combating crime. However, notably in Hungary, the spyware was used to monitor journalists, opposition figures, and activists, raising serious concerns domestically and beyond about privacy and abuse of power. In Hungary, despite evidence of political surveillance, no accountability followed, and investigations upheld the practice as legal without clarifying who was targeted.

In an interview conducted on May 11, 2025, with Ádám Remport, a lawyer at the Hungarian Civil Liberties Union (TASZ), critical legal and systemic shortcomings related to the Pegasus spyware scandal were brought to light (for full text, see Appendix). Remport emphasized that despite credible revelations about the use of NSO Group's Pegasus spyware against Hungarian journalists, political opponents, lawyers, activists, and businesspeople, no legal accountability or systemic reform has followed. According to Remport, this lack of consequences stems from a combination of legal ambiguity, lack of institutional independence, and political obstruction.

One key obstacle is that Hungary's intelligence services refuse to confirm or deny whether any individual is under surveillance, making it virtually impossible to establish state responsibility in court. Even when individuals attempt to seek redress, the relevant authority—the National Authority for Data Protection and Freedom of Information (NAIH)—offers limited transparency and typically rules that all actions were lawful without confirming whether surveillance even occurred. Remport noted that TASZ has submitted multiple individual complaints on behalf of affected clients, but all ended inconclusively.

Hungarian parliamentary oversight mechanisms are similarly ineffective. The National Security Committee (NB), tasked with holding intelligence services accountable, is effectively paralyzed by the governing party's parliamentary majority. This allows the government to block or delay investigations and renders the body structurally incapable of functioning as a check on executive power.

Beyond Hungary's borders, Remport pointed to the 2016 European Court of Human Rights (ECHR) ruling, which declared that surveillance authorization must come from an independent body, not a political actor like a government minister. Hungary has ignored this ruling, and the existing system continues to lack judicial oversight, complaint mechanisms, or any meaningful legal redress.

He underscores that the Pegasus case transformed long-standing abstract concerns about surveillance powers into tangible human rights violations, demonstrating the real-world impact of unchecked state surveillance.

TASZ is currently representing seven clients and pursuing every available domestic legal avenue. Their goal is twofold: to either achieve redress within the Hungarian system or to demonstrate the complete failure of domestic remedies, thereby justifying escalation to the ECHR. Remport further observed that similar litigation is occurring in other EU countries, such as Poland, pointing to a broader regional pattern.

On the question of legal reform, Remport advocated for changes at both the national and EU levels. While the General Data Protection Regulation (GDPR) excludes national security from its scope, he argues that cases like Pegasus surveillance should not be framed as "national security" but rather as rule-of-law issues, since they involve attacks on the constitutional functioning of democratic institutions. He sees this as a key legal reframing that could enable stronger EU intervention. The European Parliament’s inquiry committee on Pegasus has already issued recommendations, but Remport stressed that further steps are necessary to ensure democratic safeguards against digital surveillance abuse.

Overall, the Pegasus case underscores the potential for misuse of cyber tools, raising questions about the ethics of surveillance technologies and the need for stronger regulatory oversight. The case highlights how cyber tools can be misused by governments to suppress dissent and undermine democratic norms.

3.4 Role of Corporations, International Alliances and Education in Addressing Cyber Threats and Enhancing Cysec Measures

Briefly, the offense-defense dynamics of CW, along with ethical issues and legal ambiguities, underscore the complex nature of contemporary cyber conflict. Hence, nations must continue to develop secure cyber defense structures while also grappling with the ethical, legal, and other challenges that come with offensive cyber capabilities (Kello, 2017, p. 74). Consequently, the rise of CW has made it crucial for governments to strengthen cysec measures and laws regulating behavior in CS while maintaining the openness and transparency essential to democratic systems.

To combat cyberattacks effectively, some governments are enacting laws that protect critical sectors like finance, telecommunications, and utilities, which are necessary to build resilience and safeguard essential services against future disruption. A clear example is the EU’s NIS2 Directive (2023), which requires critical sectors like energy, banking, healthcare, and digital infrastructure to implement strict cysec measures, report incidents, and undergo oversight. It aims to boost resilience and protect essential services across the EU from major cyber threats.

Cyber attackers also increasingly target corporations and organizations managing essential infrastructure and financial networks, making cysec a critical concern for both public safety and national security (Slonopas, 2024). Employees of corporations have a responsibility to implement personal cysec measures, including installing antivirus software and being cautious about sharing sensitive information online. Regular updates and receiving training to recognize threats like phishing are key for identifying and mitigating potential threats.

Governments operate cyber warfare command centers to coordinate responses to cyber threats, while businesses develop security measures to protect public works.

Collaboration between businesses and governments strengthens defenses against cyber warfare International cooperation is essential in addressing cyber threats, with NATO exemplifying such alliances by coordinating defenses and sharing resources among member nations (Tikk et al., 2010, p. 54).

Academic institutions play a crucial role in shaping future cysec experts, teaching them to combat emerging threats through programs that equip students with knowledge of cyber defense strategies and the latest attack methods, preparing them to protect critical systems and infrastructure (Segal, 2016, p. 109). Governments also ought to focus on educating citizens about cyber threats, as attacks such as ransomware are on the rise.

While cyber threats are serious and ongoing (with countries like Russia, China, and Iran engaged in cyber conflict), progress is being made. Cysec spending, technology investment, and corporate engagement in securing systems have grown significantly. Technologies like AI, automation, and blockchain offer potential solutions, but the growing use of quantum computing by both defenders and attackers may disrupt the balance (Majid & Carlo, 2025).

The growing imbalance between the public and private sectors in democratic states is particularly alarming in the realm of cyberweapons. With minimal regulation over the trade of digital surveillance and intrusion technologies, private companies have been able to sell powerful cyber tools—often to authoritarian regimes—with little oversight. While some tech firms, such as WhatsApp (via Meta), have begun challenging this trend through legal action (most notably against the previously mentioned NSO Group which is now obligated to pay 167M $ in punitive damages (Sabin, 2025)) such accountability should not rest solely on corporate shoulders.

A positive example from recent years is the General Data Protection Regulation (GDPR). The European Union (EU) passed this extensive data privacy law in 2018.

GDPR aims to protect the personal data and privacy of EU citizens by regulating how organizations collect, process, store, and transfer their data. It imposes strict requirements on companies, including obtaining explicit consent for data processing, notifying individuals of data breaches, and providing them with the right to access, rectify, and delete their personal data. GDPR applies to all organizations that handle EU citizens' data, regardless of where the organization is located, making it one of the most significant data protection laws globally (Consilium, 2024).

Additionally, transparent and fair content moderation is important (Popper, 2024, pp. 7-8.). Users' free expression and providing clear guidelines to establish an efficient process of appeal should be prioritized by corporations. Conducting assessments of impact and resisting government demands are another way for companies to ensure they uphold principles of human rights. Moreover, there should be restrictions on the export of cyber and surveillance technology to countries with poor human rights records. Exporters should be held accountable through annual reporting on the impact of their products.

Meanwhile, it is necessary that people become more informed about the technologies they engage with daily on the user level. Users should realize that being on social media is not just harmless entertainment or a neutral pastime activity. Shifts in how citizens use smart devices and computers on a day-to-day basis will significantly impact surveillance methods. People should, for instance, use sufficiently complex passwords to secure all communication channels and change them frequently, while keeping in mind that the information they send and to whom they send it may not be as private as they believe.

Furthermore, those who possess expertise, whether technical, educational, or political, should share their insights.Members of a workplace can contribute to the community by educating others on using technology in privacy-preserving ways. For instance, individuals in technical fields can advocate for methods that reduce unnecessary surveillance (Popper, 2024, pp. 7-8).

Conclusion

As cyber capabilities become a central element in military strategy, their role and prominence in both conventional and unconventional conflicts are likely to increase. The early stages of future wars may very well be characterized by cyberattacks that precede or accompany more traditional forms of warfare, which illustrates the escalating impact of cyberwar in modern conflict.

Overall, a reassessment of how states engage in CS is demanded by the evolving nature of cyber conflict. The intricacies of cyber operations call for new strategies, such as structural deterrence, which focuses on influencing international norms and laws, even though traditional deterrence models still provide valuable insights (Singer & Friedman, 2014, p. 198). In order to effectively govern and secure CS, it will be essential to treat cyberattacks as part of larger geopolitical strategies rather than as isolated incidents.

Democratic states must step in and assert greater control by developing and enforcing stronger legal norms for cysec. Just as international agreements have governed nuclear weapons and conventional warfare, so too must global consensus emerge to regulate cyberspace. For too long, perpetrators of cyberattacks have operated with impunity. It is crucial for democracies to rebalance the power dynamic between governments and technology companies, which currently wield disproportionate influence in the digital domain.

Policymakers should begin by identifying which digital systems are essential to public interest and safety and formally classify them as critical. Even when these systems are privately managed, governments must establish strict criteria and oversight to ensure their protection. Unfortunately, most countries lag behind in this effort.

Equally important is the need to reframe public perception. Cyberattacks are often seen as abstract threats perpetrated by anonymous actors, but they have tangible impacts—on hospitals, schools, households, and critical services. Governments must demystify these threats and highlight their human cost to galvanize public support for cysec reforms.

Greater transparency from companies would allow media and civil society to hold them accountable, enabling consumers to make more informed choices and pushing cysec higher on the political agenda. Ultimately, meaningful change requires political will and international coordination. The EU's solutions offer a promising model: its cysec regulations (including the GDPR), and investment screening mechanisms provide a foundation for broader multilateral cooperation. EU member states have also agreed to levy collective sanctions against cyber aggressors—an important precedent for global action.

The future of international relations will be shaped by the continued integration of private companies into the cysec landscape, alongside emerging norms and legal frameworks (Kello, 2017, p. 82). Going forward, the international community must define what constitutes a cyber act of war and what responses are appropriate. Cyberattacks that cause real-world damage and human harm should be treated on par with conventional attacks.

Democracies must recognize that the nature of conflict is evolving. If they fail to respond, they risk ceding further ground to authoritarian regimes, criminal networks, and unregulated corporate power. But with decisive action, new policies and frameworks can reimpose order on CS and reassert democratic governance.

Full bibliography:

Arquilla, J. and Ronfeldt, D. (1993) *Cyberwar is coming!*. Santa Monica, CA: RAND Corp..

Asbaş, C. et al. (2023) *Cyberwarfare: War Activities in Cyberspace*. IGI Global Scientific Publishing. Available at: https://doi.org/10.4018/978-1-6684-6741-1.ch007. In: Özsungur, F. (ed.) (2023) *Handbook of research on war policies, strategies, and cyber wars*. Hershey, PA: Information Science Reference.

Bentzen, N. (2018) *Foreign influence operations in the EU*. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf.

Buchanan, B. (2017) *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford: Oxford University Press.

Center for Security Studies (2019) *Cyber influence operations*. Zurich: ETH Zurich. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-10-CyberInfluence.pdf.

Choucri, N. (2012) *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press.

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

Deibert, R. (2015) 'Authoritarianism goes global: Cyberspace under siege', *Journal of Democracy*, 26(3). Available at: https://dx.doi.org/10.1353/jod.2015.0051.

Denning, D. and Strawser, B.J. (2014) 'Moral Cyber Weapons', in Floridi, L. and Taddeo, M. (eds.) *The Ethics of Information Warfare*. Cham, Switzerland: Springer.

Edelman, R.D. (2024) 'Defining and Studying Cyberattacks', in *Rethinking Cyber Warfare: The International Relations of Digital Disruption*. New York, NY: Oxford Academic. Available at: https://doi.org/10.1093/9780197509715.003.0003

Even, S. and Siman-Tov, D. (2012). *Cyber Warfare: Concepts and Strategic Trends*. 1st ed. Tel Aviv: Institute for National Security Studies.

Gartzke, E. and Lindsay, J.R. (2015) 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', *Security Studies*, 24(2), pp. 316–348.

Gisel, L., Rodenhäuser, T. and 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), pp. 287–334

Green, J.A. (2016) *Cyber Warfare: A Multidisciplinary Analysis*. London: Routledge, Taylor & Francis Group.

Harvey, A. (2025) *Understanding Russian Hybrid Warfare: Elections in Moldova and Georgia*. War Room.

Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J., 2011. The law of cyber-attack. *California Law Review*, 100. pp. 817-885

Healey, J. (2011) 'Beyond attribution: seeking national responsibility for cyber attacks', *Atlantic Council*. Available at: www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf.

Karabacak, B., Yıldırım, S.Ö. and Baykal, N. (2016) 'A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness', *International Journal of Critical Infrastructure Protection*, 15

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

Lewis, J.A. & Timlin, K. (2011). *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*. Geneva: UN Institute for Disarmament Research

Majid, S. & Carlo, A., 2025. The Future of Information Security: AI, Blockchain, and Quantum Technologies. [online] Available at: https://doi.org/10.13140/RG.2.2.35731.59689

Maurer, T. (2018) *Cyber mercenaries: The state, irregulars, and the rise of private sector cybersecurity actors*. Oxford: Oxford University Press.

NIS2 Directive: new rules on cybersecurity of network and information systems | Shaping Europe's digital future (no date). Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

NIST. (2021). *Cyberspace*. NIST. https://csrc.nist.gov/glossary/term/cyberspace

Nye, J.S. (2004) *Soft Power: The Means to Success in World Politics*. New York: PublicAffairs.

Nye, J.S. (2016) *The Future of Power*. PublicAffairs.

Rafi, S. et al. (n.d.) *Cyberwar: Its Psychological Impact on Employees and Consequences for Organizations*. In: Özsungur, F. (ed.) (2023) *Handbook of research on war policies, strategies, and cyber wars*. Hershey, PA: Information Science Reference.

Perlroth, N. (2023) *This is how they tell me the world ends: The cyberweapons arms race*. New York, NY: Bloomsbury Publishing.

Pijpers, P.B.M.J. and Ducheine, P.A.L. (2021) 'Influence Operations in Cyberspace: How They Really Work', *Amsterdam Law School Research Paper* No. 2020-61. Available at: https://doi.org/10.2139/ssrn.3698642.

Popper, D., (2024). Review of Laura Poitras's Citizenfour & Astro Noise Project from a Policy Perspective. Introduction to Cyber Conflict course.

Ranum, M. (2011) 'Cyberwar: about attribution (identifying your attacker)', *Fabius Maximus*. Available at: http://fabiusmaximus.com/2011/10/21/30004/

Rid, T. (2013) *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Sabin, S. (2025) Israeli spyware vendor NSO must pay $167M for enabling hacks of 1,400 WhatsApp users, jury rules, Axios. Available at: https://www.axios.com/2025/05/06/nso-group-whatsapp-jury-damages

Sanger, D.E. (2018) *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Crown Publishing Group.

Schmitt, M.N. (2013) *Tallinn manual on the international law applicable to cyber warfare*. Cambridge New York: Cambridge university press.

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

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

Sheldon, J.B. (2024) *Cyberwar*. Encyclopædia Britannica. Available at: https://www.britannica.com/topic/cyberwar

Singer, P.W. and Friedman, A. (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.

Slonopas, A. (2024) *What is cyber warfare? Various strategies for preventing it*. American Public University (APU). Available at: https://www.apu.apus.edu/area-of-study/information-technology/resources/what-is-cyber-warfare/

Stone, J. (2013) 'Cyber War Will Take Place!', *Journal of Strategic Studies*, 36(1), pp. 101–108. https://doi.org/10.1080/01402390.2012.712757.

Tikk, E., Kerttunen, M. and Vihul, L. (2010) *Cybersecurity and Cyberwarfare: A National Policy Perspective*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Tsagourias, N. and Buchan, R. (2015) *Research Handbook on International Law and Cyberspace*. Cheltenham: Edward Elgar Publishing.

Zetter, K. (2014) *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. New York: Crown Publishing Group.

Appendix

Full text of transcribed interview with Adam Remport (translated from Hungarian to English) via AIrite Transcription Tool:

David Popper: My interviewee is Ádám Remport, a lawyer at TASZ (Hungarian Civil Liberties Union). We are recording this interview on May 11, 2025 and we will be discussing the Pegasus case and its consequences.

DP: So the first question is a two-parter: why does the Pegasus case represent a particularly serious precedent from TASZ's perspective, and has there been any accountability or systemic change since its disclosure?

Adam Remport: It might be harder to answer the first question, so I'll start with the second: no one has been held accountable.

AR: What happened was that it came to light that Hungarian journalists, politicians, businesspeople, activists, and lawyers had the spyware Pegasus installed on their phones. In some cases this was proven; in others it could only be inferred from the fact that their phone numbers were on a list of targeted phones. One of the problems is that legally, it's very difficult to link these attacks directly to the Hungarian state, and this makes litigation harder. It's doubly difficult because intelligence services by default don't tell anyone whether or not they process data about them — so even establishing a "yes or no" on that can require a lawsuit. And even if they admit it, we still can't necessarily link it to Pegasus — even though it's crystal clear that these attacks were carried out by the Hungarian state. But this complicates accountability in court.

There was an investigation by the National Authority for Data Protection and Freedom of Information (NAIH), which basically followed the usual patterns, and we at TASZ, representing our clients, also initiated individual investigations at NAIH to check whether our clients were affected in the Pegasus case, and if so, whether everything was done legally.

AR: These have concluded as well, and NAIH simply stated that everything was legal. Beyond that, not much more can be learned. You can't even know for sure if your client was affected by Pegasus — only that NAIH investigated and their position is that if anything did happen, it was lawful. So that's where accountability stands at the moment.

AR: Clearly, the situation is made worse by the fact that the ruling parties have a majority on the Parliament's National Security Committee, so they control the agenda, and without them, the Committee lacks a quorum — every decision requires them, meaning the whole thing can be completely sabotaged. Returning to your first question — the significance of the case: I think the point is that criticism of Hungarian surveillance practices has existed for quite a while, but it was abstract until the Pegasus scandal broke, which was around four years ago.

AR: Already back in 2016, the European Court of Human Rights (ECHR) ruled that, for example, surveillance should not be authorized by a minister, since that's clearly not an independent body — not someone who can properly assess whether the intrusion is justified from a fundamental rights perspective. Instead, it should be a judicial or quasi-judicial body, preferably a court, or at least something with similar independence. There should also be complaint mechanisms and options for legal remedy. For this, it's necessary that the person under surveillance is notified — if it no longer harms national security interests — so they can go to court. Actually, the ECHR also says that if no complaint mechanism exists, it must still be possible to go to court even without proving that the intelligence services are processing data about you. That's exactly what makes litigation difficult in our case, and a general jurisdiction court would ease this for potentially affected individuals.

AR: Also, the scope of people who can be targeted is undefined, or it's unclear how long such operations can last — according to the law, they can be extended indefinitely. So there are a lot of issues here that were already on the radar at an abstract level, but the Pegasus case, and specifically our procedures, show that these problems exist in reality too. From a purely legal standpoint, I think this is one of the major takeaways from the case. The other is that it drew public attention to the fact that this is a real issue — that the state targeted journalists, political opponents, businesspeople, and lawyers, i.e., people who are supposed to be checks on power, through the press, legal representation, defense in criminal procedures, etc. So these are targeted attacks on active citizens and people who uphold core institutions of the rule of law. That shows the seriousness of the situation. Or maybe that's the bottom line.

DP: Unprecedented, right?

AR: Yes. The fact that it came out at this scale is unprecedented.

DP: Are there any ongoing cases now, or has most of the assistance requested from your side concluded?

AR: Most of these cases are nearing their end. We have 7 clients, and with them, we're exhausting pretty much every possible legal procedure in Hungary that exists — or that we can even imagine.

Not every client goes through every procedure, because on one hand it would be very costly, and on the other hand, we want to expose the problem globally. But this is coordinated with them. The goal is to exhaust all possible legal remedies so that either we achieve something or we prove that it's completely impossible to do anything about this in Hungary — and then we can take it to the ECHR. Actually, quite a few elements of this case can be brought before the ECHR anyway, so we'll definitely go there with our clients.

DP: Have there been similar cases in other countries?

AR: Yes, for example, in Poland, there's also an ongoing case.

DP: Okay, you've already answered part of my next question, but I'll ask it anyway in case it sparks another thought: How do you assess the current legal regulation of state surveillance, especially in light of national security exemptions, and what shortcomings do you see in the legal framework? Also, how much independent oversight and judicial control is ensured over secret surveillance? But you've basically gone through all that.

AR: Yes, I think it's clear from what I've said that there's practically no independent oversight in Hungary. I can go into even more legal detail than before, but I don't know how interesting that is for this interview. Overall, I'd say that there is effectively no judicial oversight, the data protection authority doesn't fulfill its role, and neither does the National Security Committee. Although that committee is, after all, a political body — even under normal circumstances in a non-autocratizing country, decisions in such a committee would be shaped by political deals. So it's not a fully independent supervisory institution to begin with, but it could work better — and as things stand, it doesn't.

DP: I'd also like to hear — even if it's a long topic — just briefly: what kind of legal reforms would be necessary to meaningfully protect citizens' right to privacy? Should this happen on a state level or at the EU level? Should the GDPR, for example, be enforced more strictly? What do you think?

AR: Both. Starting with the EU: because of the national security nature of this data processing, the GDPR doesn't apply. The EU is generally very reluctant to get involved in national security matters — these typically fall under the competence of member states. But in our work and through international cooperation, we try to emphasize that this is not fundamentally a national security issue. When a government systematically targets representatives of constitutional bodies, institutions, or fundamental freedoms — like the right to defense — this isn't about national security but about the rule of law. And the EU should view it from that perspective.

Actually, the European Parliament had a Pegasus investigation committee, and its report includes recommendations from this perspective. That's good, but more steps are still needed. For example, it should be clearly stated that whether or not oversight mechanisms exist in intelligence operations is not a national security matter but a rule-of-law issue. Of course, there could be pushback — member states might say the EU shouldn't interfere in how they run their intelligence services or oversee them. But the EU could counter by saying that nothing guarantees those services won't be used to undermine democracy rather than protect it. This goes beyond everyday national security concerns — like who is currently seen as a threat to sovereignty or constitutional order — and there should be universal standards. So I think adopting this rule-of-law-centered approach across the EU would be valuable.

AR: Regarding the Hungarian reforms, as I already mentioned, the 2016 judgment — this was the *Szabó and Vissy v. Hungary* judgment. There's also the *Hüttl v. Hungary* one. Fun fact: all three — my colleagues Szabó Máté, Vissy Beatrix, and Hüttl Tivadar — are here with us, but that's just a side note. In this ruling, it's clearly laid out what reforms the Hungarian state should carry out. One of the most important is that surveillance should be authorized by an independent body. Not by a minister, but preferably a court or a body with judicial-like independence.

AR: So what I basically mentioned — that there should be a system of post-surveillance notification, and people should at least have the possibility of becoming aware of rights violations, and if a violation occurs, they should have access to legal remedies. I think those would be the most important. But even more precise definitions could be created — for example, who exactly can be targeted by surveillance. It could also be clarified how long a surveillance operation may last, because, as I mentioned, currently it can be extended indefinitely. Judicial oversight could be extended to the entire process — meaning a judge could assess midway whether the surveillance is being conducted in accordance with the original warrant. That’s not the case now. So, honestly, a lot could be done. We’ll have a policy paper where we’ll summarize all of this.

DP: When will that be published?

AR: Well, that’s a good question. Hopefully by autumn. In it, we’ll detail all of this. But yes, I think these are the most essential elements. I could also mention that it would be good if courts could exercise oversight over classified information — which means they could declassify information (formerly "state secrets" now called "classified data") if they deem it justified.

AR: That’s the kind of thing I’m thinking of — that there should be full oversight of the process and a guarantee of post-hoc legal redress for citizens once the procedure has ended.

DP: Okay, so the next one is a bit of a rhetorical question: Do you think that, beyond Pegasus, the use of digital technologies in surveillance moves the state in a more authoritarian direction?

AR: The use of spyware?

DP: Yes, and that there’s a broader trend — for example, now at protests, facial recognition systems have been introduced, and these are already being abused. These systems could, in principle, be used to guarantee citizen safety, but instead, they’re being used in a very different, more harmful way. Looking toward the future — what are your thoughts?

AR: Well, for sure, these new technologies can make things easier for autocracies. After all, anything that relates to surveillance or control can strengthen those in power.

AR: Obviously, as with any new technology, regulation is necessary. Some argue that certain technologies should be outright banned — including facial recognition and spyware. At the Hungarian Civil Liberties Union (TASZ), we don’t really support bans — we focus on regulation and oversight. But I can understand why some people consider these extremely dangerous technologies.

AR: In short, yes — these can definitely be abused and made more effective than earlier tools if there’s no maximum-level regulation. The bigger question is what proper regulation achieves in an authoritarian country. Ultimately, it comes down to the general state of democracy or rule of law in a country — whether that can act as a safeguard against these technologies. If that safeguard is missing, then anything can be written on paper, and the system becomes easily gamed. We’ve seen how democratic guarantees can be dismantled if the democratic institutions of a country aren’t strong enough.

DP: Okay. Final question: What would you say to someone who, as a citizen, wants to resist abuses of state surveillance — especially in a fragile democratic environment? Not just here in Hungary, but in neighboring countries or regions. Sort of as a preventative measure — so they don’t only turn to you when something happens, but ideally before anything does?

AR: Yes, this is a complex question. For those who are more legally aware — or for anyone who even just knows about the issue — it's important to talk to others, contribute to making it part of the public discourse so it's not forgotten. So that maybe people who didn't know about it become informed. I think that's definitely great — essentially a kind of awareness raising that everyone can do in their own microenvironment.

AR: Another thing I'm thinking of is how important it is for people to support independent journalism. Because the uncovering, continuous coverage, and government accountability regarding spyware abuse — those are things the independent press can do really well. As long as there's press, there will be pressure on governments. So I think it's crucial to support the media. And now I'm a bit biased, but the same applies to supporting civil society. That also helps increase the pressure on governments. Ultimately, governments find it uncomfortable when these things come to light. We can talk about the political cost — if illegal, mass surveillance becomes public knowledge, the higher the political cost, the greater the deterrent effect on the government. And that, in turn, depends on how many people find out about such things and on how willing EU institutions are to initiate infringement proceedings in such cases. So anything that results in politically uncomfortable consequences for the government is the best kind of deterrent. I think people should think along those lines. That's why I mentioned the press, NGOs, raising awareness in your community — and if needed, speaking out in other spaces too. It's also important to internalize that this is a rule of law issue. A national security one too.

AR: That's what comes to mind at the moment. And if people want to feel more secure, or want to better protect their own sense of comfort and privacy — well, there are techniques for that too. I'm not too familiar with the technological details, but you can read up on them — like restarting your phone, which can wipe out certain types of spyware. Things like that. So there are ways to defend yourself to some extent. It might be worth looking into what tools are currently out there.

DP: That's a comprehensive answer — and together with the rest, thank you very much for the interview.

AR: Oh, you're very welcome. Thanks for reaching out.