Università di Genova

PhD in Security, Risk and Vulnerability

Coordination in Offensive and Defensive Cyberoperations: Dissecting China, Russia, and NATO's Approaches in Cyberspace

Cosimo Melella S5157198

Abstract

This dissertation delves into the intricate dynamics of offensive and defensive cyber operations by analyzing the approaches of China, Russia, and NATO in cyberspace. The study investigates the critical role of coordination in cyber operations, assessing its impact on national and international security. The research is structured into several chapters, beginning with a comprehensive literature review that explores the evolution of cyber operations, their effectiveness, and the limits of cyber warfare. It also examines the offense-defense balance in cyberspace and the importance of coordination for successful cyber operations.

The core research questions focus on conceptualizing the lack of coordination in cyberspace and understanding its implications for the effectiveness of cyber operations. The dissertation explores these questions through methodological and empirical perspectives, including case studies on Sino-Russian coordination during the Ukraine war and the internal dynamics of Russian intelligence agencies. The study also assesses the potential of artificial intelligence to enhance coordination in cyber operations, as demonstrated in the NATO Locked Shields exercise.

By integrating theoretical insights with practical case studies, this dissertation provides a nuanced understanding of the challenges and opportunities in cyber operations. It highlights the need for a balanced approach that considers both offensive and defensive strategies, emphasizing the importance of effective coordination to protect critical infrastructure and maintain security in the digital age. The findings contribute to the broader field of international relations and security studies, offering practical recommendations for improving cybersecurity policies and strategies.

INTRODUCTION

Cybersecurity has emerged as a significant national and international discipline in the digital age. Cyberspace, a vast and complex domain, is now considered a virtual battleground that significantly affects nation-states' financial stability and security, also spacial, worldwide. This digital environment has become a theatre for various cyberattacks, which are now integral to intense geopolitical rivalries. For instance, the 2022 Viasat cyberattack, which targeted the satellite communications provider, disrupted internet services in Ukraine just as the Russian invasion began. This attack not only impacted military communications but also affected civilian infrastructure across Europe[1].
Such attacks do not discriminate, affecting both civil and military infrastructure, and raise significant concerns about the security and integrity of classified military data, which could be vulnerable to infiltration through computer networks. An emblematic example of cyberattack was the coordinated attack against Ukrainian infrastructure in 2015, when a sophisticated computer virus, Black Energy, temporarily disabled part of the electricity grid, causing prolonged outages[2]. This incident demonstrated how cyberattacks can be coordinated to hit critical points of a national infrastructure, affecting the internal security of a state, as well as its economic and political stability.

In this scenario, cyber-offensive and cyber-defensive operations become essential for national and international security.
Offensive operations in cyberspace require targeted coordination, which is essential to maximise the effectiveness of attacks and ensure that they are conducted precisely, avoiding unintended collateral damage. Such coordination involves technical synchronisation and careful consideration of political and legal implications.
In parallel, defensive operations in cyberspace require equally rigorous coordination. This is crucial for developing a timely and robust response against cyberattacks, facilitating the sharing of critical information and resources between the agencies and organisations involved. Such coordination ensures a coordinated response and effective threat management, which are crucial for protecting critical infrastructure and sensitive data.

Given the importance of coordination in defensive and offensive in cybersecurity strategies, the research questions that guide this dissertation are the following:

- How can be conceptualised the lack of coordination in cyberspace in order to better understand how cyberattacks affect national and international security?
- How these interactions influence the effectiveness of both offensive and defensive operations?

[1] Greenberg, Andy. "How Russian Hackers Aimed at Viasat, Causing Chaos in Ukraine and Beyond." MIT Technology Review, May 10, 2022. https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.
[2] Cybersecurity and Infrastructure Security Agency. "IR-ALERT-H-16-056-01: Cyber-Attack Against Ukrainian Critical Infrastructure." CISA, February 25, 2016. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

To gain an in-depth understanding of effective coordination strategies, I must explore the coordination dynamics between various entities in cyberspace. This exploration should consider both methodological and empirical perspectives, allowing us to measure and evaluate how these interactions influence the effectiveness of offensive and defensive operations.
This investigation can provide crucial insights into the nature of cyberspace as a domain of conflict. This thesis seeks, also, to clarify the dynamics of coordination in cyberspace and the relationship between offensive and defensive cyber operations. This study's basis involves not only a review of existing literature in the fields of international relations and security studies related to cyber operations but also original technical and empirical contributions. It aims precisely at understanding the interaction between state actors in cyberspace and performing new empirical analyses to identify patterns and trends in cyber operations. By combining these contributions with a comprehensive literature review, the study aims to advance knowledge and provide practical insights into cybersecurity.

The review highlights, indeed, two central issues. First, international relations theories have been widely applied to the offence-defence balance to conceptualise offensive and defensive actions in cyberspace. However, these theories tend to treat attack and defence as separate and distinctly analysable entities, without considering attack and defence as integrated and interdependent components that influence each other in the context of cyberspace. This segmented approach does not adequately reflect the reality of cyberspace, where offensives can often immediately generate defensive countermeasures and vice versa. Moreover, actions in this domain are characterised by such rapidity and scale of propagation that the distinction between offensive and defensive becomes fluid and often ambiguous. A second aspect still little explored in the academic literature concerns the specific functioning of coordination in cyberspace. While existing research in the field of security studies and international relations has thoroughly investigated the tangible effects of cyber warfare, there is a growing need for a more detailed understanding of how cyber operations integrate with each other and how they interact with other domains. This deepening requires a focused analysis of the role of cyber operations as a means of gathering crucial intelligence, which can offer a significant strategic advantage in various contexts[3].
It is crucial to recognise that cyber operations, beyond their ability to inflict direct damage, often act as sophisticated tools for intelligence acquisition. This distinguishes them from traditional warfare, focusing their effectiveness not on physical destruction but on collecting data and intelligence that can be used to achieve political and strategic objectives. This understanding deepens my perception of cyberattacks, which rarely result in conventional conflicts but operate in a subtle, less visible sphere of influence[4].
Therefore, research in this area should aim to further explore how coordination in cyberspace facilitates this intelligence gathering and how these operations fit into the broader context of warfare strategies. Such an investigation could provide valuable insights into how nations use

[3] Rid, Thomas. "Cyber War Will Not Take Place." Journal of Strategic Studies 35, no. 1 (2012): 5-32.
[4] Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." International Security 38, no. 2 (2013): 41-73.

cyber operations to gain a competitive advantage, thereby influencing international politics and security dynamics beyond mere physical impact.

In light of the gaps in the current literature, this thesis aims to undertake a theoretical and empirical examination of offensive and defensive cyber operations, highlighting the inherent challenges that impede coordination in cyberspace. Theoretically, the thesis aspires to rejuvenate the existing literature in international relations and security studies concerning cyberspace by focusing on the technical and structural obstacles that limit coordination in cyberspace.
Given the complex and multifaceted nature of the research topic, it is insufficient to rely solely on a methodological approach based on technical analysis. It is crucial to adopt a multidisciplinary approach to fully understand the challenges related to the lack of coordination in cyber operations. This should combine specialised knowledge in information technology (IT) with the theoretical and practical perspectives of security studies and international relations. Such an integrated approach makes it possible to examine the problem from different angles, providing a deeper and more comprehensive understanding of the dynamics at play in cyberspace.
Recognising the innovative nuances of the topic, the study will draw from a wide range of sources and a thriving literature.
To address the complexity of cyber operations with a focus on the lack of coordination, the research approach will be structured and sequential, focusing initially on the literature review. In this phase, I will review existing studies and analyses to thoroughly understand the field and identify any gaps in current research. This will serve as a foundation for the next steps.
Next, I will move on to theoretical exploration. Here, I will elaborate and develop theories based on the literature review results, formulating hypotheses and building a theoretical framework to guide further analysis. This step is crucial in setting the conceptual basis for the research.
After establishing a sound theoretical foundation, I will focus on methodology. In this step, I will define and describe the methods I intend to use to collect and analyse data. This will include the selection of qualitative, quantitative or mixed approaches, depending on what is most appropriate for the research. Critical resources for this endeavour will include bibliographic and documentary materials, supplemented with specialised software for analysing attacks. In the rapidly evolving terrain of this field, the research represents an exciting challenge. Indeed, it highlights the imperative to create a contemporary analytical framework capable of demystifying the complexities of offensive cyber operations while recognising the interconnected dynamics of technological, social and geopolitical dimensions, focusing on the prevalent lack of coordination.

The thesis is structured in several chapters to systematically address the complexity of cyber operations, focusing on the lack of coordination.

- Chapter I: Literature Review.
  In Chapter I, I will review existing studies and analyses to understand the field and thoroughly identify gaps in current research. This literature review of international

relations and security studies will be the basis for subsequent theoretical exploration and empirical analysis.

- Chapter II: Lack of coordination in cyberspace - A theoretical exploration.
  Chapter II delves into the theoretical exploration of coordination problems in cyberspace. Based on the literature review results, I will formulate hypotheses and develop a theoretical framework to guide the subsequent analysis. This stage is crucial to define the conceptual basis of the research.
- Chapter III: Research Design.
  In Chapter III, I will define and describe the methods to be used for data collection and analysis. This will include the choice of qualitative, quantitative, and technical approaches. Critical resources will include bibliographic and documentary materials, supplemented by specialized software for data collection and attack analysis.
- Chapter IV: Exploring the degree of Sino-Russian coordination in cyberspace during the Ukraine war.
  Chapter IV focuses on empirical case studies, explicitly examining coordination between China and Russia against the backdrop of the war in Ukraine. This chapter will analyse the growing collaborative cyber espionage activities against Ukrainian NATO members, highlighting the repercussions after the 2022 invasion. Key groups such as Mustang Panda, Scarab, and Judgment Panda will be studied to identify potential nuances of collaboration with Russian entities.
- Chapter V: Competition, rivalry, and coordination challenges among Russian intelligence agencies at the operational and technical levels.
  In Chapter V I will analyse the lack of coordination among Russian intelligence agencies. The discussion will focus on Russia's growing cyber capabilities, particularly evident in the Russian-Ukrainian conflict of 2022. This chapter aims to fill a gap in academic research by exploring coordination dynamics, or the apparent lack thereof, among various APT groups linked to Russian intelligence agencies such as the GRU, SVR, and FSB. The analysis will highlight internal disharmonies and historical gaps that potentially undermine a unified approach to cyber strategies.
- Chapter VI: Developing an innovative IDS dataset to counter cyberspace coordination challenges in the largest live-fire cybersecurity exercise.
  Chapter VI examines the potential of artificial intelligence in solving coordination problems in cyber operations. This chapter focuses on the NATO Locked Shields exercise, in which innovative datasets were developed for an intrusion detection system (IDS) based on machine learning techniques. The study will demonstrate the revolutionary potential of these datasets and their impact on improving cyber defence strategies.
- Concluding reflections and prospects.
  The final chapter will offer concluding reflections on the research findings and suggest directions for the future. It will summarize critical insights gained from the empirical case studies and theoretical explorations, providing recommendations for future research and practical applications in cybersecurity.

In the context of my study, the application of the proposed methodology in real-life situations and the obtaining of concrete data provide empirical evidence that confirms the theory presented.
The link between theory and case studies is a central pillar of my research. This approach not only helps to reduce the distance between conceptual knowledge and its tangible applications but also makes the results of the study relevant to the academic context and beyond. In other words, my work facilitates a better integration of theoretical insights with operational strategies, thus enhancing the usefulness of scientific findings in solving practical problems.
Finally, my project contributes substantially to the evolution of knowledge in my field of study. Through the analysis of theoretical, methodological and empirical elements, my work promotes a deeper and more enriched understanding of the topic of coordination. This not only broadens the horizon of existing knowledge but also establishes a more solid basis for future research, emphasising the continuous dialogue between theory and practice that characterises modern science.
The importance of thoroughly examining the concept of coordination in cyber operations, both offensive and defensive, becomes clear when considering the inherent complexity of cyberspace. This digital environment is characterised by an intricate web of actions and reactions, where the decisions of a single actor can influence the entire system. Effective coordination, at least in theory, becomes crucial: it ensures that operations are conducted strategically, maximising effectiveness and minimising any collateral damage.
Cyber operations often require diverse resources and expertise, which transcend the limits of a single organisation or nation. Here, coordination assumes a key role in facilitating collaboration, information and resource sharing, all of which are critical to the success of cyber operations. This interdependent aspect of coordination is vital for operational effectiveness and building a robust defence against threats.
On the other hand, risk management and security measures in cyberspace are greatly enhanced by effective coordination. Without it, organisations remain vulnerable and may not be able to respond promptly and adequately to attacks. Therefore, coordination is essential to develop robust defence strategies and proactively manage security risks.
The weight of cyber operations in the political and strategic context cannot be ignored. A thorough understanding of coordination provides a clearer view of how actions in cyberspace fit into global political strategies and how they influence international relations. Finally, considering the constant evolution of cyber threats, examining coordination helps to understand how attack and defence strategies adapt to these changes, providing vital insights into developing effective tactics.

This dissertation suggests a more nuanced picture than the prevailing public debate and academic literature. In this regard, it is recommended that cyber operations are not a substitute for or complementary to kinetic warfare; instead, they are autonomous operations that optimise information assets for strategic purposes. Moreover, contrary to what scholars as Libicki assume[5], the structural characteristics of cyber operations limit coordination in cyberspace, and

[5] Libicki, Martin C. Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND Corporation, 2009.

this has enormous implications for both offensive and defensive joint cyber operations and political alliances in international politics.

In this doctoral thesis, I enter the vast and complex world of cyber operations, approaching the topic step-by-step and well-considered. I will first begin by examining the problem of the lack of coordination in cyberspace, defined as the lack of shared rules and protocols between the various levels involved in cyber operations - strategic, operational and technical. The lack of coordination mainly concerns the rules of engagement and response strategies to digital threats. The absence of coordination in cyberspace can have significant repercussions, including ineffectiveness in dealing with cyber threats and a potential vulnerability in security at different levels: local and national (micro and meso) and international (macro). My objective is to analyse precisely this lack of coordination in the fifth domain, which is crucial in ensuring the effectiveness of offensive and defensive military operations in the cyber domain.

Secondly, notwithstanding the lack of coordination in cyberspace, I will attempt to present cyber operations as a subset of intelligence operations in this thesis. Recognising that cyber operations are more closely related to intelligence activities than traditional military ones is crucial. Indeed, cyber operations align more with intelligence methodologies and objectives, focusing on the acquisition and analysis of information rather than the use of force. Therefore, examining the vital role of intelligence provides a better understanding of the role of these operations in cyberspace. This investigation will lead us to consider precisely how cyber operations, whether defensive or offensive, can fit into the domain of intelligence and security apparatus.

Furthermore, I will address the distinction between offensive and defensive cyber operations, in particular, analysing how offensive operations geared towards manipulating and destroying information have evolved since their emergence in the late 20th century. Through this thesis, my journey will take us into the intricate landscape of cyber operations, where the insights of experts and scholars will guide us in an in-depth and critical analysis of the dynamics of cyberspace. This journey will allow us to examine existing strategies and identify opportunities for future research and development in the field of cybersecurity.

‘

CHAPTER I

LITERATURE REVIEW

This literature review examines the intersection between international relations and security studies, drawing on seminal works in security studies, particularly defence and cybersecurity studies. It does so by exploring two main themes in this thesis: the dynamics of interaction between offensive and defensive cyber operations and the central role of coordination between these elements.

The current debate, which focuses on the real or perceived risk of a large-scale attack on national infrastructures, needs a perspective that takes into account the historical context. Especially in light of the proliferation of hostile actors with the capacity to launch cyberattacks, the increasing interconnectivity and the sophistication of cyber weapons. On the other hand, it is also necessary to consider factors that could diminish the impact of this threat, including the inherent difficulties in carrying out and attributing attacks and existing protection measures. Finally, the role of intelligence in cyber warfare must be considered. Although intelligence agencies play a key role in threat prevention, there is a need to explore how intelligence can be effectively harnessed to address cyber domain challenges in both OCO (Offensive Cyber Operations) and DCO (Defensive Cyber Operations).

This literature review is carefully structured to provide a comprehensive and critical overview of studies on cyber operations, both offensive and defensive. Initially, it focuses on the main contributions that have enriched the understanding of these operations, outlining the theoretical and practical foundations that define the field. After that, it proceeds with a critical review of the existing literature, emphasising the challenges encountered and the coordination strategies required within cyberspace.

It begins with "The Scholarship on Cyber Operations: An Overview", where the evolution of cyber operations is explored, tracing a path from the concept of Netwar to modern cyberwarfare. This section highlights how the early stages of cyber operations were closely linked to military and intelligence activities, evolving towards the uncharted territory of cyber operations, with its peculiar challenges and opportunities[6].

Next, the literature review delves into the 'Effectiveness of Cyber Operations', questioning their revolutionary or evolutionary nature. The concept of Cyber Pearl Harbor is examined, followed by an examination of the importance of cyberspace in international relations. This highlights how this domain has evolved between 2010 and 2017 and what the future directions of cyber operations will be, with a focus on their ethical foundations and security strategies between 2018 and 2022[7].

The third major area of investigation concerns 'The Limits of Cyber Operations', where the complexities and challenges of cyber warfare are discussed through an integrated analysis of

[6] Lilli, Eugenio. "How Can We Know What We Think We Know about Cyber Operations?" Journal of Global Security Studies 8, no. 2 (June 2023)

[7] Chaudhary, Sunil, Vasileios Gkioulos, e Sokratis Katsikas. "Developing metrics to assess the effectiveness of cybersecurity awareness program." Journal of Cybersecurity 8, no. 1 (2022)

strategic and operational dynamics, and the dynamics of conflicts in cyberspace and their strategic implications, are examined.
The focus then shifts to 'Offence-Defence Balance in Cyberspace', analysing cyber positioning and offence-defence dynamics in the cybersecurity literature, assessing how a balance between offence and defence can be achieved in cyber operations and exploring the gaps that exist beyond this balance[8].
After exploring the historical and theoretical evolution of cyber operations and assessing their effectiveness and limitations, the next step is to analyse the delicate balance between offence and defence in cyberspace. This segment examines how offensive and defensive strategies influence each other and how they can be balanced to ensure adequate cybersecurity.
The last section, dedicated to 'Coordination in Cyber Operations', examines the vital importance of coordination in cyberspace. This segment highlights how, despite the crucial importance of this topic, there is still a lack of in-depth analysis in current academic literature. Through this analysis, it becomes clear that the coordination issue represents a fundamental pillar for the success or failure of cyber operations and assumes a central role within this dissertation. This emphasis reflects the growing need to understand cyberspace's increasingly complex challenges better. Coordination is important both in the literature and in reality because it enables a more effective and timely response to cyber threats, improving the overall security of operations and cyber resilience in general. In conclusion, it emphasises the urgent need to fill existing research gaps.
The review proceeds in chronological order in each segment, outlining how the academic debate on these issues has developed. This approach highlights the evolution of thinking and practice in computer operations and seeks to identify gaps in existing research, suggesting areas for further study. Through this methodical structure, the review aims to provide a deep and up-to-date understanding of the dynamics that characterise operations in cyberspace, offering critical insights and future directions for research.

1. The Scholarship on Cyber Operations: An Overview

1.1 Evolution of Cyber Operations: From Netwar to Cyberwarfare

Building on the pioneering work of Arquilla and Ronfeldt, the academic debate on 'cyber operations' has evolved significantly over the past three decades, with significant contributions from scholars such as Thomas Rid and Peter McBurney. This debate has focused on several key themes that have delineated the field of cyber operations and their relationship to the Revolution in Military Affairs (RMA)[9]. Below, I will provide a chronological discussion of the

[8] Glaser, Charles L., and Chaim Kaufmann. "What Is the Offense-Defense Balance and How Can We Measure It?" Belfer Center for Science and International Affairs.
[9] Van Creveld, Martin. The Transformation of War. New York: Free Press, 1991.
Knox, MacGregor, and Williamson Murray, eds. The Dynamics of Military Revolution, 1300–2050. Cambridge: Cambridge University Press, 2001.
Krepinevich, Andrew F. "The Unfinished Revolution in Military Affairs." Issues in Science and Technology 19, no. 4 (2003): 58-66.

main topics addressed by scholars in international relations and security studies who have focused on cyberoffensive and cybersecurity operations. Each of these topics will then be discussed in more detail in the following sections:

- From Netwar to Cyberwarfare (1990s - early 2000s): the transition from 'netwar', a concept introduced by Arquilla and Ronfeldt, to cyberwarfare marked the early years of this debate. Scholars focused on the revolutionary potential of information technologies in the military, exploring how the network could be used as a tool for attack and defence.
- The offense-defence dichotomy (early 2000): A predominant theme was comparing offensive and defensive capabilities in the cyber domain. While some argued that cyber operations offered a significant offensive advantage, others highlighted the complex challenges of defence in this domain, mainly due to anonymity and the difficulty of attributing cyberattacks[10].
- State and non-state actors (mid-2000s): The debate then analysed the role of state and non-state actors. As nations developed cyber capabilities as part of their defence strategy, non-state groups began to use cyberspace for propaganda operations, espionage and cyber-attacks, thus expanding the scope of cyber warfare.
- The revolutionary scope of cyber operations (late 2000s - present): Scholars such as Rid have pointed out that despite the significant impact of information technology, cyber operations have yet to transform into conventional warfare completely. This has led to a debate on the actual 'revolutionary nature' of cyber operations within RMA[11] [12].
- The attack-defence dynamic (today): The debate has also focused on the dynamic between attack and defence in cyberspace. The question is whether offensive capability in the cyber domain is inherently superior to defences, a debate that continues to influence national and international security policies[13].

In their 2012 publication, 'Cyber-Weapons', Thomas Rid and Peter McBurney delved into the intricate dynamics of cyber warfare, distinguishing it from traditional warfare concepts. Their analysis not only expanded on the fundamental ideas of Arquilla and Ronfeldt but also contextualised the term 'cyber operations'[14] into the broader landscape of information

[10] Slayton, Rebecca. "Why Cyber Operations Do Not Always Favor the Offense." Belfer Center for Science and International Affairs, February 2017
https://www.belfercenter.org/publication/why-cyber-operations-do-not-always-favor-offense.

[11] Wright, Steve. "Cyberwarfare, Netwar & The Revolution in Military Affairs." In Edited by Halpin, E., Webb, D., Trevorrow, P., and Wright, S., Palgrave, 2006.

[12] "Information as a Key Resource: The Influence of RMA and Network-Centric Operations on the Transformation of the German Armed Forces." George C. Marshall European Center For Security Studies. https://www.marshallcenter.org/en/publications/occasional-papers/information-key-resource-influence-rma-and-network-centric-operations-transformation-german-armed.

[13] Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance." Yale Journal of International Affairs. https://www.yalejournal.org/publications/cult-of-the-cyber-offensive-misperceptions-of-the-cyber-offensedefense-balance.

[14] Thomas Rid's criticism of "cyber war" is fundamental for several reasons. Rid, an expert in cyber security, argues that the characterization of cyberattacks as "war" is misleading and does not accurately reflect the reality

technology and strategic military planning. This marked a pivotal moment in the academic literature, consolidating the relevance and use of the term in discussions of modern warfare and cybersecurity[15]. However, this section will begin by analysing the distinction between military and intelligence cyber operations, particularly the concept of 'digital Pearl Harbor'[16]. It traces the history of cyber operations, starting with the seminal Arquilla and Ronfeldt report of 1993, which introduced the concept of 'netwar' and its influence on military structures and doctrines. It explores the origins of cyber warfare in the 1960s to understand its evolution to its current importance in military and national security before examining the distinction between information-gathering cyber operations and military operations to provide a clear view of the complexity and aspects of information security operations, highlighting the importance of the planning, persistence and operational phases[17].

1.2 The Early Stages: Military and Intelligence-related Cyberoperations

In 1993, John Arquilla and Dave Ronfeldt published an authoritative report for RAND[18], that explored the changing nature of armed conflicts and the necessary future military structures and doctrines. Their work introduced the concept of 'netwar', a form of conflict characterised by the strategic use of information networks and communication technologies. This 'netwar' idea aligns closely with the Revolution in Military Affairs (RMA) debate, a theory emphasising technological innovations' critical role in transforming military operations[19]. Arquilla and Ronfeldt's 'netwar' concept proposes a vision in which cyber operations can be a highly effective form of conflict, significantly influencing the dynamics of traditional armed conflicts. Andrew Krepinevich, another eminent theorist in military strategy, has contributed significantly to this debate. Krepinevich emphasises how new technologies, particularly information technology and networks, have the potential to revolutionise traditional military strategies and tactics[20].

Within this framework, Krepinevich's writings provide a complementary perspective, emphasising the importance of adapting the armed forces to new technological and information realities. His analysis and Arquilla and Ronfeldt's report highlight a crucial point: Technological progress is transforming warfare capabilities and nature, requiring new strategies and doctrines to address these emerging challenges in global security. In this context, Arquilla and Ronfeldt's article highlights how cyber operations are a powerful tool for

---

of such activities. According to Rid, most cyberattacks have more in common with espionage or digital vandalism than traditional acts of war. This distinction is crucial for understanding the nature and consequences of cyberattacks and for developing appropriate policy and security responses. Rid points out that the improper use of the term "war" can lead to excessive or inadequate responses, distorting public and political perceptions of the problem. His analysis helps promote a more precise and nuanced understanding of cyber threats.

[15] Rid, Thomas, and Peter McBurney. “Cyber-Weapons.” The RUSI Journal 157, no. 1 (2012): 6-13

[16]The "Digital Pearl Harbor" metaphor was first used in the 1990s to describe a potentially devastating cyberattack. Although it was not originally coined by Robert Gates, former US Secretary of Defense, he and others have often used the term to emphasize the seriousness of cyber threats to national security.

[17] Arquilla, John, and David Ronfeldt. “Cyberwar is Coming!” Comparative Strategy 12, no. 2 (1993): 141-165.

[18] Arquilla, John, and David Ronfeldt. "The Advent of Netwar." Rand, 1996.

[19] Arquilla, John and David Ronfeldt. “The Advent of Netwar (revisited) 1.” (2001).

[20] Krepinevich, Andrew F. "Cavalry to Computer: The Pattern of Military Revolutions." The National Interest, no. 37 (Fall 1994): 30-42.

controlling public opinion, destabilising government structures, disrupting critical infrastructure and conducting espionage activities[21].

However, the history of computer operations can be traced back to the 1960s, when they began to gain importance in military contexts and as a national security concern, even before the work of Arquilla and Ronfeldt[22].

Indeed, some noteworthy cyberattacks occurred during the 1960s, although the intent of these attacks was not explicitly related to cyber warfare as I understand it today. For example, in 1969, the ARPANET computer, the Internet's predecessor, suffered an attack called the 'Morris Worm', which disrupted the network and highlighted the need for more stringent security measures to protect computer systems[23].

In cyber operations, two types of activities are distinguished in importance and function: cyber intelligence operations and military operations. In his seminal article 'Cyber Warfare Will Not Take Place' (2012), Thomas Rid emphasises the need to distinguish between these two types of operations. Rid emphasises that cyber intelligence operations are strategic and focus on collecting and analysing data in cyberspace. These operations aim to gather vital information that can influence political and economic decisions; they require significant planning, time, dedication and commitment and often take place over an extended period. In contrast, military cyber operations aim to exploit cyber expertise to achieve military or strategic objectives. Such operations may include interventions to disrupt or destroy enemy cyberinfrastructures or defend one's own. Unlike cyber intelligence operations, they have a more direct and tangible impact on the battlefield or a nation's security[24].

Significant events occurred, such as discovering computer bugs, launching the Software Defined Network (SDN) project for secure communications, and some specific cyber attacks. However, understanding and awareness of cyber risks were still limited, and only later did cyber security and cyber warfare become more prominent and develop more advanced disciplines and strategies. The 'Morris Worm', a pivotal historical event, marked the beginning of a new era in cyber warfare. Its emergence, although not initially conceived with the intent I associate with cyber warfare today, underscored the potential of computer technology for both offensive and defensive applications. This context is crucial in understanding how strategies and tactics in cyberspace have evolved into the sophisticated tools used for intelligence and military objectives today.

1.3 The Uncharted Realm of Cyber Intelligence Operations: Challenges and Opportunities

Despite the valuable information provided by Rid, the specific role of cyber intelligence operations remains a relatively unexplored territory that requires further investigation and research. There are several reasons for this: firstly, cyber intelligence operations involve collecting and analysing information from cyber sources to inform decision-making. It can include monitoring cyber threats, assessing the capabilities of potential adversaries and

[21] Arquilla and Ronfeldt, "Cyberwar is Coming!", 141-165.
[22] Warner, Michael. "Cybersecurity: A Pre-history." Intelligence and National Security 27, no. 5 (2012): 781-799.
[23] Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." Security Studies 22, no. 3 (2013): 365-404.
[24] Rid, Thomas. "Cyber War Will Not Take Place." Journal of Strategic Studies 35, no. 1 (2012): 5-32.

understanding trends in the cyber landscape. Unlike traditional intelligence, the unique challenge of cyber intelligence lies in the sheer volume of data, the speed with which the cyber environment changes, the anonymity and the global reach of the actors involved. Secondly, these operations are about more than just defence. They also include offensive capabilities, where intelligence agencies might engage in cyber espionage, jamming or influence operations while keeping such operations secret. It blurs between purely defensive cybersecurity measures and more proactive strategies.
Buchanan emphasises the variability in the speed of cyber operations and the crucial importance of persistent attacks. He highlights how preparing specific steps in advance can add more complexity to this crucial area[25].
The role of intelligence in cyber operations is an essential, though still insufficiently explored, element of the current debate. Lindsay raises important questions about the nature of cyber operations, highlighting how intelligence plays a central role. He discusses the importance of organisational context and how intelligence can influence the design and implementation of cyber operations. Lindsay's work highlighted the complexity of the role of intelligence in cyber operations, highlighting how the analysis of information gathered through cyber operations can influence the planning and effectiveness of such operations. His work drew attention to the need for closer integration between intelligence and cyber operations, emphasising how understanding and interpreting information gathered through cyber operations is critical to the success of such operations[26].

2. Effectiveness of Cyber Operations: Are they Revolutionary or Evolutionary?

2.1 Cyber Pearl Harbor

It may be helpful to review the literature on cyber warfare through the lens of the historical evolution of cyber operations and their emergence and development over time. The controversial cyber Pearl Harbor concept can be discussed following this historical context. This term is always used to describe a potentially catastrophic cyberattack that could destroy critical national infrastructures. The Former U.S. Secretary of Defense Robert Gates first used this term to emphasise the vulnerabilities of the United States to cyber threats and the need for robust cyber defences. This concept has sparked considerable debate. Placing this concept in its historical context makes it possible to understand better the meaning and implications of such a catastrophic event.
Bruce Schneier, in his 2012 article entitled 'The Threat of Cyber War Has Been Grossly Exaggerated', openly calls the term cyber Pearl Harbor a myth, pointing out that so far, no cyber

[25] Buchanan, Ben. "The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations." Oxford University Press, 2017.
[26] Lindsay, Jon R. "The Impact of China on Cybersecurity: Fiction and Friction." International Security 39, no. 3 (2014/2015): 7-47.

attack has come close to the catastrophic scale of historical events such as the 9/11 attacks. Schneier warns against using this narrative to downplay the severity of current cyber incidents, arguing that it diverts attention from the natural and pressing issues within the cyber sphere. He advocates continued vigilance against evolving cyber threats, urging us to avoid narratives undermining current cyber challenges[27].

In particular, the cyber Pearl Harbour debate was stimulated by the publication of two significant articles. The first is by Lucas Kello, entitled 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft' from 2013, published in International Security. Kello focuses on the dangers and challenges of the 'information revolution' concept, highlighting the limitations and complexities of cyberspace in the context of theory and policy. The author warns against an oversimplified view of cyber conflict and emphasises the importance of understanding the nuances and complexities of cyberspace[28].

Some scholars have responded to Kello's fundamental analysis of cyber's destructive and revolutionary characteristics: Segal and Lindsay focus on different aspects.

In "Correspondence: A Cyber Disagreement" between Jon R. Lindsay and Lucas Kello, the discussion focuses on the ramifications of cyber warfare in global security, with Kello and Lindsay leading the narrative from two sharply contrasting points of view. Kello envisions cyber warfare as a paradigm-shifting force in the contemporary threat landscape, asserting its revolutionary potential based on several principles: first, the accessibility and ease of use of these technologies, which allow even smaller entities to exert significant influence; second, the inherent challenges in tracking and attributing cyber attacks, a characteristic that makes them a preferred tool for nations eager to ward off counterattacks; and finally, the threats posed to vital infrastructure such as energy pipelines and financial layers. On this last point, Kello emphasises the significant impact of cyber attacks on the functioning dynamics of modern societies[29].

In contrast, Lindsay adopts a more restrained perspective, questioning the scope of cyber warfare's transformative potential. He notes the relatively sporadic occurrence of large-scale attacks, arguing that cyber warfare operates within certain boundaries and constraints just like its conventional counterparts. Therefore, Lindsay advocates a broader security focus encompassing other pressing threats rather than disproportionately amplifying the cyber warfare narrative[30].

The article reveals a nuanced analysis, supported by a wealth of concrete evidence, which emerges as a vital contribution to the dialogue on cyber warfare. While Kello perceives the urgent need to formulate robust defence matrices to counter the growing threat of cyber warfare, Lindsay urges a more balanced approach, warning against overshadowing other imminent emergencies. Kello perceives cyber domination as a revolution in military affairs, heralding a radical alteration in the dynamics of warfare. In contrast, Lindsay proposes a more

[27] Schneier, Bruce. “The Threat of Cyber War Has Been Grossly Exaggerated.” CNN, July 31, 2012.

[28] Kello, Lucas. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” International Security 38, no. 2 (2013): 7-40.

[29] Lindsay, Jon R., and Lucas Kello. “Correspondence: A Cyber Disagreement.” International Security 39, no. 2 (2014): 181-207.

[30] Lindsay and Kello, “Correspondence: A Cyber Disagreement,” 181-207.

moderate perspective, arguing that it remains premature to delineate the long-term repercussions[31].

This article is an indispensable resource for understanding the complex dynamics that shape future warfare scenarios. It illuminates the prevailing discourse while offering a deeper understanding of the various ramifications of cyber warfare on the global security scene. This discussion naturally includes the complexities surrounding the identification of cyber attack instigators, the consequent obstacles in holding them accountable, and the potential threats to critical infrastructure systems. As such, it provides a solid foundation for the next segment of this literature review, which will focus on the nascent phases of cyber operations.

On the other hand, Adam Segal published 'Why Digital Pearl Harbor Makes Sense... and Is Possible' for the Carnegie Endowment for International Peace four years after Kello's article. This work explores the concept of a 'digital Pearl Harbor' and discusses its plausibility and potential consequences. Segal discusses the increasing dependence on digital networks and the vulnerabilities that result. The author also addresses the scepticism surrounding the concept of a 'digital Pearl Harbor', pointing out that the increasing digitisation of critical infrastructure and the evolving capabilities of cyber adversaries make the possibility of a large-scale cyber attack a genuine concern[32].

Although they differ in focus and perspective, Kello's and Segal's articles have essential points of contact. They highlight how cyberspace has introduced new vulnerabilities requiring a global rethinking of security policies and strategies. They also emphasise the need for a new understanding and an updated approach to security in the digital age, pointing out that old paradigms may no longer suffice. Furthermore, both authors call for critical reflection on how traditional theories of war, security and international relations must evolve to address the challenges posed by cyberspace effectively. This evolution is crucial to understanding and managing the complex dynamics of today's digital world. Through these two analyses, Kello and Segal provide an in-depth and critical view of the challenges posed by cyberspace, emphasising the need for innovative and adaptive thinking in the context of global theory, policy and security.

Despite the hyperbolic use of the term 'cyber Pearl Harbor' by some authors, it is essential to consider these different viewpoints in the debate. Many dispute the impact of information conflict on military operations, and the vision of a possible 'cyber Pearl Harbor' has led to intense debates on the actual usefulness and meaning of this concept.

Following Schneier, Robert Jervis, in his 2017 analysis 'Why a Cybersecurity Treaty Is So Difficult... and So Necessary', delves into the dangerous implications of comparing cyber attacks to a 'Pearl Harbor' event. Jervis points out that the dynamics of cyber conflict differ significantly from conventional warfare, requiring strategic and cunningly crafted responses. He warns against recklessly adopting the 'Pearl Harbor' analogy, as it could evoke an overreaction by nations, triggering a chain of negative repercussions on a global scale. Jervis

[31] Lindsay and Kello, "Correspondence: A Cyber Disagreement," 181-207.

[32] Segal, Adam. "Why Digital Pearl Harbor Makes Sense...and Is Possible." Carnegie Endowment for International Peace, 2017.

encourages in-depth reflection on the distinguishing factors between cyber conflict and traditional warfare, stimulating the development of strategies adapted to the cyber domain[33].
In summary, the dialogue around the 'Cyber Pearl Harbor' metaphor has been enriched by the critical perspectives of Schneier and Jervis, while Rid also promotes a refined understanding of cyber security. They uniformly encourage a move away from historical analogies, which not only misunderstand the true nature of cyber threats but also prevent the creation of effective and balanced responses to cyber attacks.

2.2 Cyberspace in International Relations: An Evolving Domain (2010-2017)

In the previous section, the analysis focuses on the debate around the concept of 'Cyber Pearl Harbor', exploring perceptions of cyber threats and how these can affect national and global security. In doing so, it tends to question the conflicting views on the severity and plausibility of large-scale cyberattacks, emphasising the debate on the need for continued vigilance against emerging threats in cyberspace. Continuing in this section, the focus is broadened to examine cyberspace as a key domain in international relations, highlighting how it has become a crucial sphere for global governance, cooperation, and conflict. This section emphasises the dual role of cyberspace both as a battleground for cyber conflict and as a platform for digital diplomacy and international collaboration.
As researchers Robert Reardon and Nazli Choucri defined in 2012 in their paper 'The Role of Cyberspace in International Relations,' cyberspace is a domain in which computer networks, information and communication technologies, and related human activities coexist. Although the prevailing narratives currently primarily describe cyberspace as a domain of conflict, Reardon and Choucri point to a growing body of research supporting cyberspace's influential role in governance and promoting global cohesion[34].
This space has become a contested frontier, a battleground of political and military rivalries that has led to the emergence of information warfare and cyberterrorism. At the same time, it serves as an instrumental apparatus of governance, paving the way for international cooperation through digital diplomacy and increased transparency. Moreover, it is a beacon that drives globalisation by improving global connectivity and creating pathways for broad cultural and commercial exchanges[35].
In the rapidly evolving realm of cyber operations - a term that encompasses defensive and offensive strategies in virtual space aimed at gathering intelligence, disrupting adversary networks and reshaping information systems - grasping the dynamism of cyberspace becomes crucial.

[33] Jervis, Robert. “Why a Cybersecurity Treaty Is So Difficult… and So Necessary.” The Washington Quarterly 40, no. 3 (2017): 7-22.
[34] Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." Paper presented at the International Studies Association Annual Convention, San Diego, CA, April 1, 2012.
[35] Lin, Herbert, and Jaclyn Kerr. "On Cyber-Enabled Information Warfare and Information Operations." In The Oxford Handbook of Cyber Security, edited by Paul Cornish. Oxford Handbooks, 2021; online edn, Oxford Academic, December 8, 2021.

Leading figures such as Adam Segal in 2016[36] and Lucas Kello in 2017 echo this sentiment, describing the cyber sphere as a multifaceted platform with promising opportunities and unforeseen challenges[37]. Kello and Segal unravel the subtle complexities of the digital cosmos, advocating a comprehensive approach to understanding it. While Kello urges a deep understanding of the information ecosystem, Segal accentuates the anxieties caused by an exponential dependence on digital platforms.[38].

2.3 Future Directions in Cyber Operations: Ethical Foundations and Security Strategies (2018-2022)

As outlined in Daniel Moore's article 'Offensive Cyber Operations: Understanding Intangible Warfare', delving into cyber operations involves exploring a domain with the potential to transform many aspects of the security and intelligence landscape, among other spheres. Moore embarks on a mission to meticulously analyse this vast territory, outlining domains characterised by intelligence accumulation, disruptive tactics, destructive methodologies and manipulative strategies, each with advantages and pitfalls. This field is involved in safeguarding critical information infrastructures and using strategies to counter cyber threats, thus playing a pivotal role in modern security strategies[39].

In common with his contemporaries, Moore foresees future steps towards aggressive cyber engagements and advocates a trajectory based on ethical standards and judicial involvement in the territory of cyber warfare. He calls for innovative research to develop new strategies, emphasising a two-way growth in which advances in cyber operations are accompanied by robust strategic responses, all deeply rooted in ethical convictions.

Browsing through Moore's insights, along with the analyses previously developed by Kello and Segal, it becomes clear that the horizon of international security increasingly gravitates towards cyber operations - an ever-evolving field that requires an acute understanding of its many facets, which encompass various activities on digital platforms aimed at exploiting advantages over potential adversaries. It embodies a range of strategies, from cyber espionage to sabotage. Furthermore, Moore accentuates the urgency of ethical considerations in this dynamic arena, calling for an enlightened path of moral stewardship and responsible interaction in navigating 'immaterial warfare'. The context imposes a vital need to cultivate innovation that respects moral constraints while promoting strategic and robust responses to emerging threats and challenges.

---

[36] Nocetti, Julien. "Review of The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age, by Adam Segal, and Internet Wars: The Struggle for Power in the 21st Century, by Fergus Hanson." International Affairs 92, no. 5 (2016): 1263–1266.

[37] Kello, Lucas. “The Virtual Weapon and International Order.” Yale University Press, 2017.

[38] Segal, Adam. “The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.” PublicAffairs, 2016.

[39] Moore, Daniel. Offensive Cyber Operations: Understanding Intangible Warfare. Oxford: Oxford University Press, 2022.

As I stand at the threshold of a future where cyber operations dictate the course, it is incumbent upon international security stakeholders to adopt a conscious approach that embraces technical sophistication and emphasises the essentiality of ethical adherence and responsible governance. The discourse envisages a future in which cyber operations skills will be a cardinal element in international relations and security[40]. The path based on innovation, responsibility and ethical foundations offers a way through the labyrinth of cyber warfare and supports a future in which digital interactions are marked by depth, stability and moral commitment.

3. The Limits of Cyber Operations

3.1 Complexities and Challenges of Cyber Warfare: An Integrated Analysis of Strategic and Operational Dynamics

This literature highlights the significant implications of cyber strategies for international security, highlighting the potential for misperceptions, escalation and conflict. This reflection emphasises the importance of policymakers' prudent and well-informed management of cyber operations to promote stability in the international system and mitigate the risks associated with cyber warfare.

Lindsay's article 'Stuxnet and the Limits of Cyber Warfare', published in 2013, offers a tangible perspective on cyber warfare by analysing a real-life case: the Stuxnet malware attack against Iran's nuclear enrichment facilities in 2010[41].

Examining this specific attack provides a complex picture of cyber warfare's strategic and operational challenges and reveals its limitations. Lindsay's approach fits perfectly with the themes later explored in Valeriano's[42], Jenson[43], Slayton[44] e Smeets[45] articles.

This article highlights the difficulties in achieving strategic objectives through cyber warfare, which Valeriano and Jenson also discussed.

Lindsay's analysis enriches the existing literature on the dynamics of cyber warfare, offering a real-life perspective and highlighting operational challenges and limitations. Together with subsequent works by Valeriano, Jenson, Smeets and Slayton, Lindsay provides a solid basis for understanding the complexities of cyber warfare and developing effective strategies to manage threats and promote stability in cyberspace.

---

[40] Under the oversight of thinkers like Moore, Kello and Segal, cyber operations have become a fundamental element in international relations and security. This is reflected in establishing dedicated cyber security agencies in various countries, such as the ANSSI in France and the ACN in Italy, highlighting the growing importance of cyber capabilities in national security strategy.

[41] Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” Security Studies 22, no. 3 (2013): 365-404.

[42] Valeriano, Brandon, and Ryan C. Maness. “The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11.” Journal of Peace Research 51, no. 3 (2014): 347-360.

[43] Jensen, Benjamin. “The Cyber Character of Political Warfare.” Brown Journal of World Affairs 24, no. 1 (Fall/Winter 2017–18): 159–171.

[44] Slayton, Rebecca. “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.” International Security 41, no. 3 (2017): 72-109.

[45] Smeets, Max. "A Matter of Time: On the Transitory Nature of Cyberweapons." Journal of Strategic Studies 41, no. 1-2 (2018): 6-32.

Lindsay's article on the Stuxnet attack grounds the discussion of cyber operations in an honest and influential case study, highlighting a crucial moment in the global perception of cyber warfare. This concrete example highlights the complexities, limitations and potential unintended consequences of cyber operations, establishing an empirical basis for subsequent arguments regarding the politics of cyber restraint and the importance of the balance between offensive and defensive cyber warfare. The discussion then expands to the work of Valerian, Jensen, Slayton and Smeets, creating a rich context for analysing cyber warfare not only as a technological tool but as a complex phenomenon with profound implications for international security and global politics.

The Stuxnet case illustrates the possible repercussions of offensive cyber operations. As Lindsay pointed out, there are unintended consequences, including the possibility that offensive technology can be reused and used against the attacker. This aspect further reinforces Valeriano and Jenson's argument about the need for a policy of cyber restraint, in which the focus on improving cyber defence balances offensive operations.

Valeriano and Jensen highlight the complex nature of cyber conflict, emphasising that success in this field is not guaranteed simply through advanced cyber capabilities. They explore the limitations of these operations in achieving strategic objectives, especially when compared to more traditional methods of coercion. Their work highlights the importance of integrating cyber warfare into a broader, multi-faceted approach to international security and strategy.

The Stuxnet case also illustrates the possible repercussions of offensive cyber operations. As Lindsay pointed out, unintended consequences occur, including the possibility that offensive technology can be reused and used against the attacker. This aspect further reinforces Valeriano and Jenson's point about the need for a policy of cyber moderation, where the focus on improving cyber defence balances offensive cyber operations.

Lindsay emphasises the importance of considering cyberattacks' strategic context and potential repercussions. This idea echoes Valeriano and Jenson's proposal for a cyber moderation policy and their emphasis on a robust cyber defence[46].

On the other hand, Slayton argues that the balance between offence and defence in cyberspace needs to be more accurate, focusing on the difficulties of achieving strategic goals through cyber warfare. She argues that the offence-defence balance can only be assessed using specific organisational and technological skills. She argues that the current success of offensive operations in cyberspace stems mainly from poor defence management and the relatively more straightforward objectives of the offensive. Furthermore, she points out that using cyber weapons can be very costly in exerting precise physical effects[47]. His empirical analysis of the Stuxnet attack against Iran's nuclear facilities suggests that this attack cost the offence much more than the defence. These points highlight that although cyberspace may seem like a favourable field for offensive operations, significant challenges and hidden costs make achieving concrete strategic objectives through cyber warfare complicated. Slayton highlights

[46] The debate on restraint and deterrence in the cyber domain is currently echoed in space discussions, an area still being explored within NATO and perhaps more advanced in EU discussions. It reflects the evolving nature of security strategies in new environments, where traditional concepts are adapted and reevaluated in light of emerging technologies and threats.

[47] Slayton, "What Is the Cyber Offense-Defense Balance," 73.

the importance of carefully considering both the costs and perceived benefits of cyber operations for attackers and defenders.

Lindsay also examines the potential unintended consequences of offensive cyber operations, which ties in with the analysis later made by Smeets, who discussed the risks and limitations of such operations. These themes are intertwined with Slayton's emphasis on the complexity of the balance between attack and defence in cyberspace and the associated evaluation challenges.

While Lindsay discussed the Stuxnet exploit, assessing the success or failure of a cyber operation is complex and nuanced. In this regard, Smeets' thesis is that cyber weapons are inherently transient. Indeed, Smeets argues that, unlike conventional weapons, cyber weapons quickly lose their effectiveness after their first use as the vulnerabilities they exploit are identified and corrected[48]. This dynamic makes cyberspace more 'malleable' than physical space. Indeed, once a patch for a specific vulnerability is created, it can be applied to many systems. Moreover, the transient nature of cyber weapons does not provide a significant advantage to weaker actors, as maintaining a constant offensive capability requires a continuous renewal of capabilities to counter transience. This implies that significant powers benefit more from this transient nature of cyber weapons, influencing the incentive structure for offensive actions in cyberspace and inducing a different funding structure for cyber (military) programmes than conventional weapons programmes. The time-related dynamics of cyber weapons also explain their limited use of espionage capabilities.

To deepen the analysis of the integration of offensive cyber capabilities, Smeets also addresses the issues of transparency and secrecy[49]. Just as the balance between attack and defence is crucial, so is the balance between transparency and secrecy. In particular, secrecy can act as a deterrent; keeping certain cyber operations hidden from the enemy can preserve elements of surprise and competitive advantage.

Another aspect that Smeets highlights concerns evaluating the effectiveness of offensive cyber operations. The limited empirical evidence, combined with the complexity of cybernetics, makes it difficult to determine the degree of offensive operations' success accurately. Smeets argues that, despite the challenges, evaluation remains a crucial component in developing offensive cyber strategies[50].

[48] Smeets, Max. "A Matter of Time: On the Transitory Nature of Cyberweapons." 6-32

[49] this point is crucial, both in terms of external dimension, naturally (strategic ambiguity), and for increasing internal legitimacy.

[50] Lindsay, “Stuxnet and the Limits of Cyber Warfare.”.

Smeets focuses on the international implications of integrating offensive cyber capabilities into military doctrines[51]. In line with Fanelli[52] Smeets highlights how offensive operations can significantly impact global security, regional stability and the international order.
Lindsay and Smeets' studies provide an in-depth look at the complexity of offensive cyber operations, illuminating the intricate balances that must be maintained, the strategic dilemmas that must be addressed and the challenges in assessing the effectiveness of such operations. They also emphasise the importance of the broader context, including geopolitical considerations and implications for national and international security. These articles offer valuable insights for policymakers, military personnel, scholars and all those who wish to understand the dynamics of cyberspace and its impact on contemporary society.
In the article entitled 'Cyber Campaigns and Strategic Outcomes', written with Richard J. Harknetta, Smeets also examines the concept of cyber warfare and emphasises that cyber operations consist of interconnected campaigns to achieve strategic outcomes without resorting to armed conflict strategies. The authors propose a different conceptual approach focused on cyber-strategic competition instead of cyber warfare, suggesting that cyber means can be considered a strategic alternative to warfare[53].
Sub-threshold cyber operations can have a strategic impact on national power and the distribution of power. This perspective challenges the predominant idea in the cyber literature that only highly destructive cyber attacks can achieve strategic advantage. This article's importance is expanding the construct of cyber warfare to include strategic cyber competition through information campaigns. This new approach is crucial for developing effective policies to protect the sources of national power in cyberspace, representing a new dimension through which relative power can be challenged without resorting to armed conflict. The authors emphasise the need for an in-depth study of information technology and its implications for war and militarised crises and call for further research on these issues. In conclusion, the article promotes openness in the study of cyber security and emphasises the need to understand cyber means, not only as tools for war but as strategic tools to achieve goals not necessarily associated with war.

[51] Doctrines that integrate offensive cyber capabilities include:
United States' Department of Defense Cyber Strategy (2018): Emphasizes "Defend Forward" and "Persistent Engagement" strategies involving offensive cyber operations to deter and respond to threats before they impact U.S. critical infrastructure.
NATO's Cyber Defence Policy: Recognizes cyberspace as an operational domain, allowing the use of offensive cyber capabilities in collective defense and to support NATO operations.
Russian Military Doctrine (2014): Emphasizes the importance of offensive cyber operations for national sovereignty protection and as a strategic tool against external threats.
China's Science of Military Strategy (2013): Describes the integration of offensive cyber operations into China's military strategies, highlighting the role of cyberspace in modern warfare.
[52] Fanelli, Robert L. and Gregory J. Conti. “A methodology for cyber operations targeting and control of collateral damage in the context of lawful armed conflict.” 2012 4th International Conference on Cyber Conflict (CYCON 2012) (2012): 1-13.
[53] Smeets, Max, and Richard J. Harknett. “Cyber Campaigns and Strategic Outcomes.” Journal of Strategic Studies, 2022.

Lindsay's article, combined with subsequent contributions by Valeriano[54], Jenson[55], Slayton and Smeets offer a comprehensive view of the dynamics and challenges of cyber warfare.
This literature suggests that although offensive cyber operations may offer some strategic advantages, their effectiveness and impact are heavily influenced by contextual factors and operational limitations. Therefore, an effective cyber strategy should carefully balance offensive and defensive approaches, considering possible consequences and working to promote stability and security in cyberspace. Lindsay's overview of the Stuxnet case highlights how operational reality may differ from theoretical expectations within the vast literature on cyber warfare. This case challenges the idea, put forward in some academic and political debates, that offensive cyber operations can offer a decisive advantage. Although Stuxnet effectively disrupted Iran's nuclear programme, the overall impact was limited and did not significantly alter the strategic balance in the Middle East.
This assessment further underlines Smeets' observations regarding the challenges of using cyber warfare to achieve defined strategic objectives. Contextual factors, including the adversary's level of preparedness and the possibility of adequate countermeasures, strongly influence the effectiveness of such operations. As Slayton pointed out, the balance between attack and defence in cyberspace is dynamic and can vary depending on specific circumstances.
The Stuxnet case also illustrates the possible repercussions of offensive cyber operations. As Lindsay pointed out, unintended consequences occur, including the possibility that offensive technology can be reused and used against the attacker. This aspect further reinforces Valeriano and Jenson's argument about the need for a policy of cyber moderation, in which a focus on improving cyber defence balances offensive operations.

3.2 Dynamics of Conflict in Cyberspace: An Integrated Examination of Cyber Operations and their Strategic Implications

Thomas Rid's book Cyber War Will Not Take Place should be revisited in light of the other works considered here. This book critically examines cyber warfare, challenging the prevailing assumption that cyberspace represents the next frontier of conflict. Rid argues that, despite their increasing prevalence, offensive cyber activities do not meet the traditional criteria of warfare. Instead, he proposes that cyber operations are better described as espionage or sabotage than actual acts of war. Rid also challenges the effectiveness of cyber deterrence, suggesting that anonymity and the absence of established norms in cyberspace make traditional deterrence less effective[56].
This critical approach provides an exciting contrast to the other works examined. While Valeriano, Jensen and Maness[57] view cyber capabilities as an extension of traditional power mechanisms, Rid questions their ability to produce armed conflict in the traditional sense. At

[54] Valeriano, Brandon, and Benjamin Jensen. "The Myth of the Cyber Offense: The Case for Restraint." Policy Analysis no. 862, Cato Institute, January 15, 2019.
[55] Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. Cyber Strategy: The Evolving Character of Power and Coercion. Oxford: Oxford University Press, 2018.
[56] Rid, Thomas. 2013. Cyber War Will Not Take Place. Oxford: Oxford University Press.
[57] Valeriano, Jensen, and Maness, Cyber Strategy, 2018.

the same time, his work is in tune with the points raised by Smeets regarding the challenges inherent to attribution and deterrence in the cyber domain.

Rid's thesis highlights the value of a nuanced approach to understanding cyber operations. It emphasises the importance of considering the specificities of the cyber domain in terms of anonymity, lack of norms and the intersection of state and non-state actors. In doing so, Rid contributes to a 'matrix' understanding of cyber warfare, in which cyber operations are integrated into a broader range of strategic activities. This theme resonates with the observations made by Kostyuk and Zhukov[58] regarding the interaction between cyber operations and conventional warfare.

'Brandishing Cyberattack Capabilities' by Martin C. Libicki, published in 2013, represents a further significant contribution to understanding cyber operations and strategic implications in the context of international relations. The report consistently links to previous articles' themes and perspectives examined above. Libicki analyses the challenges associated with using cyberattack capabilities as a deterrent and highlights the crucial differences between conventional and nuclear capabilities. The author highlights the peculiarities of cyberspace, such as complex attribution, the dynamic nature of vulnerabilities, and the importance of secrecy regarding offensive cyber capabilities. The paper delves into some critical challenges in using cyber capabilities for deterrence, including cyber weapon signalling, attack attribution, escalation risks and the dynamic nature of the balance between offensive and defensive capabilities in cyberspace. However, Libicki suggests that despite these challenges, cyber capabilities can still play a deterrent role if adequately understood and managed. The author emphasises the importance of a deep understanding of the unique dynamics of cyberspace and its limitations in integrating cyber capabilities into deterrence strategies[59].

Libicki enriches the existing literature on cyber operations by offering a clear perspective on the challenges and implications of using cyber attack capabilities as a deterrent. The report consistently builds on previous work, contributing to the overall understanding of the dynamics and strategies in information technology operations. Libicki emphasises the importance of carefully considering the risks and challenges of using cyber attack capabilities as a deterrent. He also highlights the potential benefits and opportunities cyber capabilities can offer to build broader deterrence strategies. The continuity with previous articles lies in constantly reflecting on cyber operations' complex and evolving nature and their strategic implications[60].

For example, the article 'The Law of Cyber Attack' by Michael N. Schmitt analyses the legal implications of cyber attacks, examining how international law applies to cyber operations[61]. Schmitt discusses the relevance of international humanitarian law and international law to cyber operations and points out that the application of these rules can be complicated by the unique nature of cyberspace and the inherent challenges such as anonymity, speed and difficulty of attribution. He concludes his article by arguing for a more in-depth debate on the

[58] Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible Digital Front: Can Cyberattacks Shape Battlefield Events?" 2017.

[59] Liebetrau, T. 2023. "Organizing Cyber Capability Across Military and Intelligence Entities: Collaboration, Separation, or Centralization." Policy Design and Practice 6, no. 2: 131-145.

[60] Liebetrau, "Organizing Cyber Capability," 131-145.

[61] Schmitt, Michael N. "Rewired Warfare: Rethinking the Law of Cyber Attack." International Review of the Red Cross 96, no. 893 (2014): 189-206.

regulation of cyber operations, emphasising the importance of adapting existing laws to meet better the challenges posed by cyber warfare.

This view complements the contributions of Lindsay, Smeets, Kostyuk, and Zhukov. It extends the analysis to the legal and regulatory implications of cyberattacks and provides a comprehensive view of cyberspace's role in contemporary conflicts, exploring the strategic, operational, tactical, and legal dimensions of cyber attacks. However, this overview must be completed and requires further research, particularly about cyberspace's technological evolution and dynamics.

Wiener's article, 'Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation', published in 2016, further contributes to understanding the growing importance of cyber operations in the military. Wiener explores the evolution of computer operations from their initial use as a defence to their current role in offensive strategies. The article emphasises the importance of penetrating adversary networks, exploiting vulnerabilities, disrupting related operations, and destroying related capabilities. The increasing reliance on information technology and interconnected systems drives this evolution. The author recognises the challenges associated with computer network operations, such as complicated attribution and potential collateral damage, and emphasises the need for legal and ethical frameworks to regulate the use of these operations in armed conflict. This aspect links Wiener's article to Schmitt's analysis of the legal implications of cyber attacks[62].

Furthermore, Wiener explores the concept of 'asymmetry' in computer network operations, where more minor or less technologically advanced actors can inflict significant damage on superior military powers through cyberattacks. Wiener's article emphasises the importance of intelligence in computer network operations, highlighting the need to understand adversary networks, vulnerabilities and exploitation points. Finally, the author explores perspectives on computer network operations, including the integration of artificial intelligence machine learning and autonomous systems. These developments point to the need to continue studying cyberspace's technological evolution and dynamics, as suggested in the existing literature[63].

"The Logic of Coercion in Cyberspace" by Borghard and Lonergan, published in 2017, offers another lens through which to examine the role of cyber operations in international coercion. This research is an essential addition to the previous works discussed, particularly those of Valeriano, Jensen and Maness, offering further insights into the multifaceted nature of cyber operations[64].

Borghard and Lonergan apply concepts of traditional military coercion to the cyber domain, proposing a framework for understanding how credibility, reporting, and determination play critical roles in coercive strategies in cyberspace. They highlight how the peculiarities of the cyber domain - such as anonymity, complicated attribution and potentially rapid escalation - can present both obstacles and opportunities for state actors seeking to exploit cyber capabilities for coercive purposes. Borghard and Lonergan's work offers a fascinating analysis

[62] Wiener, Craig. “Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation.” (2016).

[63] Wiener, Craig. “Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation.” 2016.

[64] Borghard, Erica D. and Shawn W. Lonergan. “The Logic of Coercion in Cyberspace.” Security Studies 26 (2017): 452 - 481.

of case studies such as the 2007 Estonia cyberattacks, Operation Stuxnet and the 2014 Sony Pictures attack, offering valuable insights into the challenges and opportunities presented by cyber coercion.

This study resonates with Rid's previous observations on the importance of a nuanced approach to understanding cyber operations and further expands Kostyuk and Zhukov's understanding of how cyber operations can shape events on the battlefield. Borghard and Lonergan point out that although cyber capabilities can offer new tools of coercion, their effectiveness depends mainly on how states deal with the unique challenges posed by cyber domination. This is a recurring theme throughout the literature, emphasising the importance of carefully considering context when assessing the effectiveness of cyber operations[65].

The approach taken by Borghard and Lonergan is to apply traditional concepts of military coercion to the context of cyberspace. They argue that although cyberspace presents unique challenges, the dynamics of power and coercion in this domain can be understood and analysed using established concepts. The authors explore the critical factors of credibility, signalling and determination as building blocks for successful coercion in cyberspace. They emphasise that despite the peculiarities of cyberspace, such as anonymity and the difficulty of attribution, coercive strategies can still be effective if based on these principles. Through the analysis of relevant case studies, Borghard and Lonergan demonstrate how targeted cyber attacks can influence the balance of power between state actors and shape the outcomes of conflict dynamics. However, they also highlight the unique challenges associated with coercion in cyberspace, such as rapid escalation and the need to maintain long-term credibility and resolve.

In their article "Invisible Digital Front: Can Cyberattacks Shape Battlefield Events?" published in 2017, Kostyuk and Zhukov extend the analysis of cyber conflicts to the context of conventional warfare. Just as Smeets examined the integration of offensive cyber capabilities into military doctrines, Kostyuk and Zhukov emphasise the critical role of cyber operations in battlefield dynamics and highlight how cyberattacks can influence the outcomes of conventional military conflicts[6667]. Through historical analysis and quantitative data, the authors show how cyber interference can disrupt communication networks, surveillance systems and critical infrastructure, resulting in tangible effects on the battlefield. However, they also note that the effectiveness of such attacks can vary depending on several factors, such as the robustness of the adversary's cyber defences, the sophistication of the attack tools and the integration of cyber operations with conventional military activities.

Kostyuk and Zhukov's analysis further complements and enriches the literature on cyber conflict and reaffirms the importance of continuing research on the interaction between cyber operations and conventional warfare, given the rapidly evolving cyber domain and its

[65] Borghard and Lonergan, “The Logic of Coercion in Cyberspace,” 452-481.

[66] Kostyuk and Zhukov's 2017 study, "Invisible Digital Front: Can Cyberattacks Shape Battlefield Events?", extends the analysis of cyber conflicts within conventional warfare. Echoing Smeets's examination of the integration of offensive cyber capabilities into military doctrines, they highlight the significant role of cyber operations in battlefield dynamics. They highlight how cyberattacks can influence the outcomes of conventional military conflicts, with notable examples including the 2007 cyberattacks against Estonia, the 2008 Russia-Georgia war, and the 2010 Stuxnet operation against Iran. These cases demonstrate the growing integration of cyber strategies into modern warfare since 2007.

[67] Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible Digital Front: Can Cyberattacks Shape Battlefield Events?" 2017.

increasing role in defining the outcomes of military operations. Conflicts. Their findings underline the need for a deeper understanding of the dynamics, challenges and implications of cyber attacks for national and international security[68]. Finally, studies in the literature investigate the legal and regulatory repercussions of cyber attacks.

"Cyber Strategy, the Evolving Character of Power and Coercion", by Brandon Valeriano, Benjamin Jensen and Ryan C. Maness, further expands the understanding of cyber operations in international relations. This book studies the emerging role of cyber strategies in the chessboard of global power, examining how nations can use their cyber skills to exert influence and coercion in the digital domain. According to the authors, cyber strategies represent an extension of traditional power mechanisms in international relations rather than a revolutionary form of conflict. Like traditional military, economic and diplomatic resources, states use cyber capabilities to further their strategic objectives[69].

The book details the cyber strategies adopted by various countries, focusing on the cases of the US, Russia, China and Iran, providing an in-depth insight into the motivations, goals and tactics of different state actors in the cyber environment. Key topics covered in the book include the nature of coercion in cyberspace, the use of cyber skills to achieve political and military ends, the role of deterrence in the cyber domain, and the challenges of attribution in cyber conflict.

This work enriches the understanding of the role of cyber strategies in international relations. The authors emphasise how cyber expertise while introducing new dynamics into global politics, must be seen within a broader strategic context and not as an isolated phenomenon. This perspective is in line with previous research by Lindsay, Smeets, Kostyuk, Zhukov, and Schmitt.

Various other authors and scholars have analysed the challenges and implications of using attack and defence capabilities in cyber operations. Cavelty and Chesney[70] addressed various issues, applications, and uses of ontologies in cyber operations, while Sanger[71] focused on degradation and sabotage operations.

"No Shortcuts: Why States Struggle to Develop a Military Cyber-Force" provides an in-depth and comprehensive analysis of the challenges faced by states in developing military cyber capabilities. As discussed earlier, Smeets enters this discussion by exploring states' efforts to build a military information capability in cyberspace. The author addresses the complexity of the cyber domain and argues that many states face significant obstacles in entering cyber conflict. For Smeets, bridging the gap between technology and policy is necessary: these are essential components for building a military information capability. In addition, the book addresses the challenges of assessing the effectiveness of cyber operations by discussing the limitations of transferring capabilities between states and private actors in the field of cyber operations[72].

---

[68] Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible Digital Front: Can Cyberattacks Shape Battlefield Events?" 2017.

[69] Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. 2018. Cyber Strategy: The Evolving Character of Power and Coercion. Online edition. Oxford: Oxford Academic. Accessed November 11, 2023.

[70] Dunn Cavelty, Myriam and Andreas Wenger. “Cyber security meets security politics: Complex technology, fragmented politics, and networked science.” Contemporary Security Policy 41 (2020): 32 - 5.

[71] Sanger, David E. 2021. The Perfect Weapon: War, Sabotage and Fear in the Cyber Age.

[72] Smeets, Max. 2022. No Shortcuts: Why States Struggle to Develop a Military Cyber-Force. London: Hurst.

4. Offence-Defence Balance in Cyberspace

4.1 Cyber Posturing and the Offense-Defense Dynamics in Cybersecurity Literature

Although much attention has been paid in the literature to the characteristics of computer operations[73], the critical role these operations play in intelligence needs to be addressed and is worthy of further investigation. In this context, Saltzman's 2013 article[74], 'Cyber Posturing and the Offense-Defense Balance', published in Contemporary Security Policy, offers a unique perspective. Saltzman examines how cyber posturing - the demonstration or signalling of a state's cyber capabilities and intentions - can influence the offensive-defensive balance in cyberspace. Saltzman analyses how cyber posture can lead to various outcomes, influenced by the intentions of the actors and the cyber capabilities exhibited. According to him, the cyber posture of a state can have both a stabilizing and destabilizing impact on the offensive-defensive balance and the overall security environment. The article provides a solid conceptual framework for discussing the balance between offence and defence in cyberspace, a central theme in this section.

Saltzman addresses several issues in the article that provide further insight into the complexity of cyber posture. One critical discussion point concerns using cyber posture as a deterrent tool. Saltzman illustrates how states can use their cyber posture to communicate their cybersecurity capabilities and resolve signalling and credibility dilemmas in cyberspace, thereby enhancing their deterrence and management of international perceptions; this manifestation of a state's capabilities and intentions can deter potential adversaries from engaging in cyber attacks. Awareness of a potential effective counterattack or robust defensive measures can strengthen deterrence, thus supporting a more stable balance in the cyber environment.

The other relevant aspect examined by Saltzman is the ambiguity inherent in cyber posture, which stems from the elusive nature of cyber attacks, the attribution of which is often difficult to establish with certainty[75]. Furthermore, the duality of cyber capabilities, which can be used for offensive or defensive purposes, contributes to this sense of uncertainty. This ambiguity can lead to misperceptions, with the potential risk of inadvertent escalation. Therefore, managing and mitigating this ambiguity represents a significant challenge to maintaining a stable security balance in cyberspace.

---

[73] National Research Council. 2009. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Washington, DC: The National Academies Press.

[74] Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance." Contemporary Security Policy 34, no. 1: 40-41.

[75] By discussing ambiguity in cyber posture, Saltzman contributes to a field of study in which many experts have expressed similar concerns. For example, Thomas Rid and Ben Buchanan are among the scholars who have explored the challenges of attribution in cyberspace in detail. Rid, in his work "Cyber War Will Not Take Place", and Buchanan, in "The Cybersecurity Dilemma", both address the issue of ambiguity and difficulties in attributing cyber attacks, underlining how these characteristics influence the defence strategy and international politics. So, while Saltzman offers an essential and valid perspective on the topic, he is not the only one discussing these issues. His analysis is part of a broad debate that includes several experts and scholars who have recognized and explored attribution ambiguity as a fundamental challenge in cybersecurity. The convergence of these voices highlights the critical importance of the problem and pushes towards developing more sophisticated tools and multilateral approaches to address ambiguity in the attribution of cyber attacks.

Fanelli's 2016 article "Cyberspace Offense and Defense" expands the debate on cyberspace operations by focusing on the interaction between offensive and defensive capabilities. The author examines the balance between attack and defence in cyberspace, analyzing factors such as target systems' vulnerability and actors' capabilities. The article also addresses the challenges of planning and conducting cyber operations, including the difficulty of attribution and the risk of unintended consequences[76]. Fanelli extends the discussion on the impact of cyber conflict on national security and military strategy by emphasizing the importance of developing robust cyber defences and the potential strategic advantage of offensive capabilities. The article provides an in-depth perspective on the challenges, opportunities and implications of defence and attack in cyberspace[77].

Slayton offers further insight into the dynamics between attack and defence in cyberspace in his article 'What is the Cyber Offense-Defense Balance? Concepts, Causes and Evaluation', published in International Security. Slayton's analysis focuses on the balance between cyber attack and defence and its implications for international security, critically examining the premises of this balance and the elements that influence it, including its conceptual underpinnings, the forces that shape it, and the difficulties in making an accurate analysis[78].

Slayton points out how scholars and practitioners have developed different interpretations of this attack-defence balance[79], highlighting the importance of considering it as a dynamic and context-dependent phenomenon rather than a static and universal feature of cyber conflict. Furthermore, the author investigates the factors that can influence the attack-defence balance in cyberspace; among these, Slayton highlights the nature of the targets, the capabilities and intentions of the actors involved, and the degree of vulnerability of the targeted systems.

Slayton's analysis also includes the challenges of assessing the attack-defence balance in cyberspace, recognizing the complexity of measuring it due to the lack of reliable data, evolving cyber threats and defences, and the secrecy that often surrounds information technology—state capabilities. The article considers the possible implications of the attack-defence balance in cyberspace for international security, analyzing the risks of misperception, escalation and conflict. Slayton suggests that a deeper understanding of this balance could support political governance in formulating more effective strategies to manage cyber threats and promote stability in the international system. In summary, Slayton's article offers a detailed and multifaceted view of the balance between attack and defence in cyberspace, highlighting the complex dynamics of cyber conflict and its impact on international security.

The academic literature presents different perspectives on the balance between attack and defence in cyberspace. In the context of this debate, Saltzman's work examines the concept of cyber posture as a deterrent tool, highlighting how states can communicate their cyber security capabilities and act to deter potential adversaries[80]; However, this display of expertise can also

[76]Fanelli, R. “Cyberspace Offense and Defense.” Journal of Information Warfare 15, no. 2 (2016): 53–65. https://www.jstor.org/stable/26487531.

[77] Fanelli, R. “Cyberspace Offense and Defense.” Journal of Information Warfare, 2016.

[78] Slayton, Rebecca. “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.”, 2017.

[79] Calcara, Antonio, Andrea Gilli, Mauro Gilli, and Ivan Zaccagnini. "Will the Drone Always Get Through? Offensive Myths and Defensive Realities." Security Studies 31, no. 5 (2022): 791-825. Routledge.

[80] Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance." Contemporary Security Policy 34, no. 1: 40-41.

generate ambiguity due to the elusive nature of cyber attacks and the duality of cyber capabilities. Smeets, in his article 'The Strategic Promise of Offensive Cyber Operations', published in Strategic Studies Quarterly, explores the potential strategic benefits of offensive cyber operations. Smeets carefully evaluates the effectiveness of these operations in achieving national security objectives, examining different types, including cyber espionage, cyber sabotage and cyber coercion[81].

Smeets argues that cyber espionage can provide crucial information on adversaries' capabilities, intentions and vulnerabilities, allowing policy decisions to be based on more precise national security knowledge. The article also examines cyber sabotage as a strategic tool to weaken an adversary's military, economic and political capabilities. In contrast, cyber coercion can be a means to influence adversaries' behaviour by threatening or demonstrating the ability to carry out cyber attacks. However, Smeets also emphasizes the challenges associated with offensive cyber operations, such as the communication of intentions, the risk of escalation and possible unintended consequences, and therefore recommends carefully assessing such operations' risks and potential strategic benefits.

Smeets' work enriches the discussion on the balance between attack and defence in cyberspace by offering a perspective that views offensive cyber operations as a strategic tool to achieve national security objectives. This view complements Saltzman's, highlighting the importance of coordination in cyberspace and the need to manage the ambiguity arising from the duality of cyber capabilities[82].

Valeriano and Jenson, in 'The Myth of the Cyber Offense: The Case for Cyber Restraint', challenge the dominant idea that the offensive prevails over the defensive in cyber. This policy analysis, published by the Cato Institute, states that the belief in the hegemony of cyber offensive capabilities is rooted in various misunderstandings and myths that have political effects. The authors analyze the nature of cyber conflict, the balance between attack and defence in cyberspace, and the strategic repercussions of an offensive orientation. They advocate cyber moderation, pointing out that defensive strategies are often more efficient and less likely to cause escalation than offensive ones. This article by Valeriano and Jenson is full of valuable observations. First, the two authors challenge the widely accepted assumption of cybercrime dominance, pointing out that this perceived superiority of cybercrime is rooted in a misunderstanding of the balance between attack and defence in cyberspace. According to them, many cyber-attacks need to achieve the effectiveness or level of disruption commonly attributed to them. Furthermore, they insist that defence strategies can effectively prevent and mitigate attacks[83].

Valeriano and Jenson examine the inherent limitations of offensive cyber operations, which are far from being a panacea and involve several complications such as difficulties in achieving strategic objectives, risk of escalation and challenges of attribution and communication. Next, the authors highlight the benefits of investing in defensive measures, citing network resilience,

[81]Smeets, Max. “The Strategic Promise of Offensive Cyber Operations.” Strategic Studies Quarterly 12, no. 3 (2018): 90–113.

[82] Smeets, Max. “The Strategic Promise of Offensive Cyber Operations.” 2018.

[83] Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. Cyber Strategy: The Evolving Character of Power and Coercion. Oxford: Oxford University Press, 2018.

threat intelligence and incident response capabilities. They argue that a robust cyber defence can deter adversaries, reduce the impact of attacks and decrease the likelihood of escalation.
Finally, Valeriano and Jenson present their case for cyber moderation. Instead of advocating an offensive approach, they argue that states should focus on developing strong defensive capabilities and continuous diplomatic efforts to establish norms and rules to ensure responsible behaviour in cyberspace.
In reality, states focus on cyber coercion, i.e. the use of capabilities and actions in cyberspace, such as attacks or threats of cyber attacks, to influence or coerce another actor to change their behaviour or make specific decisions instead of understanding the lack of coordination for several reasons. The first is that cyber coercion, or the use of cyber threats to achieve specific policy objectives, is a more attractive option in terms of costs and benefits than defensive efforts. Cyber coercion allows states to gain strategic advantages without facing the challenges and complexities of cyber defence. Furthermore, cyber coercion can exert pressure on other states, influence political decisions or damage adversary infrastructure.
However, the lack of defence coordination can be attributed to factors such as the very nature of cyberspace, which is open, global and interconnected, making it difficult to establish effective coordination between state actors. Cyber defence requires collaboration between governments, international organizations and the private sector; a lack of mutual trust between the various actors involved at different levels and inadequate coordination mechanisms may hinder such efforts. Some states may even prefer to maintain a strategic advantage by exploiting vulnerabilities in cyberspace rather than share their knowledge and defensive resources. This may be motivated by political considerations, national interests, the desire to keep cyber defence tools and capabilities secret, and the difficulty of coordinating the operational and tactical level with the technical level.
Slayton's studies and those of Valeriano, Jenson and Smeets offer a comprehensive overview of the dynamics of attack and defence in cyberspace. They emphasize the importance of a balanced approach that considers the potential benefits of offensive operations, as emphasized by Smeets, and effective defence and containment strategies, as suggested by Valeriano and Jenson. At the same time, these studies highlight the importance of understanding the attack-defence balance in cyberspace as a complex and dynamic phenomenon influenced by several contextual factors. This viewpoint, expressed by Slayton, challenges the more static and monolithic views of the attack-defence balance and suggests that more attention should be paid to variability and uncertainty in analyzing cyber threats and defences[84].

4.2. Balancing Offense and Defense in Cyber Operations: A Review of the Evolving Cybersecurity Landscape

Overall, this literature review shows how scholars and experts have examined various aspects of cyber operations, including cyber offence and defence, the role of cyber capabilities in international relations, the logic of coercion in cyberspace, and the challenges of cyber deterrence. These research studies offer a comprehensive overview of the dynamics, dilemmas

[84] Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. Cyber Strategy: The Evolving Character of Power and Coercion. Oxford: Oxford University Press, 2018.

and opportunities associated with cyber operations, providing valuable information for understanding and managing conflicts in cyberspace.

A critical aspect of the literature concerns the lack of a 'common design' that can effectively combine offensive and defensive operations in the context of cyber operations. The lack of an adequate balance between these two dimensions represents a significant gap that requires special attention. Assessing the effectiveness of cyber operations and distinguishing between attack and defence is inherently complex, especially in the absence of actual conflicts in which such operations have been deployed. The literature emphasises the importance of developing a coherent and integrated strategy that considers both offensive and defensive aspects in cyberspace; however, the lack of proper coordination in offensive and defensive operations leads to inefficiencies, vulnerabilities, and limitations in cyber threat management. Furthermore, cyberspace's elusive and changing nature makes it difficult to establish precise and reliable parameters[85]. Without a thorough understanding of the impact and outcomes of cyber operations, it becomes difficult to design coherent strategies and optimise available resources.

The lack of a 'common design' that integrates effective coordination in offensive and defensive operations in cyberspace is a significant challenge that requires an adequate response.

The aforementioned authors and others such as Glaster and Kaufmann[86], Buchanan[87], Fischerkeller and Harknett[88] emphasise the predominance of offence over defence in cyber operations.

Slayton emphasises[89] the role of organisational processes and the cost of bureaucracy in balancing defence and attack. However, the complexity of cyber operations makes it difficult to implement defence and attack successfully. Furthermore, the idea of a clear distinction between offensive and defensive operations in cyberspace is questioned. Healey[90] argues that understanding who has the advantage is optional, and that cyber persistence could be a strategic response to counter-offensive cyber actions. Modern technology's dynamic and adaptive nature undermines the clear distinction between attack and defence. Consequently, measuring the success or failure of cyber operations becomes a daunting task, making the theory indeterminate[91].

---

[85] An example is the 2020 SolarWinds cyber espionage campaign, where sophisticated attackers infiltrated numerous government and private sector networks. The delayed detection and fragmented response showcased the challenges in coordinating offensive and defensive operations across different jurisdictions and organizations. This incident underscored the importance of a unified and collaborative approach in both anticipating potential threats and responding promptly to breaches in the cybersecurity landscape.

[86] Glaser, Charles L., and Chaim Kaufmann. “What Is the Offense-Defense Balance and How Can We Measure It?” International Security 22, no. 4 (1998): 44–82.

[87] Buchanan, Ben. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge, MA: Harvard University Press,

[88] Fischerkeller, Michael P., and Richard J. Harknett. “Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation.” The Cyber Defense Review, 2019, 267–87.

[89] Slayton, Rebecca. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." International Security 41, no. 3 (2016): 72-109.

[90] Healey, Jason, Patricia Mosser, Katheryn Rosen, and Alexander Wortman. 2021. "The ties that bind: A framework to assess the linkage between cyber risks and financial stability." Journal of Financial Transformation 53: 94-107. Capco Institute.

[91] Healey, Jason and Neil Jenkins. “Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing.” 2019 11th International Conference on Cyber Conflict (CyCon) 900 (2019): 1-20.

Conflict in cyberspace is a continuum, where small actions can accumulate and interact with significant factors, such as territoriality, to generate larger conflicts. The distinction between offensive and defensive operations does not directly impact the actions that lead to war but can provide clues as to when war might occur. However, states' defensive capability in the context of cyber operations is often limited by bureaucratic, financial, and knowledge issues.

This literature review emphasises that, rather than the traditional literature's standard design between defence and attack, there needs to be a proper treatment of the coordinating role of cyber operations. Indeed, there is a need for coordination in cyber operations, highlighting the need to explore the role of cyber operations further and overcome existing gaps, such as the lack of a standard design that effectively combines offensive and defensive operations. The future of cyber operations may not fundamentally alter the warfare landscape, but it remains essential to carefully examine the challenges and opportunities that cyberspace offers states in pursuing new and informed objectives.

Recognising that cyber operations will not replace traditional warfare but will become increasingly relevant in pursuing specific objectives is crucial. Therefore, future research should focus on a research design that effectively integrates offensive and defensive operations in cyberspace and present original and innovative case studies that empirically demonstrate the evolution of such operations. Furthermore, it is crucial to recognise that the traditional distinctions between offensive and defensive operations in cyberspace are increasingly blurred. Modern technologies' dynamic and adaptive nature makes it complex to draw a clear line between attack and defence. This blurring poses challenges in assessing the success or failure of operations, as the effects can be complex and interconnected.

However, despite the blurring of distinctions, cyber operations remain a crucial element of the contemporary strategic landscape. The articles and books cited highlight how cyber operations could influence battlefield events, affect international relations and be used as a tool of deterrence. Cyber operations' role goes beyond destroying material capabilities and focuses primarily on information; their use for espionage is widespread in cyberspace, but offensive capabilities can also be exercised to target, degrade and sabotage an adversary's critical infrastructure. Understanding the balance between attack and defence in cyberspace is critical to developing an effective cyber strategy. While some argue that offence prevails over defence in cyber conflicts, others emphasise the importance of defence and threat resistance.

4.3 Exploring Gaps in Cybersecurity: Beyond Offense-Defense Balance

The existing literature on the offensive-defensive balance in cyberspace is extensive and informative, but some areas need further investigation. One of the least explored aspects is the integration of perspectives from different disciplines, such as psychology and sociology, to understand the motivations and repercussions of cyberattacks better. This multidisciplinary approach could offer a more comprehensive view of the dynamics of cyberspace. Another significant gap concerns the economic and social impact of cyber conflicts. It is essential to

examine how these conflicts affect national economies, critical infrastructures and citizens' daily lives, as well as the implications for security and military strategy[92].

International cooperation and norms in cyberspace are other areas that deserve more attention (apart from the coordination discourse). It is essential to explore how international norms and interstate coordination influence the balance between offensive and defensive, and the challenges in building global consensus and enforcing these norms. The advancement of technologies, particularly artificial intelligence, is changing the landscape of cyberspace. Studying how these emerging technologies affect the offensive-defensive balance could reveal new dynamics and challenges. Furthermore, the private sector's resilience in the context of cyber defence is a critical area. It is important to consider the role of the private sector in resisting and responding to cyber-attacks. An under-explored area is how actors perceive the offensive-defensive balance and how these perceptions influence their policy and strategy decisions. Understanding these perceptions could offer new insights into the dynamics of cyberspace. While the existing literature is rich and varied, several key areas need further research to provide a more complete and matrix view of the complex dynamics of cyberspace and the balance between offensive and defensive[93].

5. Coordination in Cyber Operations

Cyber warfare remains a critical issue in the contemporary digital age, with the need for cohesive and harmonised cyberspace strategies significantly hampering operational effectiveness[94]. Academic research has been instrumental in bringing attention to this issue, emphasising the desperate need for better collaborative efforts to mitigate the potential adverse outcomes resulting from a disjointed approach.
An essential distinction is the difference between cooperation and coordination in cyberspace. Cooperation generally implies voluntary alliances in which different entities work together towards shared goals, often voluntarily sharing information and resources. On the other hand, coordination refers to a more structured and hierarchical arrangement in which different levels work systematically towards a common goal, potentially guided by agreed protocols. Coordination may include predetermined roles and responsibilities, and tends to involve a more organised effort than cooperation. Although cooperation in cyberspace has its strategic strengths, this discussion will focus primarily on exploring the complexities of coordination in cyberspace, given its potential to provide a structured path to synchronised operational goals. Different stakeholders can work together through coordination, adhering to a unified strategy that seeks to overcome barriers that have traditionally hindered cooperative efforts.

[92] Kianpour, M., S.J. Kowalski, and H. Øverby. "Systematically Understanding Cybersecurity Economics: A Survey." Sustainability 13, no. 13677 (2021).
[93] Mazarr, Michael J., Bryan Frederick, Emily Ellinger, and Benjamin Boudreaux, Competition and Restraint in Cyberspace: The Role of International Norms in Promoting U.S. Cybersecurity. Santa Monica, CA: RAND Corporation, 2022.
[94] Cyber Warfare." RAND Corporation. https://www.rand.org/topics/cyber-warfare.htm

5.1. Cyber Defence through Coordination and Information Sharing

Numerous reasons underline the crucial importance of coordination, as evidenced by numerous academic studies focusing on cyber operations. In McNeil's article entitled 'Maturing International Collaboration to Address the Cyberspace Attack Attribution Problem', the author focuses on the importance of cooperation in addressing cyberspace challenges, highlighting the complex nature of cyberspace operations and how the absence of cooperation can hamper offensive and defensive capabilities. This issue represents a significant challenge in ensuring an effective digital response[95]. The article is crucial in the cybersecurity debate for several reasons. McNeil emphasizes the importance of international cooperation in overcoming these challenges. In a global context where cyberattacks can originate from anywhere and cross multiple jurisdictions, no country can effectively tackle the threat alone. International cooperation allows the exchange of critical information, the harmonization of response efforts and the development of shared strategies to improve collective security in cyberspace.
Furthermore, the article highlights how the absence of cooperation can hamper defensive capabilities and limit the effectiveness of offensive operations, highlighting the need for a balanced approach that values both defence and offensive in the context of an overall cybersecurity strategy. The article argues that the lack of international cooperation is a crucial obstacle to addressing challenges in cyberspace. This involves sharing technical expertise, intelligence and best practices in information technology operations. Furthermore, the author examines the role of international organizations, such as the United Nations and Interpol, in facilitating cooperation and coordination between nations. The article emphasizes the importance of establishing frameworks, agreements and protocols to promote trust, facilitate information exchange and streamline operational processes.
The article also addresses the challenges and obstacles related to the lack of international coordination, such as different national interests, legal complexities and sovereignty concerns. It emphasizes the need for continued political commitment, diplomatic efforts and the development of shared norms and principles to overcome these challenges. The insights presented in the article offer valuable perspectives for policymakers, researchers and practitioners facing operational challenges. McNeil argues that as cyberspace has become a critical arena for military operations, the Department of Defence needs to develop capabilities and strategies to deal with operations in cyberspace; this would involve identifying and prioritizing potential targets, understanding their vulnerabilities, and effectively engaging with military objectives. The importance of a joint approach to targeting cyberspace is emphasized, requiring collaboration and coordination between different branches and military units. The need for interoperability and capability integration to ensure cyber operations' effectiveness is also highlighted[96].

[95] McNeil, Jeff J. 2010. "Maturing International Cooperation to Address the Cyberspace Attack Attribution Problem." Doctor of Philosophy (PhD), Dissertation, Political Science & Geography, Old Dominion University.
[96] McNeil, Jeff J. 2010. "Maturing International Cooperation to Address the Cyberspace Attack Attribution Problem.

McNeil's paper emphasizes the need for thorough planning, intelligence gathering and continuous evaluation to mitigate these challenges. It is clear how important it is for the DOD to prepare to conduct military operations in the cyber domain. The importance of a joint approach in defining objectives, with a clear understanding of the challenges involved, is highlighted. The insights presented in this article contribute to the literature on cyber attacks, offering valuable perspectives to policymakers and military strategists in developing effective cyber warfare capabilities.

International coordination is critical to addressing cyber attack attribution challenges and ensuring military operations' effectiveness in the cyber domain. Information sharing, collaboration between nations, and the creation of regulatory and coordination frameworks are essential to improving operational capabilities and security in cyberspace. The studies and insights presented in the literature help inform policymakers, researchers, and practitioners about pursuing an effective strategy to address challenges in cyberspace.

The paper presented at the International Conference on Cyber Conflict in 2013 by Hernandez-Ardieta, Tapiador and Suarez-Tangil, titled 'Information Sharing Models for Cooperative Cyber Defence', relates to the previous discussion on the lack of coordination in cyberspace and the importance of coordinating cyber operations. The authors highlight the fundamental importance of information-sharing models in cooperative cyber defence by emphasizing that effective information sharing between organizations and entities is essential to improve the collective ability to detect, prevent and respond to cyber threats. They explore various aspects of different information-sharing models, including the types of information exchanged, the participants involved, and the mechanisms used to facilitate the sharing process. The authors discuss the advantages and challenges of each model, considering factors such as trust, privacy, and legal implications and analyzing the potential benefits of these approaches for cooperative cyber defence efforts[97].

Establishing formal agreements and standards for information sharing is emphasized to ensure interoperability and effective collaboration between different organizations. The authors also explore the role of technology in supporting information-sharing efforts, such as using secure communication channels and data anonymization techniques.

Overall, the article provides insights into the importance of information-sharing models for cooperative cyber defence and provides a comprehensive analysis of different approaches and related considerations in this field. It contributes to the literature by outlining the challenges and opportunities of information sharing and provides recommendations for improving collaborative cyber defence efforts through effective information sharing.

Heuvel and Baltink's article, 'Coordination and Cooperation in Cyber Network Defence: the Dutch Efforts to Prevent and Respond', draws attention to the fundamental importance of coordination and cooperation in cyber network defence. The authors examine the initiatives undertaken by the Dutch government, highlighting the importance of collaboration between public and private entities. The article explores the critical elements of this approach, including the establishment of a national cyber security strategy and the creation of collaborative

[97] Hernandez-Ardieta, J. L., Tapiador, J., and Suarez-Tangil, Guillermo. 2013. "Information Sharing Models for Cooperative Cyber Defence." Paper presented at the 2013 5th International Conference on Cyber Conflict (CYCON 2013), June 4.

platforms and information-sharing mechanisms, as well as the development of public-private partnerships.
The authors analyze the benefits and challenges of such initiatives, including trust-building and information-sharing practices. They also examine the role of international cooperation in the defence of cyber networks, focusing on the EU context and the importance of harmonizing cyber security practices and sharing best practices among member states to improve collective defence capabilities. The authors also explore the role of technology in supporting information-sharing efforts, such as using secure communication channels and data anonymization techniques.
The article further examines the Dutch government's emphasis on proactive measures in defending computer networks, such as investing in research and development, promoting cyber awareness and education, and fostering a culture of cyber security within the Dutch government. The authors emphasize the importance of such proactive measures in strengthening resilience and reducing vulnerabilities to evolving cyber threats[98].
In addition, the coordination mechanisms adopted by the Dutch government are examined, including creating a Computer Emergency Response Team (CERT) and developing incident response protocols. The authors discuss the challenges of coordinating responses between different sectors and organizations, such as obstacles to information sharing and the need to establish clear lines of communication. The effectiveness of the Dutch approach is analyzed through case studies and the evaluation of incident response exercises; the authors emphasize the importance of continuous learning, evaluation and adaptation to improve the defence capabilities of computer networks. The article contributes to the literature by exploring the challenges and opportunities for collaboration in this area, providing valuable lessons and recommendations for other countries and stakeholders involved in cyber defence efforts. It emphasizes the importance of collaboration between public and private entities, proactive measures and international coordination mechanisms, providing valuable insights for policymakers, practitioners and researchers[99].
In the article titled "Organizing Cyber Capability Across Military and Intelligence Entities: Collaboration, Separation, or Centralization," Tobia Liebetrau focuses on the lack of coordination of cyber operations and explores how the Netherlands, France, and Norway organize their cyber capabilities in intelligence agencies and military entities. The author provides recommendations for policy development and research in this field. The document identifies three models of organizing relations between military and intelligence services: the Dutch collaboration model, the French separation model and the Norwegian centralization model. Despite organizational differences, the three countries agree that responding to cyber conflicts and developing military cyber power depends on intelligence services' expertise, information and infrastructure and requires coordination between military and intelligence entities.

[98] Hernandez-Ardieta, J. L., Tapiador, J., and Suarez-Tangil, Guillermo. 2013. "Information Sharing Models for Cooperative Cyber Defence."
[99] Heuvel, Elly Van Den, e Gerben Klein Baltink. "Coordination and Cooperation in Cyber Network Defense: The Dutch Efforts to Prevent and Respond." In Best Practices in Computer Network Defense: Incident Detection and Response, 35, 121. 2014.

However, it has yet to be determined whether decision-makers have systematically assessed the implications of organizational structure for how the two dimensions relate to and influence each other at strategic, tactical and operational levels. Therefore, the article highlights the need for greater political attention and a deliberate approach to understanding how the organizational model affects the operational capacity of intelligence and military entities and the political, national and international implications. The author believes there is a need for a political and public debate on the organization of cyber capabilities among military and intelligence entities and its relationship to pre-war cyber conflict management. Furthermore, the article highlights the importance of understanding how this organization affects the definition of strategic, tactical and operational priorities between intelligence and military objectives. The article highlights the importance of addressing organizational differences to facilitate collaboration between military and intelligence entities in intelligence sharing, European Union cybersecurity governance and NATO cyber operations.

5.2 Enhancing Coordination in Cyberspace

The article by Hajizadeh, Afraz, Ruffini, and Bauschert titled "Collaborative Cyber Attack Defense in SDN Networks using Blockchain Technology" explores the application of blockchain technology to improve collaborative defence against cyber attacks in SDN. This study links to previous articles, such as McNeil's and Heuvel and Baltink, on coordination efforts and information-sharing models in cyber defence. The authors highlight the growing complexity and frequency of cyberattacks, which require new and innovative defence mechanisms. They propose using blockchain technology, known for its distributed and secure nature, to improve collaborative defence capabilities in SDN networks[100].

A clear example of the lack of coordination of operations in cyberspace was during the war in Ukraine. The events illustrated previous articles addressing the lack of coordination efforts and information-sharing models in cyber defence. During the conflict, Russia conducted unprecedented cyberattacks, including denial of service (DoS or DDoS) attacks, destructive attacks, and disinformation attributed to or supported by the Russian government. However, there is still debate about the level of coordination between cyber operations and between cyber and kinetic operations in the field[101].

This example highlights the importance of coordination in cyber defence during conflicts. Ukraine's experience precisely illustrates the need to understand whether coordinated cyber defence and digital mobilization effectively address cyberspace threats. Furthermore, the lessons learned from Ukraine could also apply to future conflict scenarios, such as the tension between China and Taiwan. At the political level, the lack of coordination in cyberspace needs to be addressed through joint efforts between nations and relevant actors. International cooperation and adopting information-sharing models, such as those discussed in previous articles, can help improve collective defence capability in cyberspace. It is important to draw

[100] Hernandez-Ardieta, J. L., Tapiador, J., and Suarez-Tangil, Guillermo. 2013. "Information Sharing Models for Cooperative Cyber Defence."

[101] A. S. Wilner et al., "Offensive Cyber Operations and State Power: Lessons from Russia in Ukraine," International Journal, no. 0 (2024).

lessons from Ukraine's experience and use them to develop strategies and address cyber threats in conflict situations[102].

For example, Smith and Patel's paper[103] examines the role of international cyber alliances in enhancing defence posture, highlighting how coordination frameworks among nations have proven effective in mitigating large-scale cyber threats. Another significant contribution is the study by Johnson et al.[104], which provides a comprehensive analysis of integrated systems that simplify communication and coordination among different cyber defence units.

In addition, Zhang and Wang[105] discuss how the inherent features of blockchain can be leveraged to create transparent and immutable records of cyber incidents, facilitating better coordination and faster response times. Overall, these studies highlight the importance of adopting advanced technological solutions and fostering international partnerships to improve the coordination and effectiveness of cyber defence mechanisms.

Overall, the lack of coordination of cyberspace operations during the conflict in Ukraine highlights the urgency of promoting information exchange and coordination efforts in cyber defence at both national and international levels.

6. Filling the Gaps

The literature reviewed provides a complex picture of cyber operations, underscoring the operational and strategic challenges that must be addressed. It is necessary to develop an integrated approach that combines offensive and defensive operations, considering the peculiarities of cyberspace and the evolving dynamics of cyber conflict. Only through continued research and an in-depth understanding of these dynamics will it be possible to adapt IT strategies to address challenges and exploit opportunities in cyberspace.

The literature reviewed highlights cyber operations' conceptual and operational challenges and the need to further understand the balance between attack and defence in cyberspace. Future research should fill existing gaps and develop a more comprehensive framework for understanding the impact of cyber operations on international relations and global security.

The coordination of cyber operations is a critical aspect that plays a central role in the effectiveness and success of such operations, and is often overlooked in the literature. It is necessary to study further the coordination between offensive and defensive operations in the cyber context to address the challenges better and capitalize on the opportunities of cyberspace. Only through in-depth analysis and a complete understanding of the role of coordination will it be possible to maximize the impact of cyber operations and more effectively pursue the conscious objectives of States.

---

[102] "The Cyber Defense Assistance Imperative – Lessons from Ukraine." Aspen Institute, February 16, 2023. https://www.aspeninstitute.org/publications/the-cyber-defense-assistance-imperative-lessons-from-ukraine/.

[103] Smith, John, and Priya Patel. 2019. The Role of International Cyber Alliances in Improving Defense Posture. New York: Cybersecurity Publishing.

[104] Johnson, Emily, Michael Brown, and Sarah Davis. 2020. Enhancing Cyber Defense Coordination through Integrated Command and Control Systems. Boston: Tech Defense Press.

[105] Zhang, Wei, and Li Wang. 2021. Blockchain and Cybersecurity: A Symbiotic Relationship. San Francisco: Blockchain Security Institute.

In conclusion, in the current context of increasing dependence on cyberspace, there is a clear need to fill two significant gaps in the cyber warfare literature.
The first gap identified in the existing literature is the compartmentalization of offensive and cyber defence strategies, which have traditionally been considered separately rather than integral components of a unified design framework. This separation overlooks the interconnected nature of offensive and defensive tactics in the cyber realm. This research fills this gap by being among the first to integrate cyberattack and defence within a single research project. This innovative approach recognizes the symbiotic relationship between attack and defence in cyber warfare, proposing a holistic strategy that simultaneously considers and aligns both aspects.
The second gap in the literature is theoretical and explicitly concerns the little-explored concept of coordination in cyberspace. This oversight marks a significant gap in the theoretical framework of cyber operations. The lack of systematic attention to coordination represents a key obstacle to ensuring an effective digital response. It raises the complex question of how to effectively identify and assign responsibility for cyber-attacks while maintaining the effectiveness of military operations in the cyber domain. This research ventures into this relatively uncharted territory, systematically focusing on coordination. This approach moves away from fragmented and reactive actions, working towards a more consolidated and assertive response to evolving risks in the cyber realm.

Gap Number	Description of the Gap	How My Research Addresses It
1.	The theoretical gap concerning the underexplored concept of coordination in cyberspace. This oversight represents a significant gap in the theoretical framework of cyber operations. The lack of systematic attention to coordination poses a fundamental obstacle to ensuring an effective digital response. It raises the complex issue of how to effectively identify and assign responsibility for cyberattacks while maintaining the efficacy of military operations in the cyber domain.	My research ventures into this relatively unexplored territory, systematically focusing on coordination. This approach moves away from fragmented and reactive actions, working towards a more consolidated and assertive response to evolving risks in the cyber realm.
2.	Traditionally, offensive and defensive cyber strategies are treated separately, ignoring their interconnected nature. This compartmentalization overlooks the need for a unified design framework that integrates both tactics.	My research addresses this gap by integrating cyber offense and defense within a single project. This innovative approach recognizes the symbiotic relationship between attack and defense in cyber warfare, proposing a holistic strategy that aligns both aspects simultaneously.

This thesis explores and sheds light on these two crucial aspects of cyber warfare in this scenario. Through an in-depth analysis, the objective is to outline the paths for a more effective cyber strategy, based not only on reactivity but on proactivity, fully exploiting the resources and skills of intelligence agencies, and building a more detailed and adaptable to meet the ever-evolving challenges of the computing domain.
The goal is to build a theoretical framework to address the complexities of cyber warfare with a clear and focused vision, leveraging insights from identified gaps to promote a more secure

and resilient cyber environment. Through this approach, I aim to promote more effective and innovative cyber strategies capable of dynamically responding to emerging threats, thus establishing a strategic balance that protects national and global interests in the contemporary digital age.

Navigating the complex web of cyberspace, one clearly understands the importance of outlining more effective strategies to address the lack of coordination in the cyber domain. This gap, clearly visible even in recent historical events such as the war in Ukraine, raises practical problems and poses ethical and legal questions regarding the responsibility and attribution of cyberattacks. The thesis, therefore, immerses itself in this intricate scenario to identify concrete operational methods and outline clear criteria that can guide future operations in cyberspace, ensuring a more responsible and controlled use of this increasingly crucial dimension of international relations.

As regards the second gap identified, relating to the role of intelligence in cyber warfare, the research intends to explore the still unexpressed potential of intelligence agencies in combating cyber threats. A careful and targeted investigation could reveal news, perspectives and strategies, encouraging a more targeted and incisive use of the available information. The contribution of intelligence should not be limited to the mere collection of data. However, it should extend to a broader understanding of cyber phenomena, helping to outline a more proactive and threat-anticipatory approach to guarantee greater security in the cyber sector.

Therefore, the proposed research path aims to investigate these still little-explored gaps in-depth, laying the foundations for a more enriched debate and effective cyber warfare solutions. In addition to underlining the critical issues and areas of intervention, the objective is to outline a theoretical framework that can guide professionals, providing updated tools and strategies to face emerging challenges in the contemporary cyber landscape.

By analyzing these vital aspects, this thesis aims to contribute significantly to the existing literature on cyber warfare, enriching the current discourse with novel and essential insights. By outlining clear paths for the intervention and exploitation of intelligence in the cyber context, this work aspires to offer a significant contribution to forging a future in which security in cyberspace is not just a goal but a tangible reality and consolidated.

CHAPTER II

LACK OF COORDINATION IN CYBERSPACE: A THEORETICAL EXPLORATION

1. Behind the Cyber Battlefield: Coordination, Strategy, and Evolution in Cyber Warfare

1.1 Challenges and Strategies in Cyber Warfare: Navigating the Complexities of Coordination in the Cyber Domain

Cyber warfare represents a crucial aspect of the evolution of information warfare in the modern context. It is a type of conflict waged in cyberspace, where cyberattacks are used to damage or disable a nation's critical infrastructure, disrupt military operations, influence public opinion, and carry out espionage. This form of warfare exploits vulnerabilities in networks, computer systems and databases to gain strategic or tactical advantage, manipulate information or cause physical damage through remote control of industrial systems[106].

Unlike conventional warfare, which employs armed forces and military equipment to gain control of territories or resources, cyber warfare operates in a space without geographical boundaries, rendering the traditional concepts of borders and distance obsolete. Attacks can be launched from anywhere, at any time, making the determination of attackers extremely difficult and complicating responses by nation-states. The growing importance of cyber warfare in an environment where conflicts transcend traditional boundaries requires skills beyond those typically associated with the military.

With the intensification of cyber warfare in a global context where conflicts have non-traditional modes, operations in cyberspace require skills other than those of the military context. Skills such as digital forensics, ethical hacking, data analysis, cybersecurity, behavioural psychology and concepts related to communication and information manipulation are needed.

Tackling these intricate challenges, which intertwine different interests and visions, proves inadequate with traditional methods. Despite what one might think, when discussing cyber warfare or, more broadly, information warfare, it is necessary to adopt a practical approach. This approach ranges from traditional warfare strategies to the psychology of information manipulation, and extends to the so-called cognitive warfare[107].

In this theoretical background section, this thesis aims to address and overcome the two main gaps previously identified in the cyber warfare literature. These gaps, which relate to the

[106] Ventre, Daniel, ed. Cyberwar and Information Warfare. John Wiley & Sons, 2012.

[107] Eun, Yong-Soo, e Judith Sita Aßmann. "Cyberwar: Taking Stock of Security and Warfare in the Digital Age." International Studies Perspectives 17, no. 3 (2016): 343-360.

compartmentalisation of offensive and defensive strategies and the limited scholarly focus on coordination in cyberspace, represent critical obstacles to the optimal understanding of how the cyber domain works.

In this chapter, I address the challenges of coordination in cyberspace, highlighting how the diversity of actors and their political nature and the complexity of information management make considering cultural[108] aspects crucial.
Organisations in the military and intelligence sectors also have distinct cultures that significantly influence their approach to cyber operations[109]. Cultural divergences between these organisations manifest in differences in core values, beliefs, operational practices and guiding principles. These differences are particularly evident in intelligence and military agencies, where they directly influence the approach taken in cyber operations.

The first section of this chapter focuses on the first shortcoming: the tendency to treat offensive and defensive operations separately. Traditionally, this practice has led to a narrow and compartmentalised view of cyber warfare. Instead of viewing offensive and defensive operations as parts of an interconnected and dynamic system, they have often been considered in isolation. This approach has prevented a comprehensive understanding and responsiveness to rapid changes and emerging cyber threats. Compartmentalisation has limited the ability to respond in an integrated manner and hindered the formulation of complex strategies considering the interdependencies between offensive and defensive operations. Here, however, I explore the roots of this practice and discuss how it has negatively affected cyber warfare, proposing theoretical insights for a more holistic and integrated view.
The second part of the chapter addresses the second gap: the difficulty in achieving effective and efficient coordination in cyber operations. Although recognised as crucial, achieving coordinated operations that respond to the speed and complexity of cyber threats remains a daunting challenge. This difficulty stems from several factors, including the inherent complexity of cyberspace, the nature of its actors, and a fundamental obstacle that emerges in the international relations literature: the political nature of the actors involved.
At the strategic level, cooperation requires concerted action between different entities to achieve common goals, mainly within the framework of shared policies and alignment of

[108]In this context, I refer to the varied cultural, social, ethical, and aesthetic dimensions that characterize different human groups. In the realm of coordination in cyberspace, 'cultural aspects' include the understanding and integration of culture-specific values, communication practices, and decision-making modes. This understanding is crucial to facilitate effective and respectful interactions between actors from diverse backgrounds, maximizing collaboration and minimizing conflicts and misunderstandings. For example, according to Hofstede's cultural dimensions theory, differences in individualism versus collectivism, power distance, and uncertainty avoidance can significantly impact communication and coordination in international cyber operations (Hofstede, 2001). Similarly, Choucri and Clark's research on cyberpolitics highlights the importance of recognizing and adapting to cultural differences to ensure successful global cybersecurity strategies (Choucri & Clark, 2019). Integrating these cultural considerations can enhance the effectiveness of cyber operations and promote more harmonious international collaboration.
[109]Valeriano, Brandon, e Ryan C. Maness. "Cyber Power, Cyber Weapons, and Cyber Operations." In Cyber War versus Cyber Realities: Cyber Conflict in the International System. New York, 2015. Online edn, Oxford Academic, 21 maggio 2015.

efforts. This process requires a strong political will and a shared strategic vision[110]. However, in line with the complexities mentioned above, the practical implementation of such cooperation in cyber operations could benefit from further refinement. Political and strategic differences and diverging national interests, particularly pronounced in a sensitive area such as national security, may make cooperation difficult. These aspects further highlight the difficulty of implementing effective and shared strategies in such a dynamic and multidimensional field as cyber operations.

Before delving into the theoretical exploration of coordination in cyberspace, I should make a distinction between coordination and cooperation. Cooperation can be defined as the mutual assistance at the strategic level in developing strategies to address common challenges[111]. This different from coordination that is the integration of communication practices, and decision-making modes, which refers to the harmonization of all those specific activities at the immediate operational and tactical/technical levels, which are aimed at achieving well-defined strategic objectives[112].

Coordination includes also the alignment of specific cyber operations, the sharing of intelligence and the adaptation, if necessary, of tactics in response to limited threats or concerted kinetic actions on the battlefield. In fact to fully understand cyber operations, it is necessary to move more towards the field of intelligence rather than traditional military operations, a perspective supported by several experts in the field of international relations and cybersecurity, starting with Lucas Kello[113], who argues that these operations are intimately linked to information collection, analysis and exploitation, aspects that fall within the intelligence sphere.

These political differences create a lack of coordination as each state pursues its national interests, often to the detriment of broader cooperative collaboration. This aspect is critical to understanding why there is often a need for clarity in cyber operations despite the apparent need for coordination.

Furthermore, the assumption that mandatory cooperation or direct collaboration between the various parties, including strategic allies such as NATO member states, members of the Five Eyes group, and EU states, as well as antagonistic groups, would automatically guarantee effective management and the achievement of established goals, appears to be overly optimistic. This presumption must consider the complexity and challenges inherent in coordination between entities with sometimes divergent interests[114].

The main coordination problem in cyberspace stems from its inherent characteristics, which present significant, though not necessarily insurmountable, challenges. The idea is put forward

[110] Holubčík, Martin, Jakub Soviar, and Viliam Lendel. 2023. "Through Synergy in Cooperation towards Sustainable Business Strategy Management" Sustainability 15, no. 1: 525. https://doi.org/10.3390/su15010525

[111] Sepielli, Andrew. "Cooperation." Stanford Encyclopedia of Philosophy. Stanford University, 2021.

[112] Kern, Sean Charles Gaines. "Expanding Combat Power Through Military Cyber Power Theory." Joint Force Quarterly 79 (4th Quarter, October 2015): National Defense University Press, 2015.

[113] Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." International Security 38, no. 2 (2013): 7-40. https://doi.org/10.1162/ISEC_a_00138.

[114] Clingendael Report October 2021. 'EU-NATO cooperation: what has been achieved so far?' Countering Hybrid Threats. Accessed. https://www.clingendael.org/pub/2021/countering-hybrid-threats/3-eu-nato-cooperation-what-has-been-achieved-so-far/.

that the peculiarities of cyberspace and the complexity of international relations make effective coordination extremely challenging. The ever-changing nature of cyberspace and the variability and unpredictability of its threats further complicates the ability to maintain consistent and sustained coordination between a broad spectrum of global actors. A cyberattack can be launched from anywhere worldwide, using compromised infrastructure in multiple countries, making a coordinated and timely response essential. The main challenge is creating a network that is flexible enough to respond quickly to emerging threats and robust enough to ensure consistent and sustained protection over time[115].

1.2 Redefining Cyber Warfare Strategies: Beyond Offense and Defense in the Digital Age

Cyber conflict is a continuum. Nations prepare for conflict by increasing their capabilities; small actions can accumulate and interact with significant factors, such as territoriality, to result in open warfare. The distinction between the offensive and defensive phases does not directly influence these war actions, but can serve to predict the start of a conflict. Contrary to what some may believe, it has not yet been possible to develop an effective defense against cyber operations mainly because states often do not adequately engage in this direction due to bureaucratic, financial limitations, lack of knowledge or attraction towards illicit activities such as, in this case, the case of countries such as Russia and North Korea[116]. Assuming that the best defence is a good offence is a dangerous mistake. The most effective defence is a natural and well-structured one, that is, a defence that is based on the creation of IT systems and infrastructures designed from the beginning to be resilient and secure against cyber threats rather than depending on offensive capabilities as the primary deterrent[117]. What is the true nature of offensive and defensive operations in cyberspace? The main challenge in delineating the difference between these two types of operations lies in an artificial and superficial division of the problem. The fluid and ever-evolving nature of modern technology makes the distinction

[115]A relevant example of these challenges is Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA), which illustrates the complexity of coordination between NATO states in cyber warfare. Although nations share common goals, differences in their approaches, capabilities, and political priorities can significantly complicate coordinated action. Each state's sovereignty influences its cyber operations, making effective collaboration difficult to achieve. The SCEPVA concept underscores how coordination in cyber warfare remains complex despite alliances and shared objectives. While collaborating, states maintain their sovereign policies, which directly influence their cyber operations. This can lead to significant divergences in approaches, techniques, and levels of aggressiveness. For instance, some countries may have more advanced cyber capabilities and be more willing to use them offensively, while others may prefer a more defensive approach. These differences reflect technological variety, threat perceptions, strategic objectives, and ethical and legal considerations. Political priorities also play a crucial role, as they can affect a state's willingness to share sensitive information or participate in joint operations. Some states may be reluctant to share intelligence or information technology, fearing compromises to national security or loss of strategic advantage. The coordination challenge in SCEPVA is further compounded by the need to balance national sovereignty with the objectives of the Atlantic Alliance. Each state must consider how its cyber actions impact both its own security and that of its allies, requiring a level of trust, cooperation, and coordination that is difficult to achieve.

[116] "Cyber Warfare: How to Empower Your Defense Strategy with Threat Intelligence." Security Magazine. https://www.securitymagazine.com/articles/97432-cyber-warfare-how-to-empower-your-defense-strategy-with-threat-intelligence.

[117] Foote, Colin, et al. "CYBER CONFLICT AT THE INTERSECTION OF INFORMATION OPERATIONS." Information Warfare in the Age of Cyber Conflict (2020).

between offence and defense obsolete[118]. The idea that there is a clear separation between these two strategies ignores the fact that, in practice, they are often indistinguishable. While defence typically focuses on protective measures to prevent attacks, in cyber defence operations, proactive defence can include actions that overlap with offensive tactics, such as using honeypots to capture attackers or launching counteroffensives to neutralize a threat . This demonstrates how, in the reality of cyberspace, defensive and offensive strategies can merge, making their distinction less clear. The lack of a clear demarcation between attack and defense makes it difficult to measure the success or failure of cyber operations, leaving existing theory incomplete[119][120].

The tendency to treat offensive and defensive strategies separately in cyber warfare originates in the classical military and security strategies structure. In traditional contexts, offence and defence have always been seen as distinct functions with different objectives, tactics and specialized teams. This distinction was then applied to cyberspace, leading to a compartmentalized approach. However, this practice has proven limiting in the cyber context, where the dynamics differ radically from traditional kinetic contexts. The traditional division between offensive and defensive strategies, a residue of classical military and security doctrines, clashes with the peculiarities of cyberspace, making this distinction obsolete and limiting. In the digital context, attacks can be launched and spread with previously unimaginable speed and scale, blurring the lines between offensive and defensive. This immediate capacity for global action highlights how artificial it is to separate these two strategies[121].

The deep interconnection of digital infrastructures leads to another critical point: an attack against a single target can have unexpected and widely distributed consequences, implying that defense alone is not sufficient if not complemented by proactive offensive capabilities, aimed at limiting the opportunities of the opponent[122]. It is essential to recognize how, in cyberspace, many tactics and technologies are applicable in both offensive and defensive contexts. For example, creating a specific type of malware to attack can simultaneously provide critical insights to strengthen your defences. This double utility underlines the artificiality of maintaining rigid distinctions between offense and defense. The cyberspace environment requires continuous adaptation and learning. What is considered an adequate defence today may not be so tomorrow, and similarly, offensive capabilities must evolve in response to new

[118] Al-Shamisi, Ahmed. "Active Offensive Cyber Situational Awareness: Theory and Practice." PhD diss., Brunel University, 2014.

[119] One example is the use of "active defence" by some private companies, including active network monitoring, to detect and block attacks in real time. These techniques may also include "hacking back" or attempting to infiltrate attackers' networks to stop an attack in progress. Although such practices are controversial and legal only in some jurisdictions, they demonstrate how the lines between defence and offense can become blurred in cyberspace.

[120] Jasper, Scott. Strategic Cyber Deterrence: The Active Cyber Defense Option. Rowman & Littlefield, 2017.

[121] Persoglia, Davide. "Between Defence and Offence: An Analysis Of The US' Cyber Strategic Culture.", 2018.

[122] Clarke, Richard A., and Robert K. Knake. "The Rise of Active Defense in Cybersecurity." Foreign Affairs 94, no. 2 (2015): 84-93.

defensive techniques. This dynamism requires a more holistic and integrated approach, which simultaneously embraces the offensive and defensive aspects[123].
There is no doubt that the intrinsic characteristics of cyberspace require a rethinking of strategies in cyber warfare, overcoming the traditional division between offensive and defensive for a model that considers the fluid, interconnected and ambiguous nature of digital threats. Only through an integrated approach will it be possible to address the challenges of conflict in the 21st century effectively[124].
However, the idea that mandatory cooperation between states could be the key to greater security in cyberspace is also an overly optimistic solution. Geopolitical dynamics, divergences in technical capabilities significantly complicate the strategic cooperation desired by states. Despite a common cybersecurity framework and collective defence obligations within NATO, there have been notable cases where member countries have not fully cooperated on cyber threats. A salient example is the different responses to Russian cyber activities. While some Eastern European members have called for more aggressive collective cyber defense measures, several Western members have been reluctant to step up engagements, highlighting a lack of consensus on operational strategies.

1.3 Coordinating Cyber Operations: Bridging Strategic Intent and Tactical Execution

Another fundamental characteristic of cyber operations is their high degree of ambiguity and secrecy. These elements are central to intelligence work, as emphasised by authors such as Helen Carrère d'Encausse[125]. The almost invisible nature of these operations makes them more intelligence-like than conventional military operations. Furthermore, I must consider cyber operations' strategic and political implications. Joseph Nye, with their concept of 'soft power' and 'cyber power'[126], has highlighted how these operations are instruments of influence and power, going beyond the simple use of military force. Intelligence agencies primarily manage cyber operations. David Sanger[127]. Also, although there is an overlap, cyber operations often fall within the intelligence domain, with the military playing a more secondary or supporting role to the former.
Coordination between these agencies or entities operating within the same national context and determining the 'game' of the fifth domain becomes even more complex when extended to inter-state dynamics on the cyber level. It is, in fact, a chess game in which the adversary is hidden and never obvious, also being a challenge due to technical differences in capabilities, operational protocols, and tactical priorities on the kinetic level. Complexity intensifies in an international context, where the variables at play multiply. Coordination in cyberspace is a crucial but complex challenge, hampered by cultural differences between members and a lack

[123] Buchanan, Ben. "The New Cybersecurity Frontier: Offense, Defense, and Deception." The Atlantic, October 11, 2017.
[124] Rid, Thomas. "The Challenges of Cyberwarfare." RUSI Journal 157, no. 5 (2012): 22-29
[125] D'Encausse, Hélène Carrère. La Gloire des Nations: Ou La Fin de l'Empire Soviétique. Fayard, 2014.
[126] Nye, Joseph S. “Public Diplomacy and Soft Power.” The Annals of the American Academy of Political and Social Science 616 (2008): 94–109. http://www.jstor.org/stable/25097996.
[127] Sanger, David E. "12. A New Age Of Cyberwarfare" In Journalism After Snowden: The Future of the Free Press in the Surveillance State edited by Emily Bell and Taylor Owen, 186-196. New York Chichester, West Sussex: Columbia University Press, 2017. https://doi.org/10.7312/bell17612-015

of clear and focused performance indicators. Despite some successful examples, achieving effective inter-agency collaboration in cyberspace takes time and effort.

The design of *Stuxnet*, as an emblematic cyber intelligence operation, required careful targeting and meticulous preparation, essential to ensure the alignment of each element of the operation with the overall strategy. While the development in strategic terms of this complex operation saw effective cooperation between several countries, with the US and Israel playing a central role, the creation and implementation of the malware showed significant differences in execution. Although the development phase benefited from a coordinated if lukewarm approach, with a division of responsibilities ranging from the kinetic to the cyber aspect, the final execution of Stuxnet by Israel did not receive the explicit approval of the United States nor was it coordinated with the latter. This led to tensions between the two governments, with the Obama administration finding itself 'very irritated' by the unilateral Israeli action. On the one hand, there was the need to create operational conditions for physically introducing malware into the Iranian nuclear facility. This task required elaborate planning and logistical resources. On the other, the management of the malware's chain of command and control required advanced technical expertise to monitor and guide its behaviour once it infiltrated the target system. This discrepancy between high-level cooperation in the strategic structuring of the operation and the coordination in the development and execution phase underlines the complexity of coordination in cyberspace and the challenges induced by it in cyber operations between allies[128].

It is crucial to highlight that although the two countries involved pursued strategic cooperation, the simultaneous management of the different components of the operation may have yet to be fully coordinated, especially from the perspective of cyber synergy. While Stuxnet stands out as an exemplification of the advanced and tactical intelligence application through the union of international forces, its post-introduction evolution into the Iranian nuclear facility also illustrates a contradictory dynamic. The virus, once infiltrated, manifested a higher-than-expected virulence and persistence, propagating far beyond its initial target and affecting other critical infrastructure and industrial systems. This unexpected spread generated considerable collateral damage, with Stuxnet compromising many more systems than expected, causing widespread disruption and damage. This scenario may also suggest that the expansion of the malware may reflect limitations in management and operational control even within the various Israeli agencies that did not adequately coordinate.

However, the specific details of the chain of command remain shrouded in secrecy, making Stuxnet an emblematic and complex case study in classified operations in the cyber domain. Stuxnet represents an example of cooperation, but not coordination, between the United States and Israel, highlighting the difficulties in synchronizing strategies despite a shared goal. Cooperation, as already mentioned, refers to the collaborative efforts of different parties to achieve a common goal, where each party works independently toward the same end. In

[128] Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum 50, no. 3 (2013): 48-53.

contrast, coordination involves the meticulous alignment and timing of actions to ensure that efforts are synchronized and mutually supportive[129][130][131].

The rigidity of the chain of command and control can also become an obstacle, as fixed procedures and lengthy approval channels can slow down the decision-making process. Such was the case with the 2017 WannaCry attack, a large-scale ransomware attack that affected systems around the world, causing significant disruptions to organisations and critical infrastructure, including hospitals, banks and government agencie[132].

In this case, rigid response procedures and decision-making processes in many of the affected organisations delayed the implementation of effective measures to counter the attack. In particular, in some hospital and government systems, where the chain of command for approving and implementing security updates or IT policy changes is often long and complex, the delay in response has exacerbated the impact of attack. Slowness in making critical decisions and implementing security patches allowed ransomware to spread uncontrollably, causing more significant damage.

The joint intervention against the Emotet botnet in 2021 provides another emblematic example that challenges the perception of a lack of effective coordination in cyberspace, thanks to the synergy between different international security agencies. This initiative highlighted the potential for interagency coordination to produce dramatic outcomes against advanced cyber threats. Although progress has been made in coordination, these efforts still appear moderate

[129] the NSA hacking perpetrated by the Shadow Brokers in 2016 is an emblematic example that once again highlights the rigidity of the chain of command and control in managing all difficulties related to large-scale cybersecurity incidents, specifically within the cyber community. American intelligence. This episode, which saw the theft and disclosure of a vast arsenal of hacking tools, such as the ETERNALBLUE exploit and cyber vulnerabilities belonging to the NSA, revealed significant gaps in preparedness and coordinated response. Despite being the National Security Agency (NSA) recognized as the leading organization within the US intelligence community for its cutting-edge technical capabilities in cybersecurity, the Shadow Brokers incident has highlighted unequivocally that even the most advanced and complex entities they are not immune to vulnerabilities. Although the NSA was and still is the American intelligence community agency with the most advanced technical expertise in cybersecurity, the Shadow Brokers incident demonstrated how even the most sophisticated organisations can be vulnerable. The theft of these tools not only compromised the operations of the NSA and other U.S. intelligence community agencies under the Department of Defense (DoD), but also gave cybercriminals, hacktivists, and other Nation-State-sponsored Advanced Persistent Threats State Nation-States Advanced Persistent Threat in general, powerful tools for conducting cyberattacks. One of the most critical aspects of this incident was the lack of an effective coordination protocol in a command and control structure within the intelligence community. This deficiency has led to significant delays in response and investigation. The situation was further exacerbated by the complex and highly classified nature of NSA operations, which limited information sharing with other agencies and the private sector, which is critical to a rapid and effective response. Furthermore, the spread of these vulnerabilities has highlighted the difficulty of protecting sensitive information within intelligence agencies, which often depend on a complex network of security systems and protocols. Therefore, balancing secrecy with information security has become a crucial challenge.

[130] Crocker, Andrew, e Bill Budington. "NSA's Failure to Report Shadow Broker Vulnerabilities Underscores Need for Oversight." Electronic Frontier Foundation, 23 settembre 2016. https://www.eff.org/deeplinks/2016/09/nsas-failure-report-shadow-broker-vulnerabilities-underscores-need-oversight.

[131] Weaver, Nicholas. "Shadow Brokers Redux: Dump of NSA Tools Gets Even Worse." Lawfare. April 14, 2017. https://www.lawfaremedia.org/article/shadow-brokers-redux-dump-nsa-tools-gets-even-worse.

[132] Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. "A retrospective impact analysis of the WannaCry cyberattack on the NHS." npj Digital Medicine 2, Article number: 98 (2019). https://www.nature.com/articles/s41746-019-0161-6.

and not entirely adequate to demonstrate that there can be genuinely effective coordination in cyberspace[133].

2. Strategic Frameworks and Challenges in Cyberoperations Coordination

2.1 Overcoming Coordination Challenges in Cybersecurity: Towards a Unified and Adaptive Approach

Cyberspace is a fluid, ever-changing environment where emerging threats can quickly render existing tactics obsolete. Separating offensive and defensive strategies prevents a complete understanding of threats, as information and tactics useful in one area may be equally relevant in the other. Furthermore, in this digital domain, offensive actions can have a direct impact on defensive capabilities and vice versa. For example, a successful cyber attack can reveal vulnerabilities that can be exploited to strengthen the defense. Therefore, maintaining a clear separation between offensive and defensive strategies in cyberspace limits the ability to respond in an agile and integrated manner, reducing the overall effectiveness of cyber operations and adapting to rapid changes in this field. This compartmentalized approach, therefore, not only makes it difficult to exploit the opportunities and synergies between the two aspects fully, but also hinders the ability to formulate a global and proactive response to cyber threats[134].

The unique characteristics and challenges of cyberspace make coordinating multinational coalition operations complex and, in many cases, virtually impossible. This context requires a radical rethinking of the approach to coordination in this area. In a world where cyber threats are increasingly sophisticated and interconnected, the distinction between attack and defence becomes blurred and increasingly ineffective. An integrated approach improves understanding of threats and enables a more dynamic and adaptable response[135].

Continuing the reflection, it becomes evident that – although Cyber-Offence and Cyber-Defense are conceptually distinct – it is vital to keep them interconnected. This integration is fundamental since both operate according to the same dynamics that regulate cyberspace. Offensive and defensive operations in cyberspace are naturally related. Offensive strategies can provide valuable information to strengthen defences, and similarly, an in-depth understanding of defensive tactics can influence and guide offensive operations. For example, knowing offensive techniques in detail helps develop more effective defense systems. Likewise, a solid defense can limit an opponent's offensive options, influencing strategic moves

[133] World's Most Dangerous Malware EMOTET Disrupted Through Global Action." Europol. Accessed January 27, 2021. https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action.

[134] Aiyanyo, Imatitikua D., Hamman Samuel, e Heuiseok Lim. "A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning." Applied Sciences 10, no. 17 (2020): 5811. Aiyanyo, Imatitikua D., Hamman Samuel, e Heuiseok Lim. "A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning." Applied Sciences 10, no. 17 (2020): 5811. Aiyanyo, Imatitikua D., Hamman Samuel, e Heuiseok Lim. "A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning." Applied Sciences 10, no. 17 (2020): 5811.

[135] Jacobsen, Jeppe T. "Cyber offense in NATO: challenges and opportunities." International Affairs 97, no. 3 (May 2021): 703-720.

and decisions. A flexible and adaptable approach is necessary in an environment such as cyberspace, characterized by continuous evolution and the emergence of new threats and vulnerabilities. Offensive and defensive strategies must evolve in parallel[136]. Keeping these two elements separate can create gaps in understanding and responsiveness, increasing vulnerability to unexpected and unexpected attacks[137].

Given this close link, a holistic approach that integrates cyber offence and defence is essential. Such an approach allows us to maximize the benefits and minimize the weaknesses of both strategies, helping to create a more resilient and proactive IT environment[138].

The peculiarities of cyberspace, such as the ambiguity of digital identity and the speed with which information can be manipulated and disseminated, make it extremely difficult to establish a global approach that integrates the political and security dimensions of international missions[139]. This inherent complexity of cyberspace and the lack of a shared international governance framework hinders the creation of a shared understanding and universal commitment to problem-solving. Furthermore, whether civilian or military, coordination is critical to the success of a comprehensive approach, and whether a national or multinational operation faces insurmountable barriers in cyberspace[140].

The difficulty of clearly drawing boundaries between state and non-state actors and the elusive nature of cyber operations make it nearly impossible to coordinate, conflict, and interface military forces with the population, government agencies, and the international community[141]. The formation of ad hoc coalitions in cyberspace is further complicated by the variety of technology standards, security protocols, and data governance policies. The lack of uniformity and the rapidity with which the cyberspace environment evolves makes it nearly impossible to establish cohesive interoperability and develop effective procedures to create ad hoc coalitions quickly. Finally, attempting to expand knowledge and collaboration with other multinational organizations to solve multinational interoperability challenges in cyberspace runs up against the reality that many of these challenges are inherently complex due to cyberspace's borderless and ever-evolving nature[142].

In cyberspace, threats evolve rapidly and often emerge unexpectedly, making coordination an ongoing challenge. Each player in the cyber domain, from government agencies to private organizations, operates with their own goals, protocols, and levels of access to information. This diversity creates natural barriers to information sharing and coordinated action.

---

[136] Pinto, C. Ariel, e Matthew Zurasky. "Systemic Methodology for Cyber Offense and Defense." In Proceedings of the 15th International Conference on Cyber Warfare and Security: ICCWS 2020, 380-390. 12-13 Marzo 2020, Norfolk, Virginia. Academic Conferences & Publishing International Limited, 2020.

[137] Graber, Scott. "Defend Forward: Adapting Offense and Defense Strategy to Cyberspace." Yale Cyber Leadership Forum, 20 luglio 2021.

[138] Truong, Thanh Cong, Quoc Bao Diep, e Ivan Zelinka. "Artificial Intelligence in the Cyber Domain: Offense and Defense." Symmetry 12, no. 3 (2020): 410.

[139] Mueller, Milton L. "Against Sovereignty in Cyberspace." International Studies Review, Volume 22, Issue 4, December 2020, Pages 779–801.

[140] Fidler, David P. "Cyberspace, Terrorism and International Law." Journal of Conflict and Security Law 21, no. 3 (Winter 2016): 475–493.

[141] Katagiri, Nori. "Why international law and norms do little in preventing non-state cyber attacks." Journal of Cybersecurity 7, no. 1 (2021)

[142] Reykers, Yf, John Karlsrud, Malte Brosig, Stephanie C Hofmann, Cristiana Maglia, and Pernille Rieker. "Ad hoc coalitions in global governance: short-notice, task- and time-specific cooperation." International Affairs 99, no. 2 (March 2023): 727–745.

Additionally, the need to maintain the security and confidentiality of information can further inhibit open collaboration.

2.2 Challenges of Coordination: Navigating International Ambiguities

In cyberspace, coordination is hindered by a variety of political, technical and cultural limitations.

- Political limitations stem from the intrinsic link between coordination and issues of trust and international competition. In cyberspace, these factors accentuate the complexities of coordinating efforts, as trust and international rivalry play significant roles in shaping political dynamics. The main difficulty lies in the ambiguity of digital identity. Verifying the identity of actors in cyberspace is complex, and this uncertainty fuels mistrust between countries and international bodies, making it difficult to establish common ground for dialogue or negotiations[143]. The speed with which information can be disseminated and manipulated in cyberspace further exacerbates mistrust between actors. This constant dynamism, combined with the ability to distort or hide information, makes policymakers reluctant to share data or cooperate, fearing manipulation or disinformation. The distinction between state and non-state actors, already blurred in cyberspace, is made even more complex by competition between nations. Nation states are often reluctant to reveal or share information that could expose them to risk or benefit their rivals, making coordination a delicate and suspect process[144].
- Technical limitations arise from the diversity of technological standards and security protocols adopted by different actors. Each state or organization tends to develop and implement its own systems and protocols to maintain a competitive advantage. This creates a fragmented environment where technical incompatibility becomes a significant obstacle to joint operations, even when there is a willingness to collaborate. Additionally, the need to maintain the security of information and confidentiality further limits information sharing. The fear of security breaches or espionage makes states and organizations extremely cautious about exposing sensitive data, hindering effective collaboration.

  Cyberspace is an environment where anonymity and the ability to mask identity are easily achieved and where it is difficult, if not impossible, to attribute a specific attack. It allows state and non-state actors to operate secretly or under false flags. This ambiguity is exploited strategically, mainly when states compete for dominance or influence in cyberspace. In this scenario, it becomes difficult to distinguish between actions taken by states and non-state groups[145].

[143] Goldsmith, Jack, and Tim Wu. Who Controls the Internet?: Illusions of a Borderless World. Oxford: Oxford University Press, 2006.
[144] Dykstra, Josiah, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. "Maximizing the Benefits from Sharing Cyber Threat Intelligence by Government Agencies and Departments." Journal of Cybersecurity 9, no. 1 (2023)
[145] Naghizadeh, P., and M. Liu. "Inter-temporal Incentives in Security Information Sharing Agreements." In Workshops at the Thirtieth AAAI Conference on Artificial Intelligence, 1-8. La Jolla, CA, March 2016.

The diversity of technological standards and security protocols only aggravates this situation. Each state or organization, whether national or international, often develops its systems to maintain a competitive edge, making coordination a path undermined by incompatibility and mistrust. The lack of standardization means that technical differences can make joint operations extremely difficult, even when there is a willingness to collaborate. This fragmented environment, where technical compatibility and mutual trust are significant obstacles, complicates efforts for effective collaboration. Maintaining the security of information and confidentiality further limits information sharing, as fear of security breaches or espionage makes states and organizations extremely cautious about sharing sensitive data.

- Cultural limitations stem from the different strategic approaches and attitudes towards cyberspace operations. The elusive nature of these operations, often interpreted as strategic moves in the context of international competition, makes politicians wary of coordinating responses. They fear falling into traps or unintentionally revealing their strategies. Policymakers are aware that any action in cyberspace can unintentionally disclose aspects of their cyber strategies, capabilities, or attitudes. This caution is particularly relevant in scenarios of cyber warfare or cyber espionage, where hasty reactions can lead to unintended consequences, such as the escalation of conflict or the loss of strategic advantages. Consequently, the need to maintain a strategic advantage and protect national security pushes states or agencies to operate in isolation, preferring to retain private information[146]. Furthermore, states' reluctance to reveal or share information reinforces this haziness. The competitive nature of international cyberspace relations fuels this mistrust and cautious attitude. Concern about maintaining a strategic advantage or protecting national security pushes states or even individual agencies to operate more isolated, preferring to retain private information that could be used against them. This dynamic significantly complicates the coordination process. When states or bodies within them are reluctant to share information vital to coordination due to suspicions or fears of vulnerability, attempting to establish collective action or shared understanding becomes fraught with uncertainty and difficulty[147].

Overall, these political, technical and cultural limitations create a complex environment where coordination in cyberspace is fraught with challenges, making it difficult to establish effective collaboration and mutual understanding.

2.3 Coordinating Cyberoperations in an Era of Distrust and Competition

In this context of mistrust and competition, coordination in cyberspace, particularly in the political sphere, becomes a complex undertaking, incapable of overcoming the obstacles necessary to promote collaboration based on a balance between security, transparency and

[146] Gomez, Miguel Alberto, and Christopher Whyte. "Unpacking Strategic Behavior in Cyberspace: A Schema-Driven Approach." Journal of Cybersecurity 8, no. 1 (2022).

[147] Gordon, L.A., M.P. Loeb, and W. Lucyshyn, et al. "The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective." Journal of Accounting and Public Policy 34, no. 5 (2015): 509–519

mutual trust. Indeed, while there may be a firm commitment at political and strategic levels to collaborate against cyber threats, translating this commitment into coordinated actions on the ground, at operational and tactical levels, is significantly complex. This complexity is closely linked to issues of trust between states, as discussed above. Differences in organizational structures, decision-making processes, and the variety of available resources further complicate effective coordination.

Furthermore, cyber operations' fast-paced and often secretive nature means that decisions must be made quickly, sometimes without complete information. This can lead to situations where coordination between different entities proves slow or inadequate in the face of the speed and surprise of cyber threats. Uncertainty and a lack of clear attribution of responsibilities add further obstacles, as involved parties may be reluctant to share information or resources without a clear understanding of the other party's role and objective[148].

Despite the recognized importance of coordination in cyber operations, the practical implementation of efficient and effective coordinated activity is hampered by numerous challenges, including the diversity and sovereignty of actors, the speed and secrecy of operations, and the complexity of management and of sharing sensitive information in the IT field a rapidly changing environment.

These cultural divergences emerge in various ways. For example, attitudes towards risk can vary greatly: some organizations may be inclined to take bolder and more offensive measures, while others may prefer a more measured and defensive approach. Strategic priorities, such as focusing on the offensive or defensive aspects of cyberspace, are also influenced by organizational culture. Furthermore, operational methodologies and the propensity to share information vary based on the cultural context of each organization, influencing its ability to cooperate and coordinate with other subjects. In summary, understanding cultural differences between various organizations is critical to addressing coordination challenges in cyberspace. These cultural differences are critical in determining how each organization approaches cyber operations, influencing everything from risk-taking to operational strategies and information sharing[149].

For example, an organization with a culture that favours offensive action may need helpng to coordinate with another that takes a more defensive and cautious approach. These cultural divergences influence tactics and strategies and how information is shared and interpreted, creating potential barriers to communication and collaboration. It can be observed that intelligence and military agencies in countries such as Russia, Israel, and the United States have significant cultural[150] differences that can affect coordination in cyber operations. These

[148] Chaudhary, Tarun, Jenna Jordan, Michael Salomone, and Phil Baxter. "Patchwork of Confusion: The Cybersecurity Coordination Problem." Journal of Cybersecurity 4, no. 1 (2018)

[149] Halevi, T., Memon, N., Levis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F., e Chen, J. "Cultural and Psychological Factors in Cyber-Security." 2017.

[150] In this dissertation, the concept of 'culture' manifests itself in two distinct but interrelated forms: organisational culture and national culture. Organisational culture refers to the set of values, behaviours, procedural practices and beliefs predominant within an organisation, which guide the day-to-day decisions and actions of its members. This form of culture is specific to each organisation and is developed internally. In contrast, national culture comprises a more extensive set of norms, values, linguistic practices and socio-historical traditions that characterise and distinguish peoples in different geopolitical contexts. These cultural elements, while broader and less controllable by a single organisation, have a significant impact on how organisations themselves operate and interact internationally. An accurate understanding of both dimensions is crucial to facilitate effective coordination

differences are manifested in different approaches, strategies and operational methodologies, and this also applies to alliances such as NATO, the Five Eyes, the European Union, ASEAN (Association of Southeast Asian Nations) and other coalitions operating in cyberspace. Despite having common goals, these alliances can be influenced by the individual cultures of member countries, adding another layer of complexity in coordinating cyber operations.

2.4 Navigating Cultural Divergences and Information Sharing Challenges

In the context of the States, in Russia, significant differences emerge between the GRU, the military intelligence agency, and the SVR, the External Intelligence Service. The GRU tends to be associated with more aggressive and direct operations, characterized by a frontal and immediate approach. In contrast, the SVR is known for adopting more subtle tactics and long-term strategies. This contrast in styles and methodologies can make coordination between GRUs and SVRs complex, particularly in situations requiring the sharing of sensitive information or the coordination of joint cyber operations[151].

The three central intelligence agencies in Israel, Aman, Shin Bet and Mossad, operate with distinct mandates and methodologies. Aman, the military intelligence agency, focuses on different aspects than the Shin Bet, which is responsible for internal security, and the Mossad, which focuses primarily on foreign intelligence. These variations in roles and approaches lead to significant differences in their operating styles. Such cultural divergences between agencies can critically affect how they interact, share information and collaborate, especially in complex operational contexts that require integration on multiple intelligence fronts[152].

In the United States, there is marked cultural diversity between agencies such as the CIA, NSA, and DIA. The CIA, geared towards human intelligence and clandestine operations, may need help coordinating with the NSA, which focuses on electronic surveillance and cybersecurity. These distinctions between agencies manifest themselves in their operational strategies and how they manage information, leading to potential coordination and collaboration difficulties. These military and intelligence agencies, deeply rooted in their national cultural koine, tend to display an attitude of suspicion and caution in sharing information. This tendency derives from the specific cultural formations of each nation, which emphasize the protection of national security and the safeguarding of its interests[153]. Such an approach can become a significant obstacle to cooperation and coordination between agencies and countries, especially in cyber operations. For example, the national security culture in the United States emphasizes data protection and external threats, leading agencies like the CIA and NSA to be especially cautious about sharing sensitive information. In Russia, where state security is a top priority,

in cyber operations, directly influencing strategies of interaction and collaboration between different entities operating in multicultural contexts.

[151] DiResta, Renee, e Shelby Grossman. "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019." Cyber Policy Center, Freeman Spogli Institute for International Studies, Stanford University, 12 novembre 2019. https://cyber.fsi.stanford.edu/io/publication/potemkin-think-tanks.

[152] Kahana, Ephraim. "Israeli Intelligence: Organization, Failures, and Successes." In The Oxford Handbook of National Security Intelligence, edited by Loch K. Johnson, Oxford Handbooks, 2010; online edn, Oxford Academic, 2 Sept. 2010.

[153] Bury, Patrick. "US Special Forces Transformation: Post-Fordism and the Limits of Networked Warfare." International Affairs 98, no. 2 (March 2022): 587–607

organizations such as GRU and SVR may be reluctant to share information that could compromise their operations or national security[154].
This caution in sharing information and the tendency to operate independently can create significant challenges in coordinating cyber operations, especially when a rapid and coordinated response to transnational threats is needed. Lack of trust and fear of exposing vulnerabilities are natural obstacles that can limit the effectiveness of joint action, making it more difficult to address complex challenges in cyberspace, where collaboration and information sharing are often crucial to the success of a specific operation.
Emerging information asymmetries can make coordination between different entities even more complicated, exacerbating challenges already present due to the diversity of technological standards, the speed of operations and the need to maintain information security. Furthermore, lack of trust, resource competition, and recognition between organizations can complicate the coordination landscape. These cultural elements and the practical and strategic difficulties discussed above highlight the urgency and complexity of developing new and practical approaches and frameworks for coordination in the cyber domain.

3. Balancing Flexibility, Autonomy, and Intelligence Integration

3.1 Balancing Command Rigidity and Operational Flexibility in Cybersecurity Coordination

While cultural and political differences undoubtedly represent limitations in coordination in cyberspace, another significant challenge to effective coordination is the difficulty of aligning the tactical/technical level with the operational level. In particular, between these two levels, there is a notable lack of coordination in cyber operations, which leads to significant problems in the Command and Control (C&C) chain, both in the flow of information and in operational effectiveness in the field. This aspect becomes even more critical in an international context, where the efficiency and effectiveness of operating methods are of fundamental importance. The complexity of establishing and maintaining a relationship of mutual trust and shared understanding of strategies and objectives between the two levels highlights the need for closer coordination. Therefore, meeting the challenge of effectively integrating the technical/tactical level with the operational level is essential to ensuring the success of cyber operations[155]. Coordination between offensive units and cyber headquarters is a significant challenge in military cyber operations. This challenge is amplified by the inherent complexity of cyberspace operations, where the speed and accuracy of tactical/technical and operational decisions are critical to success. The lack of effective coordination can lead to overlapping actions, waste of resources, slowdown of operations and increased detectability by adversaries. These problems,

[154] National Security Archive. 'The CIA and Signals Intelligence.' Last modified March 20, 2015. https://nsarchive.gwu.edu/briefing-book/cyber-vault-intelligence/2015-03-20/cia-and-signals-intelligence
[155] Priebe, Miranda, Douglas C. Ligor, Bruce McClintock, Michael Spirtas, Karen Schwindt, Caitlin Lee, Ashley L. Rhoades, Derek Eaton, Quentin E. Hodgson, e Bryan Rooney. "Multiple Dilemmas: Challenges and Options for All-Domain Command and Control." RAND Corporation, 2020

in turn, can compromise the effectiveness of offensive actions, reducing the potential impact on the enemy[156].

In particular, the discrepancy between decisions made at various levels of command can cause delays and confusion, negatively influencing the outcome of operations. The need for structured and adequate coordination emerges as a crucial element to maximize efficiency and minimize vulnerabilities in offensive strategies in cyberspace. The ability to quickly align objectives and actions between different levels of command, therefore, becomes a determining factor for the agility and reactivity of cyber operations[157].

The theoretical reflection on the importance of coordination in cyber operations underlines how the fluidity and dynamism of cyberspace require flexible and adaptive approaches. The integration of operational and tactical/technical strategies, together with the timely sharing of information and collaboration between the various actors involved, is essential to ease the challenges posed by cyberspace and to fully exploit the potential of cyber operations in the context of national security and international[158].

Rigidity in command and control structures in cyber operations, as in other domains, represents an essential strategic dilemma. On the one hand, adopting a well-defined command and control system can ensure that all actions are closely aligned with overall strategic objectives, providing order and coherence to operations. However, this rigidity can also limit the operational agility and creative capacity of units engaged in cyber activities, particularly in a rapidly evolving environment like cyberspace.

Speed and innovation are essential to maintaining a competitive advantage in cyber operations. The ability to quickly adapt to changes and respond innovatively to emerging challenges is crucial. However, an overly rigid chain of command and control can prevent operational units from fully exploiting their technical expertise, limiting their flexibility in dealing with complex and unexpected situations. In this context, rigidity can become an obstacle that slows the progress of operations and increases detectability by adversaries[159].

---

[156] Katagiri, Nori. "Two explanations for the paucity of cyber-military, cross-domain operations." Journal of Cybersecurity 8, no. 1 (2022)

[157] Nori Katagiri, "Two explanations for the paucity of cyber-military, cross-domain operations," Journal of Cybersecurity 8, no. 1 (2022)

[158] In the context of NATO cyber operations, the 2023 Crossed Swords (XS23) military exercise provided a unique opportunity to observe and analyze tactical/technical and operational coordination challenges. This exercise, which involved an Offensive Cyber Unit (OCU), an offensive unit aimed at specifically targeting coordinated directly by a Cyber Headquarters (CHQ), proved to be a relevant and significant case study. the picture that emerges as part of the exercise, specifically the execution of a simulation of attacks against the critical infrastructure systems and networks of an imaginary enemy nation, highlighted significant difficulties in the coordination of the Offensive Cyber Unit and the CHQ. Despite the involvement of a limited number of participants, the feedback from this activity highlighted fundamental elements on a theoretical level: a notable lack of coordination emerged, which caused an overlap of actions and a sub-optimal use of available resources. These issues have slowed the progress of operations and increased detectability by adversaries, thus reducing the overall effectiveness of simulated attacks. Specifically, during a phase of the exercise focused on the attack on specific objectives, a marked discrepancy was detected between the decisions made at the tactical/technical level and those at the operational level. This discrepancy caused delays and confusion, leading to the loss of crucial opportunities within the operation. The events recorded during the 2023 Crossed Swords Exercise highlighted how the lack of adequate and structured coordination between the different levels can negatively impact the effectiveness of cyber operations.

[159] Morgan, Adam S., and Steve W. Stone. 2019. "Command and Control for Cyberspace Operations - A Call for Research." Military Cyber Affairs 4, no. 1 (Article 4).

On the other hand, granting greater operational freedom to cyber units can foster creativity and innovation, allowing for a faster and more effective response to threats. However, this less structured approach can challenge coordination and strategic coherence, as non-aligned or contradictory actions can undermine overall objectives.
As a result, the need to find a balance between the need for structured command and control and operational flexibility emerges. An approach that allows for a certain degree of autonomy while maintaining solid strategic alignment may offer the optimal compromise. This requires effective communication and coordination mechanisms that enable agile information sharing and rapid decision-making, ensuring that cyber operations are innovative and strategically coherent[160].
In summary, the challenge in cyber operations lies in the distinction between offensive and defensive tactics and how command and control structures influence an organization's ability to act effectively in cyberspace. Finding solutions that balance rigidity and flexibility can guide the development of more effective and resilient cyber strategies.

3.2 Balancing Autonomy and Strategy in Cyber Operations: Implications for Innovation and Agility

In highly dynamic areas such as cybersecurity, speed of adaptation and response is crucial. Any form of delay can significantly compromise the effectiveness of operations. Structures that are too rigid risk limiting creativity, a key ingredient in cyberspace, where innovation often makes the difference. It has been observed that units with greater freedom of action tend to show superior performance, significantly when they are not constrained by overly tight coordination. This suggests that granting greater autonomy and flexibility to operational units could enhance their effectiveness, allowing them to capitalise fully on their technical and innovative skills[161].
The ability to operate with greater freedom, adapting in real-time and innovating according to the specific needs of the situation, is crucial in cyber operations. In this field, speed of reaction and the ability to think 'outside the box' is often the determining factor. The key to success. The Sandworm APT is a good example of this: the strategy adopted by Sandworm in cyber operations in Ukraine before the war began in February 2022 embodies the concept of autonomy and flexibility as critical elements for the effectiveness of offensive units. Before the war, Sandworm attacks were characterised by a more cautious and experimental approach aimed at intelligence gathering and gradual destabilisation. This initial period reflected the use of their technical and creative capabilities in a context of exploration and adaptation, preparatory to the terrain of future actions[162].

[160] Schoka, Andrew. "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat." War on the Rocks, April 3, 2019. https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/.
[161] In this context, it is specified that the 2023 military exercise Crossed Swords, organized by NATO CCDCOE, serves as a specific example, the exercise demonstrated that units with greater freedom of action tend to perform better, particularly when they are not limited by excessively stringent coordination, underlining the importance of balancing command rigidity with the need for rapid adaptation and innovation in the field of cybersecurity.
[162] Greenberg, Andy. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Anchor Books, 2020

However, Sandworm's approach displayed a transformation with the outbreak of the war, probably due to its greater hetero-direction. Operations have become more aggressive and direct, to target critical infrastructure and create immediate impact. This evolution in Sandworm operations, observed especially during the early stages of the war in Ukraine, reflects a shift towards louder and less discreet operations due to a greater need for aggression. This change of approach, aimed at supporting coordinated actions also at a kinetic level, led to a partial loss of their initial ability to act quickly and think "outside the box". Instead of maintaining its stealth and highly adaptive nature, the APT opted for a more direct and less flexible approach, necessary to achieve immediate and tangible objectives in the context of warfare that also supported kinetic units on the battlefield, as highlighted in Microsoft's report on Ukraine in the first quarter of 2022. This transition highlights a cyber trade-off: while an aggressive and less secretive strategy can be effective for short-term goals, it can sacrifice crucial elements such as agility and innovation, which it had previously been beneficial to Sandworm in 2015 cyber operations, causing significant disruptions to Ukraine's energy supply[163].

The observation that cyber operational units perform better in contexts less constrained by rigid command structures offers significant food for thought. Granting some autonomy to operators can improve the effectiveness of actions in cyberspace. This does not imply eliminating a command structure but requires a balance between operational and strategic oversight and technical/tactical freedom. Success in cyberspace relies on operators' technical expertise and ability to adapt quickly and think creatively. An operational model that integrates a clear strategic direction with sufficient space for autonomy and innovation is critical to optimizing the effectiveness of cyber actions, both offensive and defensive. In this context, finding the right balance between a rigid command structure and the need for operational flexibility is essential. Rigidity in the chain of command can limit operational capacity, highlighting the importance of a balanced approach. This difference in approaches highlights the importance of strategic considerations in cyber operations[164].

3.3 Integrating Human Intelligence (HUMINT) in Cyber Operations: A Strategic Approach to Enhancing Operational Agility

[163] Lilli, Eugenio. "How Can We Know What We Think We Know about Cyber Operations?" Journal of Global Security Studies 8, no. 2 (June 2023)

[164]The observation that OCU (Offensive Cyber Unit) during the 2023 Crossed Swords performed better in less coordinated situations with the CHQ is particularly illuminating. In the context of cyber operations, as seen in Crossed Swords, it is clear how crucial it is to find the right balance between the rigid command structure and the need for operational flexibility. The rigidity of the chain of command, which characterizes the approach of the Offensive Cyber Unit (OCU), which constitutes an essential element of the coordination activity, especially when compared with the greater freedom of action of the Offensive Cyber Operations (OCO), represents a limit on operational capacity. This difference in approaches offers essential food for thought.

The integration of intelligence, especially HUMINT (Human Intelligence)[165], is crucial for offensive and defensive cyber operations, as demonstrated by the case of Stuxnet above[166]. Cyber units benefit considerably from collaboration with HUMINT units, mainly when such coordination is based on equality and independence from the chain of command and control. This synergy allows cyber units to fully exploit the information gathered by HUMINT, which is crucial for identifying vulnerabilities and the strategic planning of attack and defence operations.

In terms of planning and executing operations, HUMINT provides essential context for threat attribution, a vital aspect in both defensive and offensive cyber. Accurate threat attribution provides insight into who is behind an attack, their motivations and capabilities. This information is crucial for developing effective strategies to neutralise adversaries or prevent further attacks. Another critical aspect is that HUMINT can offer unique insights into adversaries' behaviour, networks and intentions, which are only sometimes deducible through technical intelligence methods. This information can prove invaluable in planning offensive operations, where in-depth knowledge of the enemy can lead to more effective and targeted tactical choices[167].

Therefore, the balance between using intelligence and maintaining operational agility is essential. Using HUMINT, cyber units can significantly enrich their intelligence picture without losing the ability to adapt quickly and act dynamically. By avoiding the rigidity of centralised decision-making processes, cyber units can react more effectively and timely to threats, maximising the use of the information provided by HUMINT for both offensive and defensive operations[168]. This necessary balance between integrating intelligence, such as HUMINT, and maintaining operational agility in cyber units is reflected and explored in the resource 'Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision'. This study emphasise the importance of a decentralised approach and greater autonomy for cyber units, which are crucial for effectively managing threats in cyberspace.

The text 'Beyond the Build' analyses the synergetic collaboration between critical entities such as USCYBERCOM, DISA, NSA and the National Cyber Mission Force. Emphasis is placed on information sharing and lateral coordination, crucial aspects that enable rapid and targeted

---

[165] HUMINT, short for Human Intelligence, is a term used in intelligence to describe information gathered through human sources. This includes gathering data through conversations and direct interactions with people within relevant contexts, or by infiltrating organisations to acquire secrets or better understand a group's internal dynamics and intentions. In the cyberspace age, HUMINT's value has not waned but has been transformed. Cyber units often integrate HUMINT information with technical sources (SIGINT, CYBINT) to formulate more effective defence or attack strategies. The interplay between human expertise and advanced technologies enables a better interpretation of cyber threats and anticipation of adversaries' moves, linking traditional intelligence and new digital challenges.

[166] HUMINT provides vital insights into the intentions, capabilities and actions of potential adversaries that technical sources alone might not uncover, offering a comprehensive understanding that can significantly improve the strategic planning and execution of cyber operations. In fact, referring to the Stuxnet case, for the infiltration of the Iranian nuclear power plant in Natanz, Human Intelligence was used proactively to recruit the person who would later inject the malicious code into the plant's computer systems.

[167] Arata, Harold J., and Brian L. Hale. “Smart Bases, Smart Decisions.” The Cyber Defense Review 3, no. 1 (2018): 69–78.

[168] Nakasone, Paul M. 'A Cyber Force for Persistent Operations.' In Joint Force Quarterly 92, no. 1 (1st Quarter, 2019).

reaction to threats, similar to the dynamism of integrating HUMINT in cyber units. This lateral sharing of information is essential to enable cyber units to remain agile and responsive, taking advantage of the wealth of data provided by HUMINT and other intelligence sources[169].
On the other hand, Moore's text, Offensive Cyber Operations, focuses on the complexity of cyber warfare and the importance of advanced skills to deal with this challenging environment. It emphasises the need for an articulated approach that reflects the need for a flexible and adaptable[170]. This concept strongly agrees with the need for cyber units to effectively integrate intelligence without losing the ability to adapt quickly and act dynamically. These studies support the idea that, for cyber units, intelligence integration, particularly HUMINT, can maintain operational agility. Instead, there should be a synergy between intelligence gathering and rapid response capability, thus enabling cyber units to deal with threats in an effective and timely manner in the increasingly complex and changing environment of cyber-warfare[171].
In summary, in light of the above, the challenges related to cyber coordination call for a holistic and multidimensional approach that considers both theoretical and practical aspects. This holistic approach is closely related to the global vision concept I have discussed above. In particular, the discussion above highlights the importance of effectively integrating human intelligence (HUMINT) into cyber operations. This means that information gathered through human intelligence must be used synergistically and strategically to inform and improve the actions of IT units. This integration must maintain the operational agility of cyber units, whether defensive or offensive units, which must adapt quickly to emerging threats. Ultimately, the analysis of the above-mentioned texts provides insights into how to improve the effectiveness of cyber operations, emphasising the need for a comprehensive view, the integration of HUMINT intelligence, and the maintenance of operational agility as critical elements to successfully meet the challenges of cyber warfare.

3.4 Enhancing Cyber Operations Coordination: Towards an Integrated and Agile Approach

The challenge of coordination in cyber operations, both in the defensive and offensive phases, is a complex problem involving several aspects. To successfully address this challenge, it is essential to address technical, operational and cultural factors. To do so, it is necessary to work towards greater standardisation, communication and mutual understanding between the actors involved. Only through an integrated and universal approach, which considers all these factors, can the coordination and, consequently, the effectiveness of operations in cyberspace be improved.
To ensure successful operations, it is essential to base decisions on accurate information, make them promptly, and align with overall objectives. This process requires constant and clear communication between the parties involved and a thorough understanding of each group's internal dynamics and technical skills. Furthermore, in this era of advances in artificial

[169] U.S. Cyber Command Combined Action Group. "Beyond the Build: How the Component Commands Support the U.S. Cyber Command Vision." National Defense University Press, January 1, 2016.
[170] Moore, "Introduction," Offensive Cyber Operations.
[171] Jiang, Chaoyi. "Decoding China's Perspectives on Cyber Warfare." Chinese Journal of International Law 20, no. 2 (June 2021): 257–312.

intelligence (AI), leveraging new automation tools can be a valuable solution to improve coordination in cyber operations. Automation can help, especially in the cyber defence domain, to optimise responses to cyber threats and speed up data collection, information analysis and breach response, thereby improving the efficiency and timeliness of operations.
Despite substantial efforts to achieve coordination at the tactical and technical levels[172], several challenges persist that constitute formidable obstacles to creating a unified and decisive response in the digital realm. Despite these obstacles, the need for a collective approach characterised by shared intelligence, collaborative structures, and unified efforts to improve operational prowess is unequivocally established.

As I explore coordination dynamics within cyber operations, it is crucial to consider how a lack of coordination can be used strategically to weaken adversaries. This adversarial approach can, under certain circumstances, function as a disinformation tool or deception tactic to confuse and mislead adversaries about true cyber capabilities and intentions.

- Operational Decoys: Using the apparent lack of coordination as a decoy to divert adversaries' attention from the fundamental strategic operations.
- Compartmentalisation for Security: The practice of maintaining separate operations is not just a strategy, but a necessity to preserve operational security and prevent information leaks that could compromise entire campaigns.
- Innovation through Competition: Internal competition can stimulate innovation and the development of new technologies and tactics that, if uncoordinated, may be perceived by adversaries as unrelated and random.

Assessing these aspects offers a broader perspective on the complexity of operations in cyberspace and the need for a deeper analysis of the interplay between coordination and non-coordination in cyber strategies.

Challenges to Coordination in Cyber Operations	
Challenge	**Description**
Technical challenge	The technical complexity and rapidity of changes in cyberspace require advanced and up-to-date technical skills.
Operational challenge	The need to make rapid decisions aligned with strategic objectives in an ever-changing environment.
Cultural challenge	National and organizational differences between the various entities involved can hinder mutual understanding and coordination.
Standarditation Challenge	The lack of common standards can make interoperability and

[172] The situation in Ukraine following the outbreak of war in 2022 is a pertinent example of the challenges in achieving coordination at the tactical and technical levels in the digital realm. The conflict has seen diverse cyberattacks, including infrastructure targeting, information warfare, and cyber espionage, demonstrating the difficulty of coordinating defensive and offensive cyber strategies in a rapidly evolving and multifaceted digital battlefield.

	coordination between different systems and organizations difficult.
Communication Challenge	Challenges in effective communication can lead to delays or misunderstandings in the execution of cyber operations.
Intelligence- Sharing Challenge	Sharing intelligence between entities can improve the effectiveness of operations, but requires a high level of trust and secure sharing mechanisms.
Automation Challenge	Using automation in cyber defence operations can optimize response to threats, but requires careful management to avoid inadequate responses.

CHAPTER III

RESEARCH DESIGN

1. Introduction

1.1. Objectives and Context of the Research

In an era where cyberspace has evolved into a battlefield for geopolitical disputes, this dissertation delves into the intricate mechanisms of cyber warfare, with a particular focus on Advanced Persistent Threats (APTs). By examining APTs, I aim to understand the coordination dynamics in both offensive and defensive operations. While APTs primarily relate to offensive operations, studying them provides insights into the coordination and intelligence integration challenges necessary for effective cyber defence. This dual focus helps bridge my research's theoretical and empirical aspects, highlighting the interdependent nature of offensive and defensive cyber strategies and their impact on broader security dynamics.

This thesis spans multiple case studies, not limited to China, but also including Russia and NATO, to provide a comprehensive analysis of cyber operations in various geopolitical contexts. This focus connects my research's theoretical and empirical aspects, highlighting the interconnected nature of offensive and defensive strategies in cyberspace.

The approach encompasses a diverse array of methodological strategies to navigate the complexities inherent in this challenge. I initiate my investigation by exploring the multitude of interests at play: APTs, operating under the auspices of state entities, may pursue divergent objectives, thus complicating coordination efforts. Subsequently, I delve into operational security concerns, examining how the imperative of secrecy and a dearth of mutual trust among these groups can impede information sharing and collaborative endeavours. Additionally, my inquiry addresses the hurdles associated with coordination within the volatile realm of cyberspace, where disparities in language and time zones can present formidable obstacles to effective cooperation.

To frame my inquiry, I pose two key research questions:

- How can be conceptualized and quantify the role of coordination in cyberspace to understand how coordinated cyberattacks affect national and international security?
- How do these interactions affect the effectiveness of both offensive and defensive operations?

These questions guide my analysis as I seek to understand the impact of coordination on the efficiency of cyber operations. By examining the interaction between various APTs and their coordination challenges, I aim to reveal how technical and structural obstacles in cyberspace affect cyber conflict outcomes and broader security dynamics. For the defensive aspect, I will focus on these dynamics in a specific case of artificial intelligence that utilizes the same patterns observed in the offence context.

Through this in-depth investigation, the aim is not only to reveal the elaborate strategies deployed by APTs in the international context of cyberspace, but also to provide critical analyses of the complex power dynamics that shape relations between nations in the contemporary digital age. This dissertation, which crosses different disciplines such as international relations, security studies, computer science, and information security, is based on a wide and varied range of primary and secondary sources, including intelligence reports, academic works, and technical reviews, to develop a detailed analysis of the topic addressed.
This body of Information aims to provide professionals, both in the field of public policies and among cybersecurity specialists, with the tools necessary to navigate the complex scenario of cyber threats with full knowledge of the facts.

My research delves into the complexity of cyberspace operations, carefully selecting case studies that are significant in revealing the nature and challenges of coordination at the international level. These case studies, including Sino-Russian coordination in cyberspace during the war in Ukraine, competition between Russian intelligence agencies, and the Virtual Blue Team, were chosen for their unique insights into different aspects of cyber operations.

- *Sino-Russian coordination in cyberspace during the war in Ukraine*
  This case was selected to explore how two major cyber powers collaborate in a conflict. The war in Ukraine provides a context in which cyber operations are used as strategic tools by both Russia and China. This case helps identify the extent of coordination and challenges in joint cyber operations.
- *Competition between Russian intelligence agencies*
  The second case focuses on the internal competition between Russian intelligence agencies. Russian intelligence agencies, including the GRU, SVR and FSB, often compete, leading to a fragmented approach to cyber operations. Studying this competition reveals the inherent challenges in coordinating cyber efforts within a single nation-state. This case highlights the operational and technical difficulties that arise from the lack of coordination and the impact on the effectiveness of cyber operations.
- *The virtual blue team in Locked Shields Exercise*
  The third case study concerns the Virtual Blue Team's participation in Exercise Locked Shields, the global live-fire cyber defence exercise. This scenario provides insights into defensive strategies and the importance of coordination in a simulated environment. The exercise tests the Blue Team's capabilities to protect critical infrastructure from cyberattacks. This case highlights the need for coordination in defensive operations and the lessons learned from simulated cyber conflict scenarios.

By examining these cases, my study aims to contribute to the literature on cyber operations, offering practical insights into the coordination mechanisms that improve or hinder the effectiveness of cyber strategies. This dual focus on theory and practice not only highlights the importance of understanding coordination in both offensive and defensive contexts but also empowers the audience to develop more robust cybersecurity policies and strategies.

The objective of my investigation is to examine in detail the offensive and defensive strategies used in cyberspace to decipher the complex network of actions and tactics that characterize

today's digital landscape. These dynamics are fundamental, as they are emblematic of the power relations and alliances that form and evolve in the digital domain. Offensive operations, especially those observed in the context of the Russian-Ukrainian conflict, illuminate the more aggressive side of these cyber operations, offering fundamental insights into understanding how coordination and confrontation develop in cyberspace.

In parallel, from a defensive point of view, the objective of the third case is to examine the Locked Shields exercise, one of the leading annual cyber defence simulations organized by NATO and, in particular, by the NATO CCDCOE. Locked Shields are one of the most advanced and realistic cyber defence exercises globally. This military exercise creates a simulated environment in which a virtual blue team, competing alongside other real teams, acts as a sophisticated intrusion detection system (IDS) to detect attacks orchestrated by an adversary team, known as a Red Team or APT99, on virtual infrastructures. The exercise represents a unique platform to test and improve defence capabilities and provides crucial data and scenarios for analyzing and understanding attack and defence dynamics in cyberspace.

This defensive scenario aims to highlight the stark contrast to offensive actions, underlining its significance in illustrating how advanced defence strategies and, specifically, automation can promote improved coordination in cyberspace. This case is particularly pertinent to show how adopting sophisticated defensive tactics and creating realistic simulation environments can serve as catalysts for effective collaboration between the actors involved, helping to strengthen security in cyberspace.

Choosing two cases focused on offence (the degree of sino-russian coordination in cyberspace during the Ukraine war and the competition between Russian intelligence agencies), and one on defence (the virtual blue team) is not accidental. Through analysing such cases, the aim is to highlight how offensive operations, such as those alleged between China and Russia and disputes between intelligence agencies in the Russian context, expose challenges in coordination and mutual distrust, elements present in cyberspace. These dynamics are contrasted with the defensive approach exemplified by the Locked Shields exercise, which highlights the importance and potential for improvement in cooperation and coordination through advanced defence, although distinct from offensive operations. Locked Shields is specifically structured to serve as an exercise that promotes, at a strategic level, international cooperation and, at the same time, coordination between the various military layers operating in cyberspace. Through an iterative process of trial and error and annual lessons learned, the exercise offers a unique opportunity to test and refine defence strategies, encouraging collaboration between nations and improving the capacity for a coordinated response to cyber threats. This engagement in cyberspace ideally aims to strengthen national and international defences and establish a model of cooperation and coordination that serves as a benchmark for further cybersecurity initiatives.

By incorporating these case studies, the research aims to provide a detailed overview of the challenges related to coordination and collaboration in cyberspace. Through qualitative case study research, I seek to clarify these dynamics, exploiting methodologies that allow an in-depth understanding of the complex issues at stake. Qualitative case studies are particularly suitable for this type of research as they allow for a comprehensive exploration of complex phenomena over an extended period.

Offensive operations reveal the difficulties and complexity of alliances and the distrust between state actors. In contrast, the defensive case offers a perspective on how advanced strategies and automation can help overcome these barriers. However, the emphasis remains on the observation that, despite its potential, cyberspace continues to be a frontier characterized by coordination challenges due to competition and mistrust.
Methodologically, this research uses qualitative case study methods to examine these issues thoroughly. According to Bennett and Elman[173], qualitative research has seen significant developments in case study methods, which allow for examining a wide range of variables and understanding complex interrelationships within real-life contexts. These methodologies allow us to analyze specific instances of cyber operations, providing practical and valuable insights into the broader challenges of cyber coordination and collaboration.
By integrating these methodological approaches, our study not only highlights the inherent difficulties in offensive and defensive cyber operations but also significantly contributes to the broader academic discourse on cybersecurity. It brings to the forefront the persistent issues of competition and mistrust in the digital arena, which are crucial for understanding the challenges of coordination and collaboration in cyberspace.

1.2. Exploring Coordination Challenges in Cyberspace Through Case Studies

By adopting cutting-edge intelligence methodologies as the F3EAD intelligence cycle and a detailed analysis of publicly available data (APT Reports, Threat Intelligence Feeds,Cyber Incident Repositories) the aim is to depict a precise image of the intricate dynamics governing the cyber battlefield. Through an examination of the modes of interaction, or lack thereof, between China- and Russia-related Advanced Persistent Threats (APTs), my objective is to offer a novel interpretation of the predominant tactics observed within the digital landscape. The first case study highlights these concepts and the absence of cooperation and coordination in a macro context in the dynamics between the two states. However, distinct in theory, they are fundamental to fully deciphering the dynamics that shape international relations in the digital context. By integrating these considerations, my study strives to explore the challenges inherent to coordination and collaboration in cyberspace. Cyber offensive operations highlight the complexities and challenges of alliances and mutual trust between national actors. In contrast, the second case study focuses on a lack of coordination at a micro level, particularly the challenges among intelligence agencies in Russia. This choice of investigation aims to reveal how, in a narrower and more defined scope, the lack of synergy can represent a significant obstacle to joint operations and the results that these operations can achieve in a war context, reflecting a wide range of challenges of coordination that permeate cyberspace. This detailed analysis of the internal dynamics of Russian intelligence agencies serves not only to highlight the difficulties of coordination at an operational and technical/tactical level but also to illustrate how such challenges can negatively influence the overall effectiveness of operations in the digital domain.

[173] Bennett, Andrew, and Colin Elman. "Qualitative Research: Recent Developments in Case Study Methods." Annual Review of Political Science 9, no. 1 (2006): 455-476.

Continuing in this direction of investigation, the thesis focuses on a third case: the Locked Shield. This third case offers a comprehensive vision of how Locked Shield can act as an ideal point for clarifying the challenges of coordination in cyberspace.
However, despite the potential offered by advanced strategies and automation, cyberspace remains a complex environment characterized by coordination challenges fuelled by rivalries and mistrust. This context provides a valuable framework for understanding barriers to practical cooperation and identifying potential avenues to improve the coordination and efficiency of cyber operations at national and international levels.
This investigation fits into the broader context of my previous analyses, which explored the dichotomy between offensive and defensive operations in cyberspace, represented by interstate tensions and alliances and NATO's Locked Shields simulation, respectively. The choice of these case studies is not random but aims to reveal the coordination challenges that permeate cyberspace. In this dimension, collaboration proves crucial and difficult to achieve due to rivalries and suspicions.

1. APT Threat Analysis and Coordination

2.1. Dynamics of Coordination

To achieve the objectives set in this thesis, i.e. the detailed analysis of the activity of Advanced Persistent Threats (APTs) with alleged Chinese involvement and the evaluation of possible coordination between Chinese or Russian groups, three distinct but complementary methodologies have been adopted.
The first methodological axis is based on the analysis of competing interests. Given that APTs are often sponsored by state entities and driven by geopolitical motivations, it is plausible that different groups may pursue conflicting goals or objectives, thus hindering their ability to coordinate effectively. This aspect is fundamental to understanding the internal dynamics between groups, which, although operating under the aegis of similar state interests, may find themselves competing or disagreeing on specific operational objectives.
Next, the issue of operational security is examined. Advanced Persistent Threats (APTs) operate in a context of secrecy and may not trust each other, thus making the sharing of information or coordinating activities problematic. This element is crucial for evaluating the feasibility of coordination between different groups, since the need to preserve the security of one's operations can significantly limit collaboration.
The challenges related to resource management are also delved into. Advanced Persistent Threat (APT) operations are inherently complex and require considerable human, financial, and technological capital investment. Effectively coordinating these resources between different groups, which may have different structures and priorities, represents a remarkable undertaking. Effective collaboration can only result under specific circumstances.
Finally, communication barriers are addressed. Linguistic diversity and time zone differences between Advanced Persistent Threat (APT) groups can further complicate coordination and timely information sharing, constituting a significant barrier to collaboration.

A further methodological reflection concerns the risk of misinterpreting APTs as part of a large-scale coordinated effort based on the similarity of the tactics and techniques employed, such as spear phishing attacks, social engineering, or zero-day exploit. This presumption could obscure the understanding of the absolute independence and specificities of each APT group, as well as the complex texture of relationships between APTs.
From this emerges a panorama in which the presence of a central coordination direction behind the APT attacks could seem a logical conclusion; however, the reality of cyberspace turns out to be considerably more multifaceted. Many APTs act with a high degree of autonomy or organize themselves into tight collectives, conducting operations with minimal levels of coordination with other malicious entities. This operational independence underlines the complexity and variety of strategies adopted in the global cyber landscape.
In the context of the first and second cases, an alternative investigative approach is adopted to explore the need to intensify cooperation between different Advanced Persistent Threats (APTs). To this end, in the first case, the focus is on three specific actors: Mustang Panda, Scarab, and Judgment Panda. These groups were chosen for their significant presence following the outbreak of the Russian-Ukrainian conflict, with several indications from multiple sources of potential synergy between Russia and China in cyber operations. The selection of these groups is based not only on their temporal relevance but also on the wealth of publicly available information, which allows for an in-depth analysis of their activities from the beginning of the conflict until the end of 2022.
Through the examination of Mustang Panda, Scarab, and Judgment Panda, the intention is not only to explore the capabilities and operations of these Advanced Persistent Threats (APTs) but also to reflect on how their actions fit into the broader context of international relations in cyberspace. Particular attention is paid to the possibilities of improving coordination between different groups to address shared challenges more effectively.
In the second case, the focus is on the three leading Russian intelligence agencies, the GRU, the SVR and the FSB, examining the Advanced Persistent Threats (APTs) linked to them. This choice is based on these agencies' importance in Russian cyber operations, highlighting their crucial role in cyber warfare and digital espionage activities. Analyzing the APTs linked to the GRU, the SVR and the FSB allows us to probe in depth the tactics, techniques and procedures adopted by these entities.
By focusing on these agencies and their associated APT groups, The aim is to paint a detailed picture of Russian cyber operations, reflecting on potential synergies between these and other cyber entities and how such collaborations may influence the international cybersecurity landscape. This approach also allows us to explore the strategies these agencies adopt in navigating the complex context of international relations in cyberspace, emphasizing the importance of effective coordination between different actors to more comprehensively address emerging cyber threats.

2.1. APT Analysis Methodologies

To understand and analyse the threats posed by Advanced Persistent Threats (APTs), we use four main tools: Mandiant Advantage, the F3EAD intelligence cycle, Open Source Intelligence (OSINT) and the MITRE ATT&CK framework. This combination allows us to conduct an in-depth analysis of the

operations and techniques of APT groups. In the first and second case studies, Mandiant Advantage was essential to identify threat groups and assess the reliability of attribution. The F3EAD cycle provided a rigorous framework to explore interactions between cyber actors, while OSINT enriched the understanding of the APTs' operational context. Finally, the MITRE ATT&CK mapped the operational methodologies in detail, highlighting differences and similarities between the attack techniques of the various groups. This integrated approach has improved the accuracy of my analysis and my understanding of the complex relationships between APT groups, particularly those associated with China and Russia.

2.1.1. Mandiant Advantage

During the investigation into Advanced Persistent Threats (APT) in the two offence cases, the Cyber Threat Intelligence (CTI) databases offered by Mandiant were utilized, with explicit access to the Mandiant Advantage platform. This tool was not originally designed to explore the coordination dynamics between different APT groups.However, it has proven to be of fundamental importance to the success of my research.
Using Mandiant Advantage allowed to take several crucial steps in my analysis:

- *Threat Group Identification*: The platform provided direct access to detailed Information about various APT groups. Based on a vast set of data and intelligence reports, it was possible to filter and identify those groups explicitly associated with China and Russia.
- *Evaluation of the Reliability of the Attribution*: A fundamental aspect of my work was the evaluation of the credibility of the attribution of each APT group to a specific country. Mandiant Advantage offered us tools to analyze and understand attributions' reliability level, allowing us to focus on those APTs for which the attribution was considered "almost certain". This involved the analysis of various attack indicators and patterns, as well as the evaluation of evidence and reports linking APT activities to the national interests of the countries in question.
- *Insight into Techniques, Tactics and Procedures (TTPs)*: The platform facilitated the analysis of TTPs employed by threat groups. This allowed us to understand the attack and defence methodologies better, offering an in-depth view of the offensive capabilities of these entities and their evolution over time.
- *Collaboration and Information Sharing*: Using Mandiant Advantage, we have also benefited from Information sharing within the security community. The platform facilitates the exchange of insights and analyses between various actors in the field of cybersecurity, enriching my research with different perspectives and experiences.

The use of Mandiant Advantage in my investigation of APTs linked to China and Russia represented a fundamental pillar for data collection, analysis and interpretation. This tool has allowed us to identify and analyze threat groups with a high degree of precision and deepen my understanding of their operations, strategies and links to the national interests of the attributed countries, all using an integrated platform full of features.
In detail, the in-depth analysis of the Information available on Mandiant Advantage allowed us to perform a meticulous and specific analysis centred on the tactics, techniques and procedures

(TTPs), the infrastructure used, the timestamps associated with known attacks and other indicators of impairment (IOC) attributable to the APT groups investigated. This detailed analysis had as its primary objective the discovery of any patterns of behaviour that could indicate forms of coordination between the various APT groups and the detection of significant divergences in their work.

To accomplish this task, the Tactics, Techniques, and Procedures (TTPs) used by each Advanced Persistent Threat (APT) group were systematically catalogued and compared, observing how their attack campaigns were implemented. The analysis of the infrastructures used, including command and control servers, masking techniques and infiltration methodologies, provided further elements to understand the depth and breadth of the operations conducted. Additionally, examining the timestamps of known attacks and IOCs allowed us to trace the history of each group's campaigns, highlighting any temporal or geographic overlaps that might suggest collaboration or conflict.

A crucial aspect of the analysis was the identification of the specific objectives pursued by the different Advanced Persistent Threat (APT) groups, especially for the second case. By examining the targets of their operations, cases were identified where the goals seemed to conflict or compete with each other, revealing the complexity of the strategies. This element was particularly illuminating, as it highlighted the possible existence of shared objectives between groups affiliated with the same nation-state and the presence of competitive dynamics or mutual interference when objectives overlapped or diverged. Through this in-depth analysis work, based on the integration and correlation of data and information provided by Mandiant Advantage, a more precise and detailed picture of the inter-group relationships between Advanced Persistent Threats (APTs) was built. This understanding has significantly enriched my knowledge of how these groups operate, their ability to adapt and the nature of their campaigns, giving us a more nuanced perspective on the cyber threat landscape related to China and Russia.

My methodological approach, which has integrated the advanced use of the Mandiant Advantage platform, represents a natural evolution and deepening of my initial research. At that stage, the importance of coordination and mutual trust within cyberspace was highlighted, underlining how these elements play a crucial role, especially between state actors and Advanced Persistent Threats (APTs). My initial analysis had already highlighted the complexity of the relationships and interactions between these actors, emphasizing the need to understand better how cooperation and coordination influenced strategies and operations in the cyber context.

Mandiant Advantage has allowed us to significantly expand this understanding significantly, giving us advanced tools for analyzing and evaluating operations conducted by APTs, particularly those linked to China and Russia. This platform gave us access to a wide variety of data and Information, from technical details on the techniques, tactics and procedures used to the specific targets and infrastructure employed in the attack campaigns. Through detailed analysis of these elements, we were able to identify not only similarities but also significant discrepancies between APT groups, shedding light on potential areas of cooperation or possible conflicts of interest.

Delving further, my research explored how these entities might collaborate or, conversely, operate independently or in competition. This aspect is of particular importance since it reveals

the complex internal dynamics of cyberspace and the intrinsic challenges of coordination and cooperation between different actors. my analysis has, therefore, contributed significantly to the debate on strengthening defences and promoting more effective international cooperation in countering cyber threats.

2.1.2. F3EAD intelligence cycle.

This in-depth investigation into the offence cases used a rigorous methodological approach, at the heart of which is the F3EAD intelligence cycle. This model, rooted in Western military operational practices, has been adapted to explore the complex relationships between threat groups in cyberspace. The F3EAD structure, with its six phases of Find, Fix, Finish, Exploit, Analyse and Disseminate, provided a methodological framework to systematically investigate the existence, nature and intensity of interactions between these cyber actors.

- In the *Find phase*, we initially identified APT groups of interest, using known threat indicators and activity as a starting point. This included analysing intelligence reports and examining cyberattacks previously attributed to Russian and Chinese entities, thus facilitating the preliminary selection of groups to be examined more closely.
- into the *Fix phase*, It has been refined this selection through more detailed information gathering, exploring the specific operations, infrastructure used, and tactics, techniques, and procedures (TTPs) employed by the groups. This required intensive use of Cyber Threat Intelligence platforms such as Mandiant Advantage and analysis of open-source sources to obtain a clearer picture of the capabilities and behaviours of these actors.
- In this research context, the *Finish phase* focused on delving into vulnerabilities and attack techniques, although the main objective was analysis rather than direct intervention. This has allowed us to understand better how APT groups exploit specific weaknesses in cyberspace to advance their objectives.
- Attack pattern data have been examined attack pattern data in the *Exploit phase* to gain valuable intelligence.
- In the *Analyse phase*, patterns and connections have been identified between the Information collected, highlighting potential areas of cooperation or conflict between APT groups.
- The *Dissemination phase* involved sharing my findings with the cybersecurity community, contributing to the body of knowledge on how to counter threats in cyberspace effectively.

Through the application of the F3EAD cycle, it was deduced that, despite motivations, different operational goals and objectives can make coordination between APTs difficult or unlikely. This complex picture highlights the challenges of coordination and mutual trust in cyberspace, underscoring how competing interests, operational security concerns, and legal constraints often impede effective coordination. However, by identifying shared Tactics, Techniques, and Procedures (TTPs) and analysing the operations conducted, a more complete understanding of the threat was built, highlighting the importance of integrated defence strategies and strengthened international cooperation to address the challenges posed by APTs in the digital domain.

The Analyse phase of the F3EAD cycle proved to be particularly crucial. Through careful evaluation of the collected data, activity patterns that reflect open competition between APT groups were discerned. For example, analysis of the targets of their operations revealed that, in some cases, the objectives were so closely aligned as to suggest a form of coordination or at least an avoidance of conflicting actions. On the other hand, examining campaign attack techniques has shown how these entities can operate independently, with objectives sometimes overlapping competitively.
Notably, the challenges of gathering accurate and timely Information on these APTs remain significant. Competing interests and the clandestine nature of APT operations further complicate analysis efforts. However, the methodical application of the F3EAD cycle has proven to be a practical approach to overcome these barriers, allowing us to draw informed conclusions about the relationships between APTs and their operational strategies. my study highlighted that, despite the inherent difficulties between APTs, moments of synergy could be exploited to strengthen countermeasures and defence strategies.

2.1.3 OSINT

Open Source Intelligence (OSINT) collection has played a critical role in deepening my understanding of the dynamics between APTs, offering a lens through which to evaluate the alleged lack of coordination between various threat groups for various reasons. Unlike Cyber Threat Intelligence (CTI) databases, which focus predominantly on technical data and indicators of compromise (IOC), OSINT sources - which include social media platforms, online forums, blogs and newspaper articles - have open access to a vast spectrum of Information. These resources offered valuable insights into the tactics, techniques and procedures (TTPs) adopted by the APTs studied and the specific objectives of their campaigns, the targeted objectives and the motivations behind their actions. Integrating OSINT into my analysis toolkit has allowed us to capture the nuances of APT strategies beyond the purely technical aspect, illuminating the broader context in which these entities operate. For example, discussions in online forums and social media posts can reveal recruitment attempts or expansion of technical capabilities. At the same time, newspaper articles and blogs can provide geopolitical context or reactions to specific cyberattack campaigns, offering a more perspective on the motivations and intentions of the actors.
Furthermore, OSINT has proven crucial in identifying information gaps in CTI databases. Through the analysis of open sources, it was possible to highlight areas not sufficiently covered by traditional data collection, such as the internal dynamics between different APT groups or their reactions to international security policies. This allowed us to fill these gaps with additional Information and guided the definition of new research paths, incentivizing further investigations to refine my understanding of APT operations. More generally, using OSINT in analysing APTs has highlighted the importance of a holistic perspective in approaching cyber threats. While CTI sources provide essential technical details to understand how APTs conduct their campaigns, OSINT offers the context to interpret why these campaigns are launched and their strategic objectives. This expanded understanding is indispensable to address the challenges posed by APTs effectively, underlining the need for greater coordination between

cyber defence entities and analysts who draw on different intelligence sources to build an overall view of the threat landscape.
In the context of my in-depth analysis of the dynamics of cooperation and coordination between Advanced Persistent Threats (APT), The study was enriched with the integration of data and information deriving from specific analytical tools: the MITRE ATT&CK framework, the Malware Information Sharing Platform (MISP), and Yara rules. These tools have represented fundamental pillars for deciphering the complex interactions between APT groups, especially in identifying their tactics, techniques and procedures (TTPs) and evaluating their (lack of) cooperation.

2.1.4 MITRE ATT&CK

The MITRE ATT&CK framework, with its comprehensive taxonomy of offensive behaviours, offered a solid basis for cataloguing and comparing the operational methodologies of the APT groups under study. By applying this framework, specific attack patterns were detected that showed no evidence of active collaboration or sharing of critical infrastructure, despite targeting the same objectives or sectors. This aspect suggested the existence of largely independent operations between the groups, which could indicate a lack of coordination or, in some cases, the execution of competing agendas.
The MISP platform, an open-source tool dedicated to sharing threat intelligence between different organizations, has further expanded my scope of investigation. Analysis of the data and Information shared via MISP identified unique activity patterns, revealing situations where overlaps in attack campaigns were not supported by clear operational synergy between APT groups. This strengthened the hypothesis of operations conducted independently, sometimes even in competition.
Yara rules, used for the recognition and classification of malware by defining specific behavioural patterns or characteristics, have significantly contributed to the precise monitoring of the activities of APT groups. Analysing the matches obtained from Yara rules specific to each APT group could highlight significant differences in the malware toolkits used. These differences further indicated a lack of resource sharing and coordination between the groups, suggesting that each pursues its strategic objectives with distinct methodologies.
By combining the analyses provided by the MITRE ATT&CK framework, the MISP platform, and Yara rules, a more detailed picture of the lack of cooperation between different APT groups was painted. This study highlighted the need to develop more sophisticated cyber defence strategies capable of adapting to the continuous evolution of APT tactics. The use of these analytical tools, together with a rigorous research methodology, has made it possible not only to trace each group's specific activities but also to understand better the overall dynamics that govern interactions in cyberspace. The MITRE ATT&CK navigator tables, included in the appendix of this study, offer a systematic and easily accessible overview of the TTPs associated with the analysed APT groups, serving as an essential reference for future research and the development of effective countermeasures. Within my in-depth investigation into the dynamics of cooperation and coordination (or lack thereof) between China- and Russia-related Advanced Persistent Threats (APTs), The methodological approach was enriched by incorporating three

vital analytical tools: the MITRE ATT&CK framework, the Malware Information Sharing Platform (MISP), and the Yara rules. This integration allowed for a further refinement of the analysis, providing specific tools to decipher the complexity of the operations conducted by these threat groups and to assess the extent to which they operate in a coordinated or independent manner.

The MITRE ATT&CK framework, with its extensive taxonomy of tactics, techniques and procedures used by attackers, was the cornerstone of my comparative analysis. This tool allowed us to map the operations conducted by Chinese and Russian APTs in detail by comparing their methods to a wide range of offensive behaviours encoded in the framework. Examining the activities of these APT groups through the lens of MITRE ATT&CK revealed that, despite some overlap in objectives or tactical approach, operational modes often differed, indicating an absence of direct coordination between them. For example, the choice to exploit specific vulnerabilities or deploy certain malware toolkits varied significantly, suggesting autonomous operational strategies rather than concerted action.

In parallel, using the Malware Information Sharing Platform (MISP) has amplified the ability to detect activity patterns between different APT (Advanced Persistent Threat) groups. By analysing intelligence data shared through this open-source platform, observations were made on how, in some cases, different groups were targeting the same infrastructure or sectors without apparently sharing resources or information. This further highlighted the lack of effective coordination, reinforcing the idea of independent operations that, while converging towards similar objectives, showed no signs of strategic collaboration.

Finally, Yara rules enforcement offered a precise means to identify and track malware used by APT groups, allowing us to discern between various actors based on their unique threat profiles. Creating and analysing Yara rules specific to malware associated with Mustang Panda, Scarab, and Judgment Panda facilitated the detection of distinct attack campaigns, with evidence of different infection tools and methods indicating separate operational strategies. This targeted use of the Yara rules has revealed the complexity of the evasion and deception tactics adopted by the groups, underlining how the lack of coordination can also result from a deliberate strategic choice to disguise their operations and confuse analysts.

In conclusion, the synergistic use of MITRE ATT&CK, MISP and Yara rules has enriched my analysis of APTs, highlighting the sophisticated complexity of their operations in cyberspace. While the lack of coordination between APT groups may seem like an advantage for cyber defence, it also reflects the diversity and adaptability of cyber threats, which require my constant attention and increasingly advanced analysis methods. The MITRE ATT&CK navigator tables, included in the appendix, provide immediate reference to the TTPs identified for Mustang Panda, Scarab and Judgment Panda, serving as the basis for future investigations and the development of more effective defence strategies in countering the constant threat posed by APTs in the global cybersecurity landscape.

2. Virtual Blue Team in Locked Shields Exercise

In the third case study on the Virtual Blue Team (VBT), a rigorous methodological approach has been adopted for the collection and analysis of network data to monitor cyber defence activities during large-scale cybersecurity exercises, such as the 'Locked Shields' exercise. This approach utilized an advanced technological infrastructure and precise data collection strategies to ensure adequate capture and detailed analysis of network traffic.

3.1. Data Collection Infrastructure

A combination of cutting-edge tools and technologies, including AICA (Automated Indicator of Compromise Analyzer) and Frankenstack, was implemented for raw data collection. For a deeper understanding, AICA and Frankenstack serve as two key tools for collecting and storing data as part of Locked Shields, one of the most complex international cyber defense simulations. AICA is an advanced framework developed to automate the analysis of Indicators of Compromise (IoC).

AICA's primary goal is to simplify the process of identifying, collecting and analysing these indicators, providing more effective tools for the early detection of cybersecurity threats. AICA stands out for its ability to process and analyse large volumes of log data, network traffic and other system data types, using advanced algorithms to identify anomalies and suspicious patterns. This significantly accelerates the threat identification process, improving the responsiveness of security teams. In contexts like Locked Shields, where the speed and effectiveness of response to threats are critical, the use of AICA represents significant added value. Frankenstack is a framework designed specifically for monitoring Red Team activities in complex network contexts. Its name evokes the idea of a system assembled from different components to create something powerful and versatile, just like the famous literary character. Frankenstack is characterized by its extreme scalability and flexibility, being able to adapt to various operational scenarios and scale according to the needs of the military exercise. As part of Locked Shields, Frankenstack was used to monitor the Red Team's activities in real-time, collecting network traffic data, event logs and other relevant Information to analyze the attack techniques and tactics used. Its ability to manage a high volume of data and provide an integrated view of suspicious activities makes it an indispensable tool for defence teams (blue teams) and the organization of the exercise.

Integrating Frankenstack with AICA has allowed us to create a highly effective data collection and analysis ecosystem. Frankenstack offers a scalable platform for monitoring network activities, and AICA provides the analytical tools for data processing and interpretation. This synergy between the two tools made comprehensive and integrated data collection possible, significantly improving the ability to detect and respond to cyber threats during Locked Shields.

3.2. OSQuery and Distribution System integration

To further enrich the data collection infrastructure for capturing a holistic view of network activity during Locked Shields, OSQuery was integrated into the technology arsenal. OSQuery, a powerful open-source tool, allows for querying the state of hosts in real-time, similar to querying a relational database, but to obtain detailed metadata directly from the hosts' operating system. This tool has proven valuable for extending data collection beyond network traffic, allowing us to access a wide range of host-related metadata, such as running processes, open network connections, system configurations, and much more. Recognizing the importance of consistent and broad coverage logging, a purpose-built distribution system was developed. This system is designed to automate the logging client deployment across all Virtual Blue Team (VBT) hosts, ensuring that each participating device, distributed across different network segments, is configured to send logging data to a centralized repository. Automating this process has significantly reduced the time and effort required for manual setup, ensuring that data collection is complete and consistent across the operating environment.
OSQuery integration, along with advanced tools like AICA and Frankenstack, has created a complex data collection and analysis ecosystem. This combination made it possible to monitor the activities of the Red Team and Blue Teams efficiently. It offered the possibility of obtaining deep insights into the security state of the simulated IT infrastructure. The dedicated distribution system further optimized this process, enabling agile and responsive management of logging clients and ensuring that each host contributed to the flow of analytical data, which is critical for the timely detection of threats and vulnerabilities during the Locked Shields exercise.

3.3. Network Traffic Acquisition

As part of the methodological approach for data capture and analysis during Locked Shields, a network traffic capture strategy was implemented that leverages Encapsulated Remote-Switched Port Analyzer (ERSPAN) technology. This choice allowed network traffic to be mirrored from different segments within the complex Locked Shields architecture directly to a dedicated Arkime instance, an advanced network traffic analysis tool. This method fits perfectly into the workflow outlined above, which included using OSQuery for host-based logging and the synergistic combination of AICA and Frankenstack for raw data collection and storage. Deploying ERSPAN has extended my monitoring capability, allowing us to pass network traffic across Locked Shields' vast network without needing dedicated hardware for each network segment, thus facilitating remote, centralized analysis.
Once the traffic was redirected to the Arkime instance, an Exploratory Data Analysis (EDA) was undertaken to scrutinize the traffic. This EDA process was crucial in identifying attack patterns, anomalies, and other suspicious activity within network traffic. Thanks to Arkime's computational power and flexibility, it was possible to filter, analyze, and visualize data in real-time, significantly improving the ability to detect threats.

The methodology adopted, from data collection with advanced technologies such as ERSPAN, OSQuery, AICA, and Frankenstack, to exploratory analysis with Arkime, represented an overall and integrated strategy. This approach allowed us to effectively and efficiently monitor network activity during Locked Shields and provide defense teams with the tools and Information needed to quickly identify and respond to threats in a highly competitive and dynamic simulated environment.

3.4. Exploitation of Metainformation

As part of my data collection and analysis methodology for the Locked Shields exercise, a distinguishing feature was access to a rich set of meta-information provided by the green team. This unique access greatly enriched my ability to understand and navigate the complex network environment created for the exercise. The meta-information included essential data such as the MAC and IP addresses of the virtual machines (VMs) employed in the exercise and a detailed mapping of the entire supporting infrastructure, which simulated a realistic and multifunctional IT environment.

The integration of this meta-information represented a logical continuation and enhancement of the previously described strategies, particularly the use of technologies such as ERSPAN for network traffic mirroring and exploratory data analysis (EDA) via Arkime. Thanks to the in-depth knowledge of network architecture and host configurations provided by the Green Team's meta-information, Analysis techniques were further refined, specifically targeting those network segments and IP addresses most relevant to the investigation of potential threats and suspicious activities. This in-depth understanding of the infrastructure has allowed us to more accurately identify anomalous or potentially malicious traffic patterns, significantly improving my efficiency in identifying and categorizing threats. Furthermore, access to Information on the full range of IP addresses and network segments used in the exercise facilitated the orchestration of a more targeted and informed security response, allowing defence teams to focus their resources where they were most necessary.

Metainformation within Locked Shields has significantly broadened my analytical horizon, allowing us to integrate data collected through advanced traffic capture and log analysis tools with a detailed understanding of the simulated network environment. This comprehensive approach has ensured unprecedented visibility and understanding, essential to successfully address the challenges posed by such a dynamic and complex cyber defence scenario.

3.5. Innovations in Arkime

During exploratory data analysis (EDA) as part of the Locked Shields exercise, a significant challenge was encountered in accurately labeling captured network traffic data. The presence of dynamic or misconfigured IP addresses in the dataset made reliably identifying threats and suspicious activities complex. To address this issue and improve labeling accuracy, an initiative was undertaken to develop and integrate support for Generic Routing Encapsulation (GRE) into Arkime, a vital tool in the traffic analysis arsenal of the networks.

The integration of GRE support into Arkime represented a crucial methodological advancement, allowing us to overcome the limitations related to managing variable IP addresses. This technology has allowed us to filter network traffic more effectively by associating dynamic or local IP addresses with previously identified known and suspicious IP addresses. As a result, the accuracy of data labelling has significantly improved, making it easier to identify anomalous or potentially malicious traffic patterns and, consequently, detect threats more precisely and timely. This development fits perfectly into my overall methodology for analyzing cybersecurity during Locked Shields. Adopting advanced tools such as OSQuery, AICA, Frankenstack, and in-depth analysis through Arkime, now enriched by GRE support, has underlined the importance of a robust technological infrastructure and sophisticated data collection and analysis methodologies. This integrated approach has significantly enhanced my ability to monitor, detect and analyze threats in real-time, providing a more agile and informed response to complex cyber defence challenges.

Furthermore, using these advanced strategies has opened up new avenues for using artificial intelligence and machine learning in cybersecurity. Through more precise data collection and in-depth analysis, high-quality datasets could be fed into machine learning models, improving the systems' ability to predict and counter emerging threats. This approach has demonstrated how the intersection between advanced technology and innovative data analysis techniques can significantly contribute to developing increasingly effective and proactive cyber defence mechanisms.

3. Challenges and Opportunities in the Coordination of Cyber Operations

Effective coordination between different operational units emerges as a cornerstone for mission success in modern cyber operations. The intrinsic complexity of the cyber domain, characterized by rapid technological evolutions and a highly dynamic operational environment, requires unprecedented synergy and flexibility between specialized units. In particular, the interaction between the Offensive Cyber Unit (OCU) and the Command and Control Headquarters (CHQ) represents a critical factor that can significantly influence the effectiveness of operations conducted in cyberspace. Recognizing this reality, my research focuses on exploring the coordination dynamics between these two crucial entities to identify areas of strength and potential gaps that could be addressed to improve overall operational performance.

The survey conducted during Crossed Swords 2023 aimed to offer a detailed overview of how the coordination between OCU and CHQ is perceived by those directly involved, what challenges are faced and what strategies can be implemented to overcome them. Through a methodical and structured approach, the aim is to collect valuable data that can illuminate internal dynamics and facilitate a constructive dialogue on optimizing synergies between these operational units. This introduction lays the foundation for an in-depth understanding of the methodology adopted in the survey, outlining the path taken to address these crucial questions and contribute to the body of knowledge in cybersecurity and cyber operations.

In the planning and execution phase of the survey conducted during the Crossed Swords 2023 exercise, my investigation focused on examining the internal dynamics and collaboration

between the Offensive Cyber Unit (OCU) and the Cyber Headquarters (CHQ). The intent was to identify and understand the challenges and opportunities to improve coordination between these two crucial entities in cyber operations.

The research process began with the precise and accurate definition of the survey objectives, a fundamental action to ensure the effectiveness and relevance of the data collected. This initial phase was crucial to align each question of the questionnaire with the central themes of my investigation: to explore in depth the issue of the lack of coordination between the Offensive Cyber Unit (OCU) and the Cyber Headquarters (CHQ), with particular attention to the resulting operational and tactical challenges. The commitment to clearly delineating objectives facilitated the creation of a structured framework for the questionnaire, ensuring that each question was aimed at eliciting Information directly relevant to my research interests.

In selecting my sample, particular attention has been paid to the unique composition of my interest group, namely the active members within the OCU and the CHQ. Recognizing the importance of specificity and relevance of perspectives in this highly specialized context, a selective and exclusive approach was taken to defining the sample. This strategy aimed to ensure that the Information collected reflected the actual experiences and perceptions of those who operate daily at the interface of the coordination dynamics. Through careful selection, a variety of roles and functions within the OCU and CHQ units were included to capture a full range of insights and perspectives. This methodical approach increased the relevance of the data collected and enriched the understanding of the complex interactions that characterize cyber operations, providing a solid basis for subsequent analysis and the generation of informed recommendations.

In the questionnaire design phase, a focus on creating targeted questions has been designed to probe the operational dynamics within the units involved, the problems related to the overlap of objectives, the effectiveness of the strategies implemented and the perception of rigidity in decision-making mechanisms. The objective was twofold: to collect solid and reliable quantitative data and to open a channel towards more prosperous and detailed qualitative insights. To achieve this goal, the questionnaire was structured with a series of well-defined questions, each aimed at exploring specific areas of interest within the operational environment of cyber defense units. This included questions designed to assess the clarity and efficiency of communication and coordination flows between units and identify any points of friction or inefficiencies in the management and implementation of cyber operations.

At the same time, the possibility of conducting semi-structured interviews has been integrated into the approach. This complementary methodology was chosen for its ability to provide a space where participants could freely express their experiences, opinions, and perceptions in a less structured and more open context than the standardized questionnaire.

For this study, interviews were conducted with Red Team members and officers ranging from lieutenant to colonel from 41 countries, including NATO member states and NATO partners.

The interviews were based on a detailed questionnaire designed to evaluate the coordination between the Cyber Headquarter (CHQ) and the Offensive Cyber Unit (OCU) during the Crossed Swords 23 (XS23) exercise. The questions aimed to assess various aspects of communication, command and control efficiency, strategic direction, real-time adaptability, and overall effectiveness of both CHQ and OCU.

Participants provided detailed responses and the key areas explored included:

- Effectiveness of communication between CHQ and OCU.
- Clarity of the command and control chain from CHQ to OCU.
- Efficiency of CHQ in providing strategic direction to OCU.
- Real-time adaptability of OCU to directives from CHQ.
- Challenges faced by OCU in implementing CHQ's strategies.
- Successful joint planning examples between CHQ and OCU.
- Decision-making processes within CHQ and their impact on OCU operations.

The interviews provided the opportunity to probe more deeply into the complexities and nuances of the operational and decision-making dynamics within the OCU and CHQ. This enabled a more detailed and nuanced understanding of the key issues under consideration, such as specific situations where CHQ effectively guided OCU during an operation, and suggestions for improving the command and control process.

Through a holistic approach to questionnaire design and semi-structured interviews, a wide range of data and perspectives were captured. This has not only facilitated a more prosperous and deeper analysis of cyber operations and related challenges but has also positioned my research in an advantageous position to generate meaningful and actionable insights destined to positively influence future operational strategies and practices within the context of cyber operations.

During the crucial data distribution and collection phase, meticulous attention was paid to ensuring the process was characterized by high flexibility and accessibility. These elements were essential to encourage active participation within a highly specialized and numerically limited group, such as the Offensive Cyber Unit (OCU) and the Command and Control Headquarters (CHQ). To achieve this goal, several strategies were implemented, including scheduling interviews at times convenient for participants and utilizing easily accessible digital platforms for questionnaire administration. This approach allowed me to overcome logistical and temporal obstacles, thus ensuring extensive and significant data collection despite the natural size limitation of my study sample.

Subsequently, the analysis of the data collected became a precious opportunity to explore the dynamics within and between the units in depth. Adopting sophisticated software tools for qualitative analysis has been fundamental in this process. These tools facilitated a methodical decoding of the responses obtained, allowing us to identify emerging patterns and trends precisely. This analytical process made it possible to identify recurring themes and significant divergences in the experiences and perceptions of the participants, offering critical food for thought on the coordination and communication mechanisms between the OCU and the CHQ. Furthermore, the use of advanced data analysis techniques allowed the responses to be broken down into thematic categories, thus facilitating the identification of correlations, discrepancies and unique points of view between the members of the two units. This approach has broadened my understanding of shared operational challenges and specific barriers to effective collaboration, while revealing the existence of potentially innovative perspectives and solutions proposed by the participants.

Through this detailed data collection and analysis process, A complex and multifaceted narrative of internal relationships and operational effectiveness within the cyber environment was constructed. The results emerging from this investigation have enriched the academic literature on cybersecurity and provided concrete foundations for developing improvement strategies to optimize the coordination and efficiency of cyber operations between the OCU and the CHQ.

The final phase of my study saw particular attention paid to the compilation and analysis of the results, culminating in drafting a comprehensive report. This crucial document served as a summary of my findings, highlighting not only areas of excellence but also those needing improvement. My commitment to providing recommendations based on solid evidence collected during the survey was significant in providing stakeholders with information tools capable of positively influencing future strategies for more effective coordination of cyber operations.

This detailed report marked a turning point, acting as a catalyst for dialogue between the different operational units and decision-makers. The proposed recommendations have been designed to be pragmatic and actionable to facilitate continuous improvement in operational practices and manage collaboration between the Offensive Cyber Unit (OCU) and Command and Control Headquarters (CHQ). The objective of this initiative was twofold: on the one hand, The goal was to strengthen existing operational synergies, while on the other hand, to promote an increase in the overall effectiveness of cyber operations within the scope of Crossed Swords 2023.

Adopting and implementing the recommendations that emerged from my analysis represented critical steps in my improvement process. Through constructive dialogue and collaborative engagement between stakeholders, innovative solutions were developed in response to the specific needs that emerged. This collaborative approach has allowed us to refine operational tactics and strategies and favoured creating a more integrated and high-performance environment for cyber operations. The implementation of this study and the application of its conclusions have contributed significantly to the evolution of my understanding and methodologies. Identified and addressed operational challenges have laid the foundation for future cyber operations, which will be characterized by increased integration and effectiveness. Ultimately, the path undertaken has enriched my approach to cyber operations, offering valuable lessons learned that will continue to influence my operational strategies and practices in future contexts positively.

CHAPTER IV

EXPLORING THE DEGREE OF SINO-RUSSIAN COORDINATION IN CYBERSPACE DURING THE UKRAINE WAR

1. Introduction

In a significant turn of events, the British newspaper The Times reported in April 2022 that on the eve of Russia's invasion of Ukraine (February 23), China-based hackers launched a massive cyberattack against Russia's military and nuclear facilities. This attack, which targeted more than 600 websites belonging to the Ukrainian Defence Ministry and other institutions, clearly indicated the escalating cyber warfare in the region[174]. Ukrainian intelligence services said they detected hacker attacks that had characteristics of the People's Liberation Army's cyber warfare unit[175][176].

The analysis underscores the intricate nature of coordinating APTs with shared objectives. The potential cooperation between Russian and Chinese APTs in Ukraine would necessitate the transfer of knowledge, resources, and a level of sophistication that would be exceedingly challenging, even if Beijing and Moscow's strategic goals align more in the medium or long term. This suggests that offensive cyber operations' inherent characteristics inherently limit cyberspace coordination.

Several researchers and cybersecurity firms have also reported Chinese cyber activity. Several researchers and cybersecurity firms have also reported Chinese cyber activity[177] raising questions about whether China had anticipated Russia's plan in Ukraine and whether Beijing was somehow helping Moscow. This is consistent with China and Russia's willingness to work together in cyberspace. If confirmed, these hypotheses would have significant political and military implications. There is a vast amount of literature on convergence[178][179], or divergence[180] between NATO's two strategic competitors and potential adversaries.

---

[174] This Article has been published by STAST Conference in 2023.
M. Tucker, "China accused of hacking Ukraine days before Russian invasion," The Times, Mar. 2023. [Online]. Available: https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf

[175] K. Tanmay, "DECODED - Did China Help Moscow Hack Ukraine & Share Critical Intelligence Before The Russian Invasion?" Apr.2022. [Online]. Available: https://eurasiantimes.com/decoded-did-china-help-moscow-hack-ukraine-russian-invasion/

[176] I. Kagubare, "Ukraine intelligence accuses China of hacking days before invasion: report," Apr. 2022. [Online]. Available: https://thehill.com/policy/cybersecurity/3256792-ukraine-intelligence-accuses-china-of-hacking-days-before-invasion-report/

[177] G. Corera, "Mystery of alleged Chinese hack on eve of Ukraine invasion," Apr. 2022. [Online]. Available: https://www.bbc.com/news/technology-60983346

[178] R. K. Perizat, "China and Russia: between partnership and competition," Jan. 2022, section: EDITORIALS. [Online]. Available: https://theasiatoday.org/editorials/china-and-russia-between-partnership-and-competition/

[179] P. Stronski and N. Ng, "Cooperation and Competition: Russia and China in Central Asia, the Russian Far East, and the Arctic.": https://carnegieendowment.org/2018/02/28/cooperation-and-competition-russia-and-china-in-central-asia-russian-far-east-and-arctic-pub-75673

[180] J. Srinivas, "Russia and China in BRICS: Convergences and Divergences," in Future of the BRICS and the Role of Russia and China, J. Srinivas, Ed. Singapore: Springer Nature, 2022, pp. 147–192. [Online]. Available: https://doi.org/10.1007/978-981-19-1115-6 5

Their possible cooperation in cyberspace could strengthen the convergence thesis. From a cyber warfare perspective, potential coordination between Chinese cyberattacks and Russian cyber and conventional operations would require fundamentally reevaluating Western strategy and posture in cyberspace[181]. Their cooperation in cyberspace could strengthen the convergence thesis. From a cyber warfare perspective, potential coordination between Chinese cyberattacks and Russian cyber and conventional operations would require fundamentally reevaluating Western strategy and posture in cyberspace[182].

Given the strategic willingness of China and Russia to collaborate in cyberspace and the potential Chinese support in Ukraine, the research question at the heart of this chapter is of utmost importance: while at a strategic level higher, China and Russia are trying to cooperate in the cyber domain, are their advanced persistent threat affiliates coordinated and working towards shared goals?

This investigation into the coordination of Chinese and Russian cyber operations, particularly the links between their military Advanced Persistent Threat (APT) activities, could have profound political and military implications[183][184].

In this chapter, I have two main objectives:

- First, using more data and open-access sources, I want to investigate whether there was any coordination between Russian and Chinese APT groups following the Russian invasion of Ukraine (February–December 2022). In particular, I focus on three Chinese APT: Mustang Panda, Scarab and Judgment Panda. The analysis suggests a more nuanced picture than the public debate. Although they sometimes share the same military objectives, China and Russia have very different and sometimes divergent goals in cyberspace. Thus, this chapter aims to provide an empirical contribution to the literature on offensive cyber operations.
- Second, I focus on the implications of the presence or absence of Russian-Chinese coordination for my understanding of nationally coordinated efforts in cyberspace and, more generally, the role of coordinated or uncoordinated offensive cyber operations.

This chapter represents an offensive case study in my thesis and serves to answer the two key questions of this thesis:

- How can the lack of coordination in cyberspace be conceptualised to understand better how cyberattacks affect national and international security?
- How do these interactions affect the effectiveness of both offensive and defensive operations?

These questions aim to clarify how the lack of coordination can provide a deeper understanding of the dynamics of cyberspace and its strategic implications.

---

[181] R. J. Harknett and M. Smeets, "Cyber campaigns and strategic outcomes," Journal of Strategic Studies, vol. 45,no. 4, pp. 534–567, Jun. 2022, publisher: Routledge eprint: https://doi.org/10.1080/01402390.2020.1732354.

[182] L. Kello, "Cyber Disorders: Rivalry and Conflict in a Global Information Age." https://www.belfercenter.org/publication/cyber-disorders-rivalry-and-conflict-global-information-age

[183] M. D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," no. 42, 2013. https://carnegieendowment.org/email/South Asia/img/CLM42MSnew.pdf

[184] J. R. Lindsay, T. M. Cheung, and D. S. Reveron, China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. Oxford University Press, May 2015.

This chapter is useful because it allows us to explore the specific cases of Chinese and Russian APT groups in detail, providing an empirical analysis of their activities during significant conflict. By analysing groups such as Mustang Panda, Scarab and Judgment Panda, and observing their operations in the context of the Russian invasion of Ukraine, we can gain a clearer insight into the tactics, techniques and procedures used by these actors.
Furthermore, studying the coordination (or lack thereof) between these entities provides valuable insights into the dynamics of collaboration and rivalry in cyberspace. This is crucial to understanding how offensive cyber operations can be conducted more effectively and what the main challenges and limitations faced by nations in integrating their cyber capabilities are. Although Russia and China may sometimes share common military objectives, exploring the differences between their cyber objectives highlights how these nations pursue different and often divergent strategies. This understanding is crucial to developing targeted policy and strategic responses and improving global cybersecurity.
This chapter significantly contributes to the existing literature on offensive cyber operations, offering new empirical and theoretical perspectives. It provides practical insights into improving the coordination and effectiveness of cyber operations, both offensive and defensive, thereby enhancing our understanding and management of cyber threats globally.

2. China's Cyber Espionage: Strategic Operations and Technical Maneuvers

2.1 China's Cyber Warfare Strategy: Espionage, Influence, and Geopolitical Power

The People's Republic of China has significantly advanced its capabilities in cyberspace, emerging as a global powerhouse in cyber operations. The Chinese government, employing specialized units like the People's Liberation Army Unit 61398, has orchestrated large-scale cyber-espionage activities to gather sensitive data from foreign governments, companies, and international organizations. Executed with sophisticated tactical techniques and procedures, these operations are designed to infiltrate undetected computer systems. China's strategy in the cyberspace domain is best understood as 'cyber warfare', a concept that places cyberspace at the heart of strategic and national security operations, akin to traditional domains such as land, sea, air, and space. This vision is grounded in the recognition that, in the contemporary era, dominance in this fifth domain can shape the outcome of geopolitical confrontations and conflicts[185].
China's cyber warfare strategy encompasses a range of objectives and methodologies. At its core is intelligence collection: cyberespionage operations enable China to gain vital information about other nations' policies, defensive capabilities, and technological advancements. This knowledge empowers Beijing to prepare and respond more effectively to international developments with a clear understanding of other countries' intentions and capabilities. Simultaneously, cyber espionage serves economic ends. The theft of trade secrets and intellectual property enables Chinese companies to gain a competitive edge in the global market by accelerating domestic technological development and reducing reliance on foreign

[185] Courtney, W., and P. A. Wilson. "If Russia Invaded Ukraine." December 2021. https://www.rand.org/blog/2021/12/if-russia-invaded-ukraine.

innovations. This aspect is particularly significant for China, which aspires to achieve autonomy and leadership in the future's key technologies[186].

A third pillar of China's cyber warfare is the enhancement of military and technological capabilities. Through cyber espionage, China aims to deeply understand the strengths and vulnerabilities of potential adversaries, developing strategies and technologies to neutralize them. The objective is to ensure a strong position in any confrontation scenario, exploiting the vulnerabilities discovered for strategic and operational purposes[187]. However, China's cyber warfare extends beyond data collection. It also includes offensive operations capable of targeting other states' critical infrastructures, disseminating disinformation, and shaping global public opinion. These actions, part of the broader 'hybrid war' strategy, illustrate how cyberspace has evolved into a battlefield where victories are measured in territorial control and the ability to influence, destabilize, and manipulate[188].

In this context, the importance of defence should be remembered. China invests heavily in protecting its cyber infrastructure through developing advanced security technologies, training cyber defence specialists, and implementing laws that strengthen its networks' resilience. The goal is to create a secure and controlled digital environment in which threats can be effectively identified and neutralized[189].

To assert its supremacy in cyberspace, the People's Republic of China has taken significant steps, channelling considerable resources toward developing an arsenal of offensive and defensive cyber tools. A vital element of this strategy has been the formation of specialized cyber military units, reflecting the growing importance Beijing has placed on cyber warfare as a core component of its national defence and security doctrine. However, this intense activity in cyberspace has not gone unnoticed on the international scene, raising concerns and mistrust among other states. These concerns focus on China's orchestrated cyber-espionage operations and cyber-influence campaigns, which have raised questions about data security and the integrity of the world's information infrastructure[190].

Beijing's triumph in these cyber operations is not a stroke of luck but a testament to its meticulous long-term strategic planning and massive investments in cybersecurity research and development. This combination has propelled China to the forefront of creating sophisticated tools and techniques for cyberspace warfare, a feat that commands respect and admiration[191].

A crucial and alarming aspect of the Chinese cyber strategy is using hacker groups, which operate under state auspices and in unofficial settings. These groups, commonly classified as

---

[186] Keir, G. "Putin Does Not Need to Invade Ukraine to Get His Way." December 2021. https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way.

[187] Carly, P. "US, UK and EU Blame Russia for 'Unacceptable' Viasat Cyberattack." TechCrunch. https://techcrunch.com/2022/05/10/russia-viasat-cyberattack/.

[188] Microsoft. "An Overview of Russia's Cyberattack Activity in Ukraine." Tech. Rep., 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[189] Bateman, J. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications."https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

[190] Vicic, J., and R. N. Metha. "Why Russian Cyber Dogs Have Mostly Failed to Bark." March 2022. https://warontherocks.com/2022/03/why-cyber-dogs-have-mostly-failed-to-bark/.

[191] Scroxton, A. "Mandiant Analysts: Russia-backed APTs Likely to Ramp up Attacks." Computer Weekly. https://www.computerweekly.com/news/252512299/Mandiant-analysts-Russia-backed-APTs-likely-to-ramp-up-attacks.

Advanced Persistent Threats (APT), specialize in long-lasting cyber campaigns. Their operations are marked by a complexity and sophistication that makes them extremely difficult to identify and counter. APTs can silently infiltrate the computer systems of government bodies, companies and international organizations, remaining hidden for years and extracting large quantities of data without arousing suspicion[192].
Beijing's strategy is built on the crucial understanding that cyberspace dominance is fundamental to ensuring a strategic advantage in the global geopolitical context. Through these advanced techniques and the creation of cyber military units, China aims to protect its national interests, promote its policies and, where necessary, compromise the security and stability of adversaries. This comprehensive approach to cyberspace underscores how cyber warfare has become a central pillar of China's security and defence strategy, capable of influencing the international balance of power[193].

2.1 China's State-Backed Hackers

As global cyber operations become increasingly sophisticated, nation-state-affiliated hacker groups play an increasingly central role in cybersecurity and cyberespionage strategies. Among these are China-associated threat actors such as Mustang Panda, Scatab, and Judgment Panda, which have gained notoriety for their targeted and technically advanced campaigns. These groups use a wide range of techniques, tools, and procedures (TTPs) to infiltrate networks of governmental and non-governmental organisations with the intent of collecting sensitive information that may prove crucial to China's national interests.
The ability of these groups to modify their geographic and sectoral objectives in response to changes in the global geopolitical landscape is a clear indicator of their versatility and the support they presumably receive from state entities. Furthermore, operational flexibility is further demonstrated by China's increased cyber espionage activity, observed in conjunction with major geopolitical events, such as the build-up of Russian troops on the border with Ukraine[194].

[192] Miller, M. "Russian Invasion of Ukraine Could Redefine Cyber Warfare." January 2022. https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051.
[193] Wei, Y. "China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty." Section: Feature, June 2016. https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/
[194] Gilli, A., and M. Gilli. "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage." International Security 43, no. 3 (February 2019): 141–189.

FIGURE 1. Chinese APT activities targeting Russia and Ukraine, as reported by Mandiant.

2.2 Mustang Panda

Mustang Panda, also known as "RedDelta" or "Bronze President"[195], is a China-linked threat actor that has traditionally focused on targeting non-governmental organizations in Asian countries. However, in a significant shift, in July 2021, Slovakian cybersecurity company ESET detected malicious activity related to Mustang Panda's targeting of European organizations[196]. This shift was also confirmed by Google's Threat Analysis Group (TAG), which stated that "targeting European organizations represents a change from Mustang Panda's regularly observed Southeast Asian targeting"[197]. Shortly before and shortly after the Russian invasion of Ukraine, Proofpoint, a California-based security vendor, noticed an increase in activity from a group known as Red Delta. This group was previously linked to Mustang Panda, and some researchers believed it was part of the same group[198]. In its report, Proofpoint points out that "the operational tempo of these campaigns, particularly those against European governments, has increased significantly since Russian troops began massing on the border with Ukraine" [199]. The malicious file used for the phishing attack was titled: "Situation at EU

[195] Mustang Panda, TA416, RedDelta, BRONZE PRESIDENT, Group G0129." MITRE ATT&CK®. https://attack.mitre.org/groups/G0129/

[196] Côté Cyr, A. "Mustang Panda's Hodur: Old Tricks, New Korplug Variant." Section: ESET Research, March 2022. https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/.

[197] Huntley, S. "An Update on the Threat Landscape." March 2022. https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/.

[198] Chinese State-Sponsored Group 'RedDelta' Targets the Vatican and Catholic Organizations." Recorded Future, 2020. https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf.

[199] Raggi, M. "The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates." Proofpoint US, March 2022. https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european.

borders with Ukraine.zip", suggesting that Google and Proofpoint had been observed engaging in the same activity.

My analysis of Mustang Panda's Tactics, Techniques, and Procedures (TTPs) reveals a wide range of tools and techniques used by this threat actor. Like other Advanced Persistent Threats (APTs), Mustang Panda employs essential solutions for hosting files and sending emails, such as Dropbox and SMTP2GO. However, they also demonstrate high adaptability and sophistication, using various methods for initial access, execution of malicious code, persistence, privilege escalation, and defence evasion. For instance, they utilize WMI, PowerShell, Command Shell, Visual Basic, Word document macros, and Windows Scheduled Tasks for code execution. They also employ DLL sideloading, WMI exploitation, and scheduled tasks for persistence and privilege escalation. Their defence evasion techniques range from simple file hiding to more advanced methods like file renaming and double extensions. This variety of tools and techniques underscores the adaptability and sophistication of Mustang Panda.

The latter featured more complex tools such as InstallUtils and MSHTA in script launch and execution phases. Credentials are accessed by extracting hashes from volume clones of NTDS.dit files, a database at the heart of Active Directory containing information about users, entities, and groups. Discovery of tactical objectives is typically achieved by searching documents using standard searches. Network configuration and layouts are found through common CLI commands such as ipconfig and netstat -ano. The same goes for process discovery, which is usually done by task list commands. One of the most peculiar techniques used by the Mustang Panda is that removable media, such as USB connections, are used to achieve lateral movement. Data collection is usually done with batch scripts; the data is then RC4 encrypted and stored password-protected. RC4 encryption is also used in C2 communication via standard HTTP methods, such as POST. Mustang Panda is also known to be able to exfiltrate data from air gap networks via removable media, such as USB drives[200].

The sophisticated TTPs used by Mustang Panda made it extremely unlikely that disparate groups such as Chinese and Russian hackers could operate in a coordinated manner. The lack of coordination between the Russian and Chinese groups also seems to be confirmed by Mandiant data, according to which the Mustang Panda was targeting Eastern European countries, including Ukraine, well before the Russian invasion. Furthermore, no significant links or coordination activities have been identified between this threat actor, which Mandiant identifies as (uncategorized) UNC3716 and the other Russian APTs on the Ukrainian front.

Most importantly, while Mustang Panda targeted Eastern Europe and Ukraine, I observed the Chinese group's activities against Russian targets. The malicious executable carrying PlugX was included in a report on the Blagoveshchensk Border Detachment, a city of strategic importance to Russia, located on the Sino-Russian border, called "Blagoveshchensk - Blagoveshchensk Border Detachment[.] Exe". The file name was chosen to target military officers and personnel familiar with the region. That executable, which appeared to be a legitimate document using a PDF icon, distributed the PlugX malware when opened.

[200] Bienstock, D., M. Derr, J. Madeley, T. McLellan, and C. Gardner. "UNC3524: Eye Spy on Your Email." https://www.mandiant.com/resources/blog/unc3524-eye-spy-email.

Mustang Panda's goal appears to be to exploit the war between Ukraine and Russia to obtain both sides' sensitive economic and military information. The most common file types exfiltrated by Mustang Panda in attacks against Russia are Microsoft Office documents (.docx, .xlsx, .pptx, etc.), PDF documents, and plain text files. Other exfiltrated files include audiovisual data in various forms, including audio recordings (.mp3) and images (.jpg, .png, etc.) or drawings. Emails, including entire conversations, are also exfiltrated. This APT also tries to collect data from browser profiles of various web browsers such as Chrome, Firefox, Opera and others. Sensitive data is collected from victims' computers, and, in most cases, these are computers used by the government, state administration, police and army.

2.3 Scarab

FIGURE 2: Chinese APT Scarab targeting Russia, Ukraine and US as reported by SentinelOne

SentinelOne, an American security firm, has identified a Scarab hacker group, allegedly linked to the Chinese government, as notably active before and after the Russian invasion of Ukraine. This timing underscores the group's strategic approach and the potential implications for cybersecurity. SentinelOne's analysis aligns with alert no. 4244, issued by the Ukrainian Computer Emergency Response Team (CERT-UA) in mid-March 2022, unveiled indicators of a threat actor named UAC-0026, which CERT-UA associated with the Scarab APT[201]. According to SentinelOne, the Scarab attack on Ukraine is a significant development, representing the first publicly reported attack against Ukraine by a non-Russian [Advanced Persistent Threat]. This underscores the evolving nature of cyber threats and the need for constant vigilance. The email used in the attack may have been created on a computer using the Chinese language, as suggested by Tom Hegel, the company's senior cyber threat researcher[202]. As of November 2022, more public, documented information needs to be

[201] Hegel, T. "Chinese Threat Actor Scarab Targeting Ukraine." March 2022. https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/.
[202] Teraoka, A. "Chinese Hackers Launch Cyberattacks Against Ukraine Amid War."https://asia.nikkei.com/Politics/Ukraine-war/Chinese-hackers-launch-cyberattacks-against-Ukraine-amid-war.

available about Scarab[203]. This makes a complete analysis of all MITRE ATT&CK tactics particularly difficult.

FIGURE 3: Chinese APT Scarab cyberespionage campaign as reported by SentinelOne.

In terms of reconnaissance, this APT is only known for using active and passive intelligence-gathering tools on commodities. There is no documented use of custom tools tailored for this purpose. Regarding asset development, this actor has been observed to have reused numerous loaders, malware, and C2 infrastructure over the years. This reuse of resources has led researchers to confidently attribute the recent attacks in Ukraine, dubbed UAC-0026, to the group known as Scarab. Initial access is primarily gained through phishing and spear-phishing campaigns that use malicious attachments with titles carefully tailored to their targets. For example, in the March 2022 attack against Ukraine, documented by the Ukrainian CERT, a .rar file named "On the preservation of video recordings of criminal actions of the Army of the Russian Federation.rar" was used as a decoy document. Interestingly, the metadata of the latter document reveals that the file was created in a Windows environment with Chinese locale, as the author of the file is the Windows default Chinese “用户” (yo'nghu` - user). This specific attack against Ukraine is also a great example of how this group executes malware and gains persistence. The aforementioned .rar file contains an .exe file with a similar name. Once you run this file, three things happen. First, the user is shown a decoy PDF document, while malware called HeaderTip is executed, and persistence is ensured by adding an autorun key to the registry. In the past, Scarab used two backdoors in succession, the first, a simpler one, called “Scieron”, which installed the more complex one, “Scieron B”, a more advanced backdoor with a rootkit-like component. This advanced backdoor could open shells, manage processes, files and directories, and modify registry entries. At the same time, the rootkit-like component would help hide some of the malware's network activity that occurs over TCP. Scieron could be the predecessor of HeaderTip, as they share many common patterns, for example both

[203] Li, Y. "Scarab Attackers Took Aim at Select Russian Targets Since 2012." https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8bfa7311-fdd9-4f8d-b813-1ab6c9d2c363&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

leverage DLL loading for code execution and defense evasion. As mentioned earlier in the document, Command and Control most often happens via DDNS and partly via common HTTP methods[204].

It is essential to note the ongoing uncertainty around the attribution of Scarab's activity. While public reports have attributed HeaderTip's activity to China-linked actors, Mandiant has yet to make a definitive attribution on the origin of this intrusion, and currently loosely attributes UNC532 to the Chinese actor APT5. This lack of clear attribution underscores the complexity of the cybersecurity landscape and the challenges in identifying and tracking APT groups. Based on targets known since the start of the Ukrainian invasion, and not just those pursued on Ukrainian soil since March 2022, HackerNews assesses with moderate confidence that Scarab will operate to gather militarily sensitive information[205].

2.4 Judgement Panda

Between March and April 2022, Google revealed that it alerted the US government to a phishing attack conducted against Gmail users in Eastern Europe by the Chinese-backed hacking group APT31, also known as “Zirconium” or “Judgment Panda”. This group, active for many years, specializes in intellectual property theft and cyber espionage, often against non-governmental entities and private actors.

Judgment Panda groups use standard tools for both active and passive reconnaissance. Judgment Panda is also known to employ email phishing and spear-phishing techniques widely[206]. Regarding resource development, Zirconium is known for purchasing the domains needed for its operations and using standard file hosting websites to store its malware, such as code management websites like GitHub. Initial access is gained via phishing and spear-phishing emails containing malicious links and web beacons. The Windows command shell and Python scripts are used to execute the code once initial access is gained. The APTs launched by Judgment Panda have a peculiar way of achieving persistence: they create a registry execution key called “Dropbox Update Setup” that executes a malicious Python binary. The binary mentioned above is also sometimes used to achieve privilege escalation. The CVE-2017-0005 exploit is another well-known technique that APT uses to gain unintended additional privileges. The fake Registry Run key can also be considered a blatant defence evasion. At the same time, Judgment Panda also uses other means to evade defences, such as encrypting exploit code and payloads with AES256 (and assuming a decryption key derived from SHA1) and using the msiexec.exe command-line utility to launch Malicious MSI files. Regarding access to credentials, little data is available. The only known documented technique is that this APT can retrieve credentials from browsers such as MSIE and Chrome[207]. Judgment

[204] "CVE - CVE-2017-0005."https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0005.

[205] Ravie, L. "Another Chinese Hacking Group Spotted Targeting Ukraine Amid Russia Invasion." Section: Article. https://thehackernews.com/2022/03/another-chinese-hacking-group-spotted.html.

[206] Kaminska, M., J. Shires, and M. Smeets. "Tallinn Workshop Report," 2022.

[207] Gatlan, S. "Microsoft: State-backed Hackers Are Targeting the 2020 US Elections: https://www.bleepingcomputer.com/news/security/microsoft-state-backed-hackers-are-targeting-the-2020-us-elections/.

Panda´s main detection objectives are related to system time, network settings, proxy server configurations, and system architecture. These are all used later for C2 communication. Most communication within the C2 is JSON-based, encrypted with AES256. Evidence shows they leverage Dropbox APIs for their communication and control activities. The same communication line with Dropbox allows for data exfiltration, a valuable tool to rule them all. There must be publicly documented information on how this APT performs lateral movement. There is little evidence of coordination between Judgment Panda and APTs launched by pro-Russian groups. The Google Threat Analysis Group noted in particular that APT31, while having carried out reconnaissance actions in Eastern Europe and Ukraine, also targeted government and military organizations in Russia. In April 2022, using Yandex.Disk as a C2 server to disguise itself, APT31 allegedly attacked several Russian energy and media companies through a malicious document. Analysis of the malware showed that Judgment Panda was behind the attacks: both campaigns in Eastern Europe and Russia contained identical code fragments to collect information on network adapters and collect data on the infected system; the document matrices had apparent similarities. In both cases, cloud servers were used to control the malware.

Some analysts and experts have noted that Russian cybercriminals have used hacking forums such as "RAMP" and "XSS" to engage their Chinese counterparts in conversations to collaborate on joint cyberattacks. A 2021 Flashpoint report highlighted that the RAMP forum had seen at least 30 new registrations from Chinese users[208]. However, it should be noted that based on previous observations, this may be a disinformation activity. The RAMP forum was created in July 2021 to allow diverse hackers to openly discuss ransomware-related tools after banning ransomware-related topics on several underground forums. Back in October 2021, RAMP administrator "Orange" ("boriselcin"), who also operated the website "Groove" published a post calling for Chinese threat actors to attack the United States. After the post received media attention, "Orange" claimed that the operation was launched only to manipulate the media and researchers.

Mandiant often sees threat actors from different countries collaborating in covert forms. Expanding recruitment to include actors from other regions can undoubtedly improve the group's overall capabilities, as members can share tactics, tools, malware, and methods. However, in the case of Judgment Panda, it is difficult to see coordination between cyber groups affiliated with Russia and China.

3. Conclusions

Although the media and some observers have speculated about the presence of coordination between APTs conducted by pro-China groups and Russian cyber and kinetic operations, my analysis shows no evidence to support this argument.[209]. Through a detailed investigation of

[208] Wadhwani, S. "Russian Darknet Forum RAMP Reemerges With Chinese-speaking Hackers At the Wheel. https://www.spiceworks.com/tech/security/news/russian-darknet-forum-ramp-reemerges-with-chinese-speaking-hackers-at-the-wheel/.

[209] Toulas, B. "Russian Ransomware Gangs Start Collaborating with Chinese Hackers. https://www.bleepingcomputer.com/news/security/russian-ransomware-gangs-start-collaborating-with-chinese-hackers/.

three APTs active in Eastern Europe and allegedly conducted by Chinese hacker groups - Mustang Panda, Scarab, and Judgment Panda - I discovered the technical characteristics of these cyberattacks and their possible links to Russian APTs.In terms of techniques, I found that these APTs mainly use essential tools and various sophisticated techniques to obtain information from their intended targets through reconnaissance, initial access, execution, persistence, privilege escalation, access to credentials, and lateral movement.[210]. These APT groups have rarely been found to develop entirely new bespoke tools. Regarding the connection with Russian groups, I have seen that the behaviors of these APTs aim to target both Ukrainian and Russian political and military objectives and, plausibly, try to exploit the war (and the confusion it is causing) to gather sensitive information on both sides.

This section addresses the research questions of my thesis, serving as an offensive case study. The analysis helps understand how the lack of coordination in cyberspace can be conceptualized to better understand how cyberattacks affect national and international security. Additionally, it explores how these interactions influence the effectiveness of both offensive and defensive operations.

This chapter has significant political-military implications. My analysis strengthens the thesis of structural divergence between China and Russia. The pro-China groups examined have sensitive Russian information among their primary targets. I also highlight the difficulties in coordinating offensive cyber operations. Coordination in cyber operations requires the transfer of knowledge and resources and a high level of sophistication. By their very nature, APT activities require close coordination between the actors conducting them, which is challenging to achieve between hacker communities with different modus operandi and behaviours, forums, payment methods, codes of conduct, and values.[211].

At a technical level, cooperation between APTs also requires sharing preparatory and command and control infrastructures for the operation. This includes domain names of phishing sites, leaked email addresses, and infrastructure that operates remotely to maintain communication with compromised systems within a target network. Preparatory infrastructure covers the tools used to prepare and conduct information operations and includes databases used for target mapping.

Rarely does an attacker dismantle this infrastructure[212] after a (failed) operation, a state or a group of hackers has no incentive to share it with other subjects. Another obstacle to cooperation at the technical level between APTs would be the nightmarish complexity of integrating code and software written by different and heterogeneous groups due to different development methodologies, coding styles, polyglot environments and stringent “need to know requirements”. In summary, therefore, based on the threat groups examined, it looks pretty challenging to achieve, in the cyber domain, the level of coordination between different actors

[210] Austin, G., K. Lin Tay, and M. Sharma. "Great-Power Offensive Cyber Campaigns: Experiments in Strategy." Tech. Rep. https://www.iiss.org/blogs/research-paper/2022/02/great-power-offensive-cyber-campaigns.

[211] DeSombre, W., and D. Byrnes. "Thieves and Geeks: Russian and Chinese Hacking Communities," 2018. https://go.recordedfuture.com/hubfs/reports/cta-2018-1010.pdf.

[212] Hutchins, E. M., M. J. Cloppert, and R. M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," 2011.

that I am accustomed to in other fields, such as that of kinetic military operations, even when countries have shared strategies.

Based on these considerations, this chapter can open exciting avenues of research. From an academic perspective, coordination, as a behavior, in offensive cyber operations should be further studied. Other studies have highlighted difficulties in transferring cyber weapons and commands due to the transitory nature of cyber weapons[213]. From an empirical point of view, my analysis shows that combining technical tools and databases with systematic cross-checking of open-source information can lead to detailed analyses of APTs and a better understanding of offensive cyber operations. This methodological toolkit allows scholars and analysts to gain insights into complex and multifaceted phenomena such as APT's modus operandi and behavior. It also helps public and international organizations such as NATO or the EU, as well as Western countries, to better protect themselves from malicious cyber activities.

[213] Smeets, M. "Cyber Arms Transfer: Meaning, Limits, and Implications." Security Studies 31, no. 1 (January 2022): 65–91. https://doi.org/10.1080/09636412.2022.2041081. Publisher: Routledge.

CHAPTER V

COMPETITION, RIVALRY AND COORDINATION CHALLENGES AMONG RUSSIAN INTELLIGENCE AGENCIES AT OPERATIONAL AND TECHNICAL LEVELS

1. Introduction

According to Damjan Štrucl, Offensive Cyber Operations (OCO) have become a key aspect of contemporary conflicts, but the Russian invasion of Ukraine on February 24, 2022, underscored Russia's extensive cyber capabilities. A widespread assumption was that these offensive cyber operations, particularly involving the distribution of malware, should have a significant impact in the outcome of the war and likely spill over to other countries and organizations, similar to the Stuxnet and NotPetya cases. However, a remarkable empirical conundrum has emerged: the limited effects of these Russian Offensive Cyber Operations (OCOs)[214][215].

These empirical observations introduce a theoretical conundrum: How can coordination be managed or integrated within OCOs? This chapter suggests considering each Russian intelligence agency, especially the GRU, SVR, and FSB[216], unique entities possessing individual strategies, technologies, and protocols. The limited effects of Russian OCOs and the lack of coordination between the various advanced persistent threats (APTs) are mainly due to the lack of more operational and technical coordination between these agencies.

This section addresses the research questions of my thesis, serving as an offensive case study. The analysis helps understand how the lack of coordination in cyberspace can be conceptualized to better understand how cyberattacks affect national and international security. Additionally, it explores how these interactions influence the effectiveness of both offensive and defensive operations.

In support of this claim, I take a two-pronged approach. First, I explore the concept of coordination at the operational and tactical level within intelligence agencies engaged in cyber defence. I then empirically examine this phenomenon in Russia's intelligence infrastructure, shedding light on the interplay of internal competition and political rivalry between agencies and their subsequent influence on state cyber threats[217].

---

[214] This article has been published by ACIG: Melella, Cosimo, Francesco Ferazza and Konstantinos Mersinas. "Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies." *Applied Cybersecurity & Internet Governance* (2024): n. pag.

[215] Štrucl, Damjan. "Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare." CONTEMPORARY MILITARY CHALLENGES/SODOBNI VOJAŠKI IZZIVI 24 (2022): 103 - 123.

[216] GRU (Main Intelligence Directorate) is Russia´s largest foreign intelligence agency, responsible for military intelligence. The SVR (Foreign Intelligence Service) is Russia´s primary civilian foreign intelligence agency, equivalent to the US CIA. Its duties include intelligence and espionage operations outside Russia and the analysis and dissemination of intelligence to the Russian president and government. The FSB (Federal Security Service) is the leading security agency of Russia, similar to the FBI in the United States, and has various tasks, including counter-intelligence, internal and border security, counter-terrorism and surveillance.

[217] Jones, Joseph. "Integrating and Shaping Military Cyber Defence in Operational and Intelligence Planning." Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3) (2022).

This chapter contributes to the ongoing debate on state-sponsored cyber operations by providing a potential explanation for the lack of coordination observed between different hacking groups allegedly linked to Russia. Examining the impact of internal competition and political rivalry within Russia's government and intelligence apparatus offers a unique perspective on the nature and structure of state-affiliated cyber threats.

In some cases, political rivalry can lead to a politicisation of these agencies, where officers or civil servants are chosen based on their political affiliation rather than their qualifications or experience[218]. Such a situation can lead to a deterioration in the quality of the agency's services and less trust in government institutions by the public. Collectively, political rivalry can create significant externalities in the competition between public agencies, creating challenges for leaders and executive officials as they seek to deal with changing priorities while maintaining the integrity and effectiveness of their operations. In recent years, there have been numerous tensions between different intelligence agencies in Russia, especially between the FSB and the GRU. For example, there were reports that the FSB was not satisfied with the GRU's involvement in the 2014 annexation of Crimea, as the FSB considered it a violation of its competence. Similarly, there were reportedly tensions between the FSB and the GRU over handling Sergei Skripal´s poisoning in 2018[219].

The landscape of inter-agency competition, compounded by political rivalries, is full of challenges. This unstable environment can induce uncertainty and instability, hampering technical and operational coordination. To illustrate, tensions have been observed within the Russian intelligence community, particularly between the FSB and the GRU, due to alleged excesses of jurisdiction and operational abuse. This chapter adds to the discussion of state-sponsored cyber operations by providing an explanatory lens for coordination deficiencies observed among hacking groups allegedly linked to Russia[220]. Furthermore, I seek to answer two central research questions regarding the degree of integration between cyber defence agencies' technical and tactical levels and the factors contributing to any observed lack of integration: "What is the degree of integration between the technical and tactical levels of intelligence agencies involved in implementing government policies aimed at offence in cyberspace?", and "What are the factors contributing to the lack of integration between the technical and tactical levels in intelligence agencies involved in implementing government policies aimed at defence in cyberspace?"

In doing so, I emphasize the critical role of the technical and tactical levels within intelligence agencies. While the technical level focuses on the skilful use of information management technologies, the operational level primarily addresses the strategic use of information for immediate decision-making. These two layers, while distinct, often need to be closely integrated for an effective response to threat or opportunity. Lack of coordination, therefore, risks creating a schism between strategic objectives and their operational execution, leading to operational inefficiencies[221].

---

[218] Ebinger, Falk, Sylvia Veit and Nadin Fromm. "The partisan–professional dichotomy revisited: Politicisation and decision-making of senior civil servants." Public Administration (2019).

[219] Moses, Joel. "Political Rivalry and Conflict in Putin's Russia." Europe-Asia Studies 69 (2017): 961 - 988; Moses, Joel. "Political Rivalry and Conflict in Putin's Russia." Europe-Asia Studies 69 (2017): 961 - 988.

[220] Taillat, Stéphane and Frédérick Douzet. "Collective security and strategic instability in the digital domain." Contemporary Security Policy 40 (2019): 362 - 367.

[221] Maguire, Laura M.D.. "Managing the hidden costs of coordination." Communications of the ACM 63 (2020): 90 - 96; Martínez, Jon I. and J. Carlos Jarillo. "Coordination Demands of International Strategies." Journal of International Business Studies 22 (1991): 429-444.

My research aims to illuminate these coordination challenges and propose mechanisms for greater integration within state-sponsored cyber operations. Indeed, moving forward, let´s examine the potential implications of a fragmented intelligence community. It erodes the quality of services rendered by agencies. Furthermore, the well-known political competition within public agencies can produce significant externalities[222]. Navigating the shifting currents of rivalries and evolving strategic priorities pose significant challenges for agency leaders and officers, potentially disrupting the effectiveness and integrity of their operations.

Historical tensions within the Russian intelligence community have often led to strategic misalignments. For example, the FSB has reportedly expressed dissatisfaction with the GRU's role in the 2014 annexation of Crimea, considering it a violation of its jurisdiction. Similarly, the handling of Sergei Skripal´s poisoning in 2018 is said to have intensified friction between the agencies[223].

The misalignment between strategic objectives and their execution due to internal fragmentation can lead to operational inefficiencies and potential vulnerabilities, highlighting the need for better integration at a technical and tactical level. I hope to contribute significantly to the broader discourse on offensive state-sponsored cyber operations through this lens.

[222] Alderighi, Marco and Christophe Feder. “Institutional design, political competition and spillovers.” Regional Science and Urban Economics (2020).

[223] Ostrow, Joel M.. “Conflict-Management in Russia's Federal Institutions.” Post-Soviet Affairs 18 (2002): 49 - 70.

2. Russian Cyber (lack of) Coordination

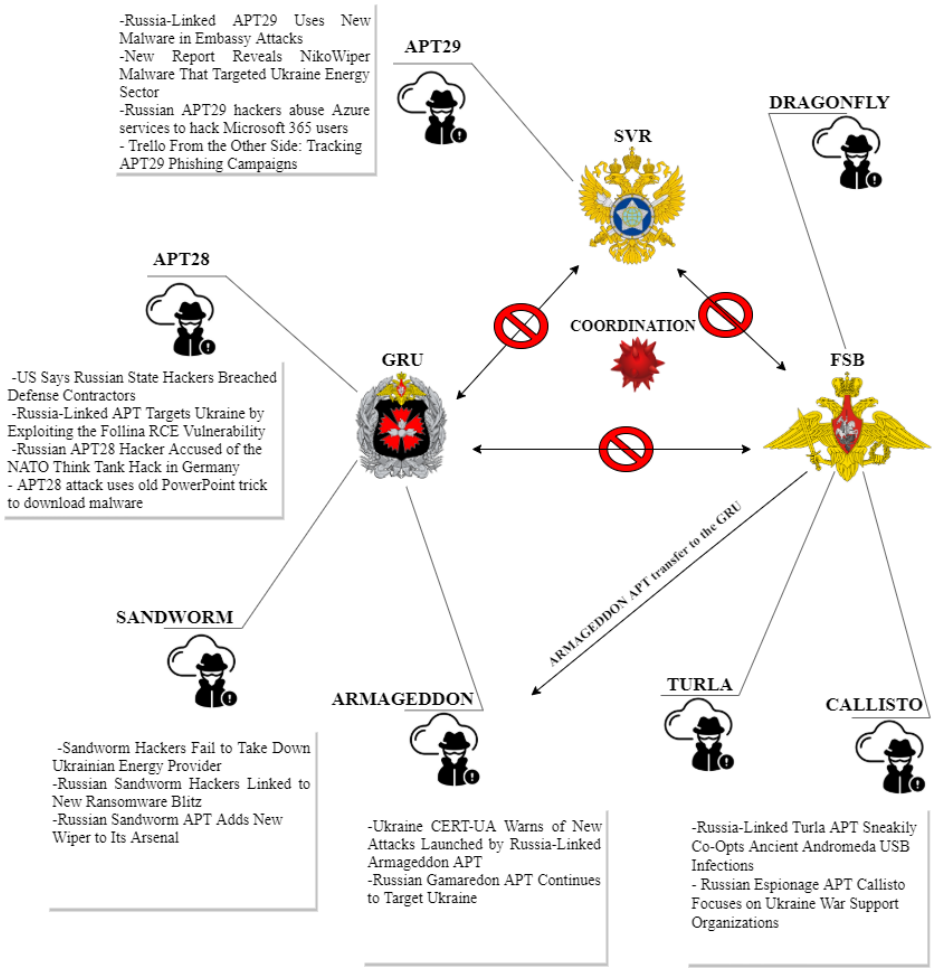


FIGURE 1: Map of Russian Intelligence APTs

2.1 Challenge of Coordination

Coordination between different Advanced Persistent Threats (APTs) in achieving similar or different goals depends on the goals set by their coordinating intelligence agencies. If the intent is to maximise the impact of an operation, it may be appropriate to aim simultaneously at the same goal[224]. Conversely, if the operation is aimed at stealth, cyber-espionage or evasion of detection, it is more appropriate to target different targets simultaneously. Mandiant, which has been monitoring cyber threat intelligence activities in various Ukrainian organisations since the beginning of the conflict, has reported incidents where the detection of one APT's operation led to the discovery of another APT's activities. It occurs due to data collected by Security Information and Event Management (SIEM) systems that identify specific tactics, techniques, and procedures (TTPs) linked to one or more threat actors.
Additionally, coordination between APTs can be challenging as it requires high trust and synergy between sponsoring organisations. This increased interaction can increase the risk of

[224] Ahmad, Atif, Jeb Webb, Kevin C. Desouza and James Boorman. "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack." Comput. Secur. 86 (2019): 402-418.

exposure and compromise, negatively affecting the operation's success. The coordination between APTs and the achievement of similar or different objectives will depend on several factors, including the operation's objectives, the resources available to the sponsoring organisations, and the target infrastructure's security posture[225].

A case in point of this scenario is the Democratic National Committee (DNC) hack in 2016, which involved two separate Russian hacker groups: APT28, affiliated with the GRU, and APT29, linked to the SVR. This cyber breach was notable for its sophistication and volume of sensitive data stolen, including emails and other DNC documents[226]. While APT28 and APT29 are commonly believed to have coordinated the hack, evidence suggests they still needed to synchronise their efforts. For example, APT28 used a spear phishing campaign to access the DNC´s email system, while APT29 used a different method involving a compromised VPN. Furthermore, the tools and TTPs used by the two groups varied, indicating a target-based fit. For example, APT28 reportedly used X-Agent for data exfiltration, while APT29 used a different tool, SeaDaddy. Despite the lack of coordination, APT28 and APT29 successfully executed a cyber-attack on the DNC. However, this lack of coordination may have led to overlooked opportunities or inefficiencies[227].

In recent decades, and before the invasion of Ukraine, Russia has leveraged sophisticated cyber capabilities to conduct global disinformation campaigns, propaganda, espionage and destructive cyber-attacks. Russia oversees numerous units that carry out these operations under various security and intelligence agencies. These Russian security agencies often compete and conduct parallel operations on the same targets, complicating specific attribution assessments. Over the past two decades, Russia has expanded the staffing of its security agencies, thereby developing extensive capabilities to undertake a wide range of cyber operations. No single Russian security or intelligence agency holds sole responsibility for cyber operations. Instead, three agencies share this role: the GRU, the SVR and the FSB[228].

The distribution of responsibilities between the GRU, SVR and FSB can sometimes lead to overlapping or conflicting operations. Each of these agencies maintains its information units and strategic goals, which reflect the broader goals of their parent organisations.

The GRU is traditionally associated with military intelligence and has been implicated in numerous cyber operations to disrupt or destabilise foreign infrastructure. It includes the DNC hack attributed to APT28, which was aligned with the GRU´s more aggressive operational stance.

Meanwhile, the SVR focuses on traditional espionage and foreign intelligence gathering. SVR-related cyber operations, such as those attributed to the APT29, usually reflect this goal, targeting foreign governments, organisations and individuals for intelligence gathering rather than disruption.

---

[225] Khaleefa, Eman J. and Dhahair A. Abdulah. “Concept and difficulties of advanced persistent threats (APT): Survey” (2022).

[226] Shackelford, Scott J., Michael Sulmeyer, Amanda N. Craig, Ben Buchanan and Brian Micic. “From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do about It.” Conflict Studies: Terrorism eJournal (2017).

[227] Simonson, Richard, Joseph Roland Keebler, Mathew Lessmiller, Tyson Richards and John Lee. “Cybersecurity Teamwork: A Review of Current Practices and Suggested Improvements.” Proceedings of the Human Factors and Ergonomics Society Annual Meeting 64 (2020): 451 - 455.

[228] Gioe, David V.. “Cyber operations and useful fools: the approach of Russian hybrid intelligence.” Intelligence and National Security 33 (2018): 954 - 973.

Finally, the FSB, primarily an internal security agency, is also involved in cyber operations. These operations often have a more defensive slant, focusing on internal security, counter-intelligence, and maintaining control over Russia´s information space. However, the FSB has also been associated with offensive cyber operations, particularly those targeting dissidents, activists and other alleged threats to the Putin´s government.
The division of cyber responsibilities among these agencies reflects Russia´s cyber strategy´s complex and multifaceted nature. However, as has been noted, this division can lead to inefficiencies and missed opportunities due to a lack of coordination. For example, the different methods and tools used by APT28 and APT29 in the DNC hack could have allowed for a more thorough or effective operation if there had been more collaboration between the two groups. While there is no indication that the GRU, SVR or FSB will have sole responsibility for these operations, there may be increased efforts to coordinate and streamline activities between these agencies. It could lead to a more unified and powerful Russian cyber threat. However, the inherent challenges of coordinating between large and complex organisations with differing goals and operating cultures should not be underestimated[229].

2.2 Factors impacting coordination

Coordination between the technical and the operational layer in cyberspace, faces several challenges, affecting the efficiency, security and reliability of communication and collaboration. First, different systems, platforms, and protocols can make seamless communication and coordination difficult. Ensuring interoperability between various devices, applications and networks so that they work together requires standardisation, implementing standard protocols and constant updating. Communication delays can hinder real-time coordination, especially in cases where an immediate response is needed. Latency, an additional factor, can be caused by network congestion, physical distance, or routing inefficiencies. Finally, scalability also has a direct effect. As the number of devices, users and systems involved in cyberspace increases, ensuring that the infrastructure of one or more agencies can handle this growth becomes a challenge. Scalability issues can lead to degraded performance or even system failure[230]. Furthermore, for the above reasons, coordination fails between intelligence agencies in cyberspace (for offensive or defensive purposes[231]).
The lack of coordination between the operational and technical layers of these organisations can make it more challenging to carry out attacks with a destructive effect. Without proper coordination between these two layers and the consequent information sharing at the operational and strategic levels, these groups can instead inadvertently undermine each other's efforts, increasing the risk of being discovered. Cultural and historical differences between these agencies hinder effective communication and coordination in cyberspace. Added to this are confidentiality issues: the need to balance security and privacy with the ability to coordinate

[229] Cheravitch, Joe and Bilyana Lilly. "Russia´s Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond." (2020); Zoller, Richard G.. "Russian Cyberspace Strategy and a Proposed United States Response." (2010).
[230] Frederick T. Sheldon, G. Peterson, A. Krings, R. Abercrombie, A. Mili. Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies. April 13, 2009.
[231] Bonnet, Grégory and Catherine Tessier. "Coordination despite constrained communications : a satellite constellation case." (2008).

and share information creates technical limitations. This competition creates disjointed efforts, undermining the efficiency of cyber-attacks.

Intelligence agencies, rather than pursuing large-scale destructive attacks through their units, have preferred to use their APTs mainly for cyber-espionage purposes, sometimes trying to integrate the cybernetic plan with the kinetic one to achieve their operational goals[232].

Cyber operations conducted by different intelligence agencies involve a complex set of technical and operational layers working together. The technical level typically involves using advanced technologies such as malware, remote access tools, and other sophisticated hacking techniques to gain unauthorized access to targeted computer systems and networks. Especially, cyber espionage operations conducted by different intelligence agencies involve a complex set of technical and operational layers working together. The technical level typically involves using advanced technologies such as malware, remote access tools, and other sophisticated hacking techniques to gain unauthorized access to targeted computer systems and networks[233]. The operational level, on the other hand, encompasses the execution of the operations themselves. This level involves identifying and prioritising targets, choosing appropriate methods of attack, and coordinating the actions of operators engaged in the operation. To effectively integrate the technical and operational levels, an intelligence agency typically employs highly trained agents trained to understand cyber espionage's technical and operational aspects. These operators work together in a coordinated way to develop and execute complex attacks on targeted systems and networks[234].

On a technical level, the operators use various tools and techniques to gain unauthorized access to the target's computer systems and networks. It can involve exploiting vulnerabilities in software, using phishing attacks to trick users into giving up their login credentials or using social engineering techniques to gain access to sensitive information. Once access is gained, agents can use various information-gathering tools, such as keylogging software, to capture passwords and other sensitive information or malware to monitor the target's activities and communications[235].

At the operational level, operators use their understanding of target motivations and behaviour to leverage the information gathered to deploy attack tactics. For example, they can use the information to influence the target´s decisions or to gather more information about other targets. Successful cyberespionage operations require high technical and tactical sophistication and a deep understanding of the target's motivations, behaviours, and vulnerabilities. The coordination of the technical and operational layers is essential for the success of these operations and requires a high degree of skill and coordination between the operators involved.

---

[232] Eom, Jung-Ho. “Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace.” Published 2014. Computer Science, Engineering; Bateman, Jon. “Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications.” Carnegie Endowment Paper, December 16, 2022. https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

[233] Iasiello, Emilio. “What is the Role of Cyber Operations in Information Warfare?”, Journal of Strategic Security 14, no. 4 (2021): 72-86.

[234] Rollins, John W. and Clay Wilson. “Terrorist Capabilities for Cyberattack: Overview and Policy Issues.” (2005).

[235] Samojlova, A.“Social Engineering Methods.” SCIENTIFIC DEVELOPMENT TRENDS AND EDUCATION (2019).

2.3 Objectives, skills and culture as coordination challenges

While intra-agency coordination is feasible, despite the difficulties encountered in integrating the technical and operational level, coordination between different intelligence agencies is often more complicated due to various factors, including differences in organisational cultures, competing priorities, lack of integration in the infrastructure and different levels of technical and tactical proficiency[236]. A key challenge is that different intelligence agencies may have different goals and priorities. For example, one agency might focus on gathering information about a particular target, while another might be more interested in disrupting the target's activities or using intelligence to influence decisions[237]. These differing priorities can make it difficult to coordinate operations effectively, as each agency may have a different approach to intelligence collection and use. In some cases, agencies may even have conflicting goals, such as when two agencies are interested in a particular target audience but have different goals and modi operandi on how to approach the task[238]. Another challenge is that different agencies may have different technical and tactical expertise levels. For example, one agency may be more proficient at developing and executing complex cyber-attacks. At the same time, another may have skillsets for gathering information from various sources and deploying psychological operations[239].

2.4 The principal-agent dynamic

Furthermore, there may be a disruption in the principal-agent dynamic between the technical and operational levels between APTs working for different intelligence agencies and the decision-makers who deal with high-level coordination activities. The "principal-agent problem" in economics, as in international relations and security studies[240][241], models the situation where one or more "agents" operate on behalf of the "principal" who has hierarchical dominance over the agents. This relationship involves information asymmetries, since the agents usually have access to more information than the principal, and conflicts of interest, since agents might not operate in accordance with the principal's benefit. Principals cannot

[236] Egnell, Robert. "Civil–military coordination for operational effectiveness: Towards a measured approach." Small Wars & Insurgencies, vol. 24, no. 2, 2013, pp. 237-256. 30 Apr 2013.

[237] Clough, Chris. "Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation." International Journal of Intelligence and CounterIntelligence, vol. 17, no. 4, 2004, pp. 601-613.

[238] Hammond, T. H. "Why Is the Intelligence Community So Difficult to Redesign? Smart Practices, Conflicting Goals, and the Creation of Purpose-Based Organizations." Governance, vol. 20, 2007, pp. 401-422.

[239] Kralovánszky, Kristóf. "Certain Connections between Cyber Operations, Artificial Intelligence and Operational Domains." Military Science Review Archives Vol. 14 No. 4 (2021): Hadtudományi Szemle Hadművészet.
https://orcid.org/0000-0002-5560-3525.

[240] The principal-agent problem is also well-documented in international relations and security studies, where it highlights the complexities in delegating authority in intelligence operations. Scholars such as Robert Jervis have discussed how these dynamics can affect strategic decision-making and operational efficiency. The literature suggests that this problem can lead to significant inefficiencies and misalignments between strategic goals and operational execution, further complicating coordinated efforts in cyberspace.
Jervis, Robert. Perception and Misperception in International Politics. Princeton University Press, 1976.

[241] Byman, Daniel, and Jeremy Shapiro. The Challenge of Defeating the Islamic State: Report of a Workshop on "Fighting ISIS: Measures and Models." Brookings Institution, 2011.

monitor closely the actions of the agents, and agents have motivations which might not serve the principal's goals.
In my case, conflicts can arise by a need for more understanding: actors with technical expertise working within groups may need to understand decision-makers´ broader goals and strategies clearly. On the other hand, decision-makers may need help understanding the technicalities.
Furthermore, this is why decision-makers (at the strategic level) and those who execute these decisions (at the operational level), both essential elements of tactical planning, need to spend more time identifying and prioritizing their goals. The problem of information sharing in this context is aggravating: intelligence agencies (acting as "agents") have access to more information and are often reluctant to share this information with those working at the coordination level (the "principals") or with other engineers from different entities, resulting in a lack of coordination and collaboration. Intelligence agencies may be reluctant to share information for various reasons, such as protecting sources. Disclosure of this information could put these sources or specific operations at risk.
Similarly, agencies may want to protect the specific methods by which they conduct operations and collect information. If these techniques become public knowledge, they may become less effective. These bodies may want to maintain control over the information they collect to ensure it is used appropriately and to have a bargaining edge when influencing political decisions. Additionally, there may be some resistance to information sharing if agencies feel they need more recognition for their work or are concerned that other agencies may use the information to advance their interests at their own expense. These problems can lead to hampering the overall effectiveness of the intelligence system.
Moreover, the principals, that is, the agency-coordinating entities at the higher level, do not necessarily share their broader strategy with the agents, i.e. the agencies. Thus, in lack of the 'broader picture' (another information asymmetry) the aforementioned factors and coordinating challenges can be maintained and perpetuated.
Even in the case of minimisation of information asymmetries, the historical analysis of the agencies under examination reveals an often competitive stance amongst the agencies. Whether this is a deliberately cultivated environment from senior leadership or a phenomenon that has evolved organically amongst the agencies can be debatable. But, in either way, such an environment maintains the aforementioned challenges.
These differences in expertise and access to information can make it difficult to coordinate operations effectively, as agencies may need to fully understand each other's capabilities, limitations, and motivations. This setting can lead to misunderstandings or communication problems, compromising operational success.

2.5 Cultural differences

Different organizational cultures exhibit varying behaviours and approaches; these differences might make it difficult for different intelligence agencies to work together effectively. There are several studies on the effects of cultural characteristics. Empirical research identifies a number of cultural dimensions to describe a national or regional culture. Such dimensions can be equally applied to organizations, and, for my purposes, can indicate how differences in these dimensions can impair coordination between them.

While there are many of these dimensions, proposed by different researchers[242][243], we focus on a selected subset, that is, the ones that are likely to have the highest impact on the coordination between the examined agencies. For my purposes, I consider intelligence agencies as entities which have their own characteristics, that is, they have measurable 'scores' across the following dimensions.

One of the most relevant dimensions, in this sense, is that which describes how trust is gained, for trust is a pivotal aspect of highly-confidential environments. Different organizational cultures might have different ways to attribute trust, and coordinating groups where trust is gained in different ways can be tricky. For example, one group might find higher trust value in personal relations - such as simply having attended the same military academy - while the other group might find higher trust in a long, spotless, career of success.

Another important cultural aspect is that of leadership; some organizations might be more hierarchically structured, with strict and well-defined vertically ordered ranks, while others might have more loose, egalitarian structures which reach decisions via consensus.

The degree of uncertainty avoidance that an organization can tolerate is also a very important dimension to focus on. Some organizations require everything to be normed and deviation from these norms is often a cause of neuroticism, conflict and confusion. Other organizations might be more flexible, caring less about norms and more about practice and actual results.

Last, but not least, another relevant cultural aspect is that of decision-making; some organizations might favour a top-down approach, where individuals make decisions, while others where decision-making is more consensus-based.

In the light of the above, it appears clear that the so-called, human aspects, be it in the form of principal-agent dynamics, or cultural differences, can amplify or diminish coordination challenges between agencies. In the next section, I present the case studies of GRU, SVR, and FSB, along with their indicative corresponding APTs.

3. The Agencies - case studies

3.1 GRU

The Main Directorate of the General Staff of the Armed Forces of the Russian Federation, commonly called the GRU, is Russia's military intelligence agency. The GRU has been implicated in some of the best-known cyber operations, and the public profile of the units underscores a high operational pace. The GRU would also control several research institutes tasked with developing new malware. Over the years, researchers and analysts have noted an apparent willingness on the part of GRU computer units to conduct aggressive espionage operations, sometimes with questionable operational security and secrecy levels[244]. In particular, Unit 26165, to which, APTs such as Fancy Bear and Sandworm, are linked, is one of the two Russian groups identified by the US government as responsible for hacking the DNC during the Clinton-Trump presidential campaign. Western governments and media have linked

[242] Hofstede, Geert. Culture's consequences: International differences in work-related values. Vol. 5. sage, 1984.
[243] Meyer, E. (2014). The culture map: Breaking through the invisible boundaries of global business. Public Affairs.
[244] Giles, Keir. ""Information Troops" - A Russian Cyber Command?" 2011 3rd International Conference on Cyber Conflict (2011): 1-16.

Unit 26165 to numerous offensive operations against public and private sector targets in the United States and Europe[245]. Then there is Unit 74455, which is linked to some of Russia's most brazen and damaging cyber-attacks. Unit 74455 was identified as responsible for the coordinated release of stolen emails and documents during the 2016 US presidential election[246]. Focusing primarily on systems penetration and intelligence gathering, Unit 74455 appears to have a significant offensive cyber capability, including developing the NotPetya malware that hit multiple targets in Ukraine in June 2017, then spread globally and caused significant damage outside Ukraine[247]. Finally, there is Unit 54777, also known as the 72nd Special Service Center, which would be responsible for the GRU psychological operations, including online disinformation campaigns[248].

3.1.1 Sandworm

FIGURE 2: Sandworm APT Targeted Regions in 2022 as reported by Mandiant

While Sandworm is not Kremlin's most prominent hacker group, it is the most visible one since the beginning of the war, and its track record of successful attacks with global impact, most notably the NotPetya malware and several attacks on the Ukraine have made it a severe concern for the Computer Emergency Response Team of Ukraine (CERT-UA). In 2017, the group used Wiper NotPetya malware disguised as ransomware to take down hundreds of networks between Ukrainian government agencies, banks, hospitals and airports, causing an estimated $10 billion in global damage. By presenting destructive attacks as ransomware, Sandworm would be able to cover its tracks and make it more difficult for researchers to attribute the attacks to a state-sponsored group. Since the beginning of the war, Sandworm has relentlessly targeted Ukraine

[245] Ciosek, Ireneusz. "AGGRAVATING UNCERTAINTY – RUSSIAN INFORMATION WARFARE IN THE WEST." Torun International Studies (2020).
[246] Dawson, Andrew J and Martin Innes. "How Russia's Internet Research Agency Built its Disinformation Campaign." The Political Quarterly (2019).
[247] Goel, Sanjay. "Cyberwarfare: connecting the dots in cyber intelligence." Commun. ACM 54 (2011): 132-140.
[248] Pynnöniemi, Katri. "Information-psychological warfare in Russian security strategy." Routledge Handbook of Russian Security (2019).

with various malware strains. Some were highly sophisticated, while others exploited known vulnerabilities that made them easier to detect and prevent from spreading. Researchers believe Sandworm experimented with malware strains to bypass Ukraine's best defences. Most of the attacks were neutralized in the early stages, and the second blackout researchers expected from Sandworm after targeting Ukraine's power supply in 2015, and 2016 never occurred[249].

In April 2022, Sandworm attempted to take down a large energy supplier in Ukraine using a new iteration of the "Industroyer" malware dubbed "Industroyer2" just for ICS systems, as well as a new version of the "CaddyWiper" malware to destroy data of the organizations affected. According to reports, Industroyer2 has been customized to target high-voltage power substations and then use CaddyWiper and other malware for data wiping (e.g. OrcShred, Soloshred and Awfulshred for Linux and Solaris systems) and then wipe any trace of the attack[250] .

It is still unknown exactly how Sandworm compromised the energy supplier's environment or how it moved from the IT network, according to researchers at the computer company ESET, who worked with CERT-UA to secure the network to the ICS environment. ESET strongly believes that Industroyer2 was created using the source code of Industroyer, exploited by Sandworm in 2016 to shut down power in Ukraine. According to CERT-UA and ESET, Sandworm planned to initiate the final phase of this attack by distributing the malware on April 8, 2022, on Azure servers and automated Windows workstations, Linux servers running OrcShred and AwfulShred, high voltage power substations and active network equipment. CERT-UA points out, however, that the implementation of Sandworm's evil plan has so far been prevented thanks to efficient operational detection and incident response planning. ESET also noted in a technical report on the malware used in the attack that "Sandworm allegedly attempted to distribute Industroyer2 malware against high voltage power substations in Ukraine". ESET researchers further report that Industroyer2 is configurable and includes detailed hardcoded configuration, which requires it to be recompiled for each new target. ESET points out, however, that given that the Industroyer malware family has only been deployed twice, with a five-year gap between each release, Sandworm operators still need to develop different versions. The malware sample shows functionality similar to Industroyer´s IEC-104 module, primarily a protocol used in Europe and the Middle East for TCP communications within electrical systems. There are conflicting reports about the impact of this operation. While the full impact remains to be seen, this operation serves as a reminder of Russia´s capabilities to cut off electricity in different parts of Ukraine and its readiness to employ them. This activity poses a higher risk to Ukraine´s electricity transmission and distribution services[251].

Sandworm is also allegedly responsible for a new round of ransomware attacks hitting targets across Ukraine with the new variant of the .NET RansomBoggs ransomware. Also, ESET, in a series of tweets about ransomware attacks, claims to have informed CERT-UA of a variant of RansomBoggs that it spotted as the ransomware targeted several local organizations. Reports indicate that the exploited .NET malware is new and distributed similarly to previous

[249] Egloff, Florian J. and Max Smeets. "Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers." Journal of Cyber Policy (2020).

[250] Greenberg, Andy. "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine." Wired, April 12, 2022.
https://www.wired.com/story/sandworm-industroyer-attack-ukraine/

[251] Scroxton, Alex. "Sandworm rolls out Industroyer2 malware against Ukraine." ComputerWeekly.com. April 12, 2022

campaigns linked to the GRU. The ransom note (SullivanDecryptsYourFiles[.]txt) shows the authors impersonating James P. Sullivan, one of the main characters in the Pixar film Mosters&Co. The executable file is also called Sullivan[.]exe. There are similarities to previous Sandworm attacks: A PowerShell script used to distribute .NET ransomware from the domain controller is nearly identical to the one seen last April during the Industroyer2 attacks against the energy sector, ESET researchers explain. The PowerShell script used, which CERT-UA dubbed "PowerGap", was also used to distribute the "CaddyWiper" malware alongside Industroyer2 using the "ArguePatch" loader[252].
ESET also says the operation resembles a ransomware campaign conducted in October 2022 that targeted Ukrainian and Polish logistics companies with the "Prestige" variant. The ransomware's activity targeting Ukrainian organizations named RansomBoggs has not been directly observed. However, the PowerShell script used to distribute the .NET ransomware known as POWERGAP is tracked. This script can enumerate Group Policy Objects using the Active Directory service interface, in line with other recent activity involving NEARMISS, CADDYWIPER, and JUNKMAIL, all delivered via GPO. In particular, the activity that exploits of these tools together with POWERGAP is attributed - at the time of writing - to APT28 too, which, like Sandworm, would be under the control of the GRU[253].

3.1.2 Fancy Bear

The cyberespionage activity of Fancy Bear, also known as APT28, Strontium or Sofacy, has mainly targeted entities in the United States, Europe and the countries of the former Soviet Union, including governments and armed forces, the media, dissidents at the present Russian government. In recent years, Russia appears to have been usingd APT28 increasingly to conduct intelligence operations commensurate with broader strategic military doctrine. APT28 uses the same pattern to hit its victims: after compromising a victim organisation, APT28 steals sensitive data, which will then be leaked for other political narratives aligned with Russian interests[254]. These have included the conflict in Syria, NATO-Ukraine relations, the European Union refugee and migrant crisis, and the 2016 US presidential election[255].
Since 2014, APT28´s online activity has likely supported intelligence operations designed to influence the domestic politics of foreign nations. These operations have involved taking down and defacing websites, false flag operations using fake hacktivists, and data theft later publicly disclosed online. APT28 is also responsible for the attack on the DNC and other entities related to the 2016 US presidential election cycle. These breaches involved the theft of internal data, primarily emails, which were later strategically leaked through multiple forums and

[252] Antoniuk, Daryna. "Sandworm hacking group linked to new ransomware deployed in Ukraine." The Record. November 29, 2022.
https://therecord.media/sandworm-hacking-group-linked-to-new-ransomware-deployed-in-ukraine
[253] Molina, Ricardo Misael Ayala, Sadegh Torabi, Khaled Sarieddine, Elias Bou-Harb, Nizar Bouguila and Chadi M. Assi. "On Ransomware Family Attribution Using Pre-Attack Paranoia Activities." IEEE Transactions on Network and Service Management 19 (2022): 19-36.
[254] Lemay, Antoine, Joan Calvet, François Menet and José M. Fernandez. "Survey of publicly available reports on advanced persistent threat actors." Comput. Secur. 72 (2018): 26-59.
[255] Linvill, Darren L., Brandon C. Boatwright, Will J. Grant and Patrick L. Warren. ""THE RUSSIANS ARE HACKING MY BRAIN!" investigating Russia's internet research agency twitter tactics during the 2016 United States presidential campaign." Comput. Hum. Behav. 99 (2019): 292-300.

calculatedly propagated, almost certainly intended to further particular objectives of the Russian government[256].

In a report published on January 7, 2017, the US Office of the Director of National Intelligence (ODNI)[257] described this activity as an "influence campaign". This influence campaign - a combination of network compromises and subsequent data leaks - aligns closely with the Russian military´s publicly stated intentions and capabilities. Influence operations, also often called information operations, have a long history of inclusion in the Russian strategic doctrine and have been intentionally developed, deployed and modernized through the so-called Gerasimov doctrine with the advent of the Internet. APT28 is believed to have played a significant role in the ongoing conflict in Ukraine, mainly through its cyber operations. The group has been linked to several cyber-attacks against the Ukrainian government, including military targets and critical infrastructure, as well as disinformation campaigns designed to influence public opinion in the country[258].

APT28, as early as January 14, 2022, a month before the invasion, reported that the Google Threat Analysis Group (TAG) would have been the proponent of a phishing campaign focused on Ukraine. On March 16, CERT-UA issued an alert highlighting that UAC-0028, the name CERT-UA gave APT28, was phishing UkrNet accounts. On March 4, Microsoft reported that it also noticed that the government network in Vinnytsia, a city in west-central Ukraine, was compromised by APT28 through a vicious spear phishing campaign targeting Ukrainian military and Ukrainian government personnel in the region. On May 3, Fancy Bear was then observed targeting its victims with a new variant of the infostealer malware, distributed via email attachments, while On May 6, CERT-UA issued a new alert on another campaign by 'APT, which allegedly sent malicious emails posing as the CERT-UA, containing an attachment in the form of a password protected RAR archive "UkrScanner.rar" and inside the RAR file, a self-extracting archive (SFX) containing a malware called CredoMap. The data collected by the malware was exfiltrated via HTTP POST requests to *.m.pipedream[.]net hostnames[259].

In particular, the CERT-UA warned that Sandworm, also linked to the Russian government, would collaborate with APT28 in these months of the conflict to target and actively exploit the vulnerability known as "Follina" in Microsoft Windows Support Diagnostic Tool (MSDT) (CVE-2022-30190) in malspam attacks. According to CERT-UA, the malspam messages use subject lines such as "LIST of links to interactive maps" within a malicious Word document (for example, LIST_of_links_in_interactive_maps[.]docx) and have already reached more than 500 recipients. The CERT-UA advisory reads that attackers continue to exploit the CVE-2022-30190 vulnerability and increasingly resort to emails from compromised government-domain emails. Ukrainian government experts have traced this activity to UAC-0113, a threat actor they say with medium confidence is associated with Sandworm. In reality, Mandiant keeps track of the activity reported publicly as UAC-0113 and believes it is UNC3666, an undefined

[256] Mwiki, Henry, Tooska Dargahi, Ali Dehghantanha and Kim-Kwang Raymond Choo. "Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin." Advanced Sciences and Technologies for Security Applications (2019).

[257] The ODNI is a United States government agency created in 2005 to coordinate the 16 American intelligence community agencies.

[258] Dawson, Andrew J and Martin Innes. "How Russia's Internet Research Agency Built its Disinformation Campaign." The Political Quarterly (2019).

[259] Burt, Jeff. "Russia's APT28 targets Ukraine government with bogus Windows updates." The Register, 2 May 2023.

persistent threat which might be associated with APT28, with moderate confidence, and which serves explicitly to carry out everyday coordination activities between the two APTs for attacking the same targets. UNC3666 has likely targeted Ukrainian organizations as early as December 2021[260] .

3.2 SVR

The Foreign Intelligence Service (SVR) is Russia's principal civilian intelligence agency for foreign countries. Its task is to collect information using Human Intelligence (HUMINT), Signal Intelligence (SIGINT) and Cyber Intelligence (CYBINT) methods[261]. Most analysts conclude that SVR operates forcefully, emphasizing secrecy and detection avoidance[262]. Most cyber operations related to the SVR focus on intelligence gathering[263]. The SVR also has high technical expertise, often trying to achieve and maintain persistence within compromised networks. Some computer analysts refer to SVR hackers as Cozy Bear or Turla[264].

3.2.1 Cozy Bear

FIGURE 3: APT29 Targeted Regions in 2022 as reported by Mandiant

Cozy Bear, also known as APT29, CozyDuke, the Dukes or PowerDukes, is a threat actor which has been active much earlier than the Russian-Ukrainian conflict, and is shown to have strong ties with the SVR since 2008. APT29 is also known to have been, together with APT28,

[260] Kumar, Vinay and Shah, Chintan. "Countering Follina Attack (CVE-2022-30190) with Trellix Network Security Platform's Advanced Detection Features." July 19, 2022.

[261] HUMINT (Human Intelligence) is intelligence obtained through human interaction, while SIGINT (Signal Intelligence) refers to intelligence gathered through the interception of signals. CYBINT (Cyber Intelligence) is a sub-category of intelligence involving collecting information from cyberspace for analysis and use in cybersecurity.

[262] Staar, Richard Felix and Corliss Anne Tacosa. "Russia's Security Services." Mediterranean Quarterly 15 (2004): 39 - 57.

[263] Thornton-Trump CD, Ian. "RUSSIA: THE CYBER GLOBAL PROTAGONIST." EDPACS 65 (2022): 19 - 26.

[264] Mwiki, Henry, Tooska Dargahi, Ali Dehghantanha and Kim-Kwang Raymond Choo. "Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin." Advanced Sciences and Technologies for Security Applications (2019).

involved in the US Democratic National Committee compromise in 2015. Following the 2016 US presidential election, APT29 was found responsible for spear-phishing campaigns targeting US-based governmental and non-governmental organizations. The phishing emails were sent to defence, national security, international affairs and law enforcement personnel. Some of the emails even pretended to originate from the Clinton Foundation to share election analysis. APT29 has continued to evolve and improve, showcasing new TTPs. Undoubtedly, APT29 has quite a diverse toolkit of custom-developed tools that continually improves as new information is published to the infosec community. This set of tools mainly focuses on gaining permanent access to the victim's machine through backdoors and harvesting information, files, credentials, etc. and their exfiltration. APT29 used a wide range of different programming languages to develop its malware, from pure Assembly (present in some components of the MiniDuke malware) to C++ (CozyDuke) and from C#, Visual Basic .NET (HammerDuke and RegDuke) to Python (SeaDuke). The group's creativity goes even further, as they customise and try different technologies, infection vectors, infrastructures, and more[265].

In summary, APT29 represents a dangerous advanced persistent threat. The group is technically skilled and capable of adapting to the defences of its chosen targets. It often uses techniques and tools that have been identified in previous attacks. The “fingerprints” of its attack activity are becoming well documented and the subject of considerable ongoing scrutiny[266].

Against the backdrop of the war in Ukraine, APT29 is exploiting a “lesser-known” Windows feature called Credential Roaming following a successful phishing attack against a European diplomatic entity. The diplomacy-focused targeting is consistent with Russian strategic priorities and APT29's historic targeting, as reported by Mandiant researcher Thibault Van Geluwe de Berlaere. APT29 is known for its intrusions aimed at gathering information in line with the strategic objectives of the SVR[267].

Some of the collective´s cyber activities are publicly monitored under the Nobelium moniker, a threat cluster responsible for widespread supply chain compromise through SolarWinds software in December 2020. Google said it identified the use of Credential Roaming during the period APT29 was present within the victim´s network in early 2022. Then, “several LDAP queries with atypical properties” were executed against the Active Directory system. Introduced in Windows Server 2003 Service Pack 1 (SP1), Credential Roaming allows users to access their credentials securely on different workstations in a Windows domain. According to Microsoft, Credential Roaming stores user credentials in ms-PKI-DPAPIMasterKeys and ms-PKI-AccountCredentials in the user object. The latter is a multivalued LDAP property containing a sizeable binary object (BLOB) containing data and encrypted credentials. According to the TAG group, one of the LDAP attributes queried by APT29 concerned ms-

[265] Brogi, Guillaume and Valérie Viet Triem Tong. “TerminAPTor: Highlighting Advanced Persistent Threats through Information Flow Tracking.” 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (2016): 1-5.

[266] Hutchins, Eric Michael, Michael J. Cloppert and Rohan M. Amin. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” (2010).

[267] Waters, Rob. "APT29 using Windows Credential Roaming bug to target diplomats. Mandiant finds APT29 increahttps://www.cybercareers.blog/2022/11/apt29-using-windows-credential-roaming-bug-to-target-diplomats/singly targeting NATO and its allies in 2022." Cybercareers, 10 November 2022.

PKI-Credential-Roaming-Tokens, which manages blob storage of encrypted user credential tokens for roaming[268].

3.2.2 Turla

Turla, also known as Snake, Uroburos, Venomous Bear or Waterbug, is the other group that, together with APT29, has links to the SVR, although, it is noteworthy that Microsoft places it within a cluster of known threats linked to the FSB. Since at least 2007, this threat actor has allegedly been responsible for high-profile cyber-attacks and espionage campaigns against government, military and diplomatic entities, research and defence organizations in Ukraine, and several NATO states. Turla is also known for its sophisticated and stealthy techniques, often using custom malware and advanced tools to infiltrate its targets' networks and remain undetected for long periods. Over the years, the collective has been involved in several high-profile cyber espionage campaigns, including campaigns in the United States, Europe and the Middle East[269]. Some of the unique tools and malware used by Turla include: Snake/Uroburos: A highly sophisticated rootkit used for espionage and data exfiltration, capable of infecting both 32-bit and 64-bit systems. It is designed to run on infected systems for extended periods undetected. KopiLuwak: A JavaScript-based malware used in targeted attacks, which can perform various tasks, such as downloading and executing additional payloads, communicating with specific command and control (C2) servers, and data exfiltration. Epic Turla (also known as Wipbot or Tavdig): A modular backdoor that provides remote access to compromised systems and has been used in cyber-espionage campaigns since at least 2012[270].
In a year of conflict, Turla was observed exploiting vulnerabilities in the systems of critical Ukrainian organizations and infrastructures with malware developed over a decade earlier to deliver reconnaissance tools and backdoors to specific targets in Ukraine. Mandiant, who has been monitoring APT´s various operations since the beginning of the war, said that the malware used corresponds to a variant of a malware called ANDROMEDA (aka Gamarue), uploaded to VirusTotal back in 2013. Since the start of the Russian invasion military of Ukraine in February 2022, the collective was allegedly linked to a series of phishing and credential reconnaissance activities targeting various entities in the country. Among the incidents analyzed by Mandiant, in one, an infected USB stick was used in a Ukrainian organization as early as December 2021, leading, once inserted into the systems, to the distribution of ANDROMEDA on different hosts, thanks to the launch of a malicious link (.LNK) masquerading as a folder inside the USB drive[271].

---

[268] Lakshmanan, Ravie. “APT29 Exploited a Windows Feature to Compromise European Diplomatic Entity Network.” The Hacker News, 9 November 2022.
https://thehackernews.com/2022/11/apt29-exploited-windows-feature-to.html

[269] Pereira, Daniel. “The Origin Story of the APT Turla, the Hunt for 'The Snake' Malware, and Current Steps for Prevention.” OODA Loop, June 7, 2023.
https://www.oodaloop.com/archive/2023/06/07/the-origin-story-the-fsbs-turla-the-hunt-for-the-snake-malware-and-current-steps-for-prevention/

[270] Securelist by Kaspersky. “The Epic Turla Operation.” APT REPORTS, 07 August 2014.
https://securelist.com/the-epic-turla-operation/65545/

[271] Gyongyoși, Livia. "Turla Uses Old Malware Infrastructure to Attack Ukrainian Institutions: Andromeda USB Spreading Malware Used for Data Exfiltration." Heimdal Security. January 9, 2023.
https://heimdalsecurity.com/blog/turla-uses-old-malware-attack-ukrainians/

The threat actor then repurposed one of the dormant domains of ANDROMEDA´s defunct C2 infrastructure - re-registering the domain in January 2022 - to profile the victim by launching the KOPILUWAK dropper. Two days later, on September 8, 2022, the attack moved to its final stage with the execution of a .NET-based implant called QUIETCANARY (aka Tunnus), resulting in the exfiltration of all files created after January 1, 2021. Mandiant also allegedly identified a spyware application for Android masquerading as a "Process Manager" service to stealthily steal sensitive information stored on infected devices.

Interestingly, this app — has the package name "com.remote.app" — establishes contact with a remote command and control server, 82.146.35[.]240, which has been identified as infrastructure belonging to Turla. When the application runs, a warning about the permissions granted to the application is displayed. Permissions include screen lock and unlock attempts, global device proxy settings, screen lock password expiration settings, storage encryption settings, and disabling cameras. Once the app has been activated, the malware runs in the background, abusing broad permissions to access device contacts, call logs, track device location, send messages, access external storage, take pictures, and record audio.

The collected information is in JSON format and transmitted to the remote server. Also, unknown at this stage is the exact initial access vector used to distribute the spyware and the intended goals of the campaign. The rogue Android app also attempts to download a legitimate application called Roz Dhan (meaning "daily wealth" in Hindi), which has over 10 million downloads and allows users to earn cash rewards for completing surveys and questionnaires.

In July 2022, however, TAG revealed that Turla would create another malicious Android app, this time, however, to support pro-Ukrainian hacktivists to launch Distributed Denial-of-Service (DDoS) attacks against Russian sites. This activity by Turla dovetails with what has been written so far to support the group's casualty profiling efforts coinciding with the Russo-Ukrainian war and SVR interests, helping the agency gather information of interest to the Russian government[272].

3.3 FSB

The Federal Security Service, or FSB, is Russia's principal internal security agency, responsible for internal security and counter-intelligence. The FSB´s tasks are protecting Russia from foreign cyber operations and monitoring domestic cybercriminal groups, a mission undertaken jointly with Department K of the Ministry of Internal Affairs[273]. In recent years, the FSB has expanded its remit to include foreign intelligence gathering and offensive cyber operations. Today's state-sponsored hacker groups linked to the FSB are Callisto, Energetic Bear, Gamaredon, TeamSpy, Dragonfly, Havex, Crouching Yeti, and Koala. SBU intelligence analysts say the FSB has two primary centres overseeing information security and cyber operations. The first is the 16th Center, which houses most of the FSB's intelligence capabilities. The second is the 18th Center for information security, which oversees operations within national borders, but also conducts operations abroad. Like the GRU, the FSB oversees dedicated training and research institutes, which directly support the agency's offensive

[272] Leonard, Billy. "Continued Cyber Activity in Eastern Europe Observed by Threat Analysis Group." July 19, 2022.
https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/

[273] Turkaeva, Laura. "Federal Security Service in the national security system." (2020).

activities. Most of the operations appear to be reconnaissance or clandestine surveillance[274]. In 2021, Ukrainian intelligence released information and recordings about Crimean-based 18th FSB Center officers as part of the Gamaredon hacker group. Media reports indicate that this FSB unit is capable of developing advanced malware, and modifying known malware to imitate other APTs to hide their activities. Here I limit the analysis to the two main APTs linked to the FSB: Callisto and Gamaredon.

3.3.1 Callisto

Callisto has been an APT focused on cyber espionage at least since 2015. Over the years, this group has targeted various organizations, including government institutions and military officials in Eastern Europe and the South Caucasus. The APT uses spear-phishing campaigns and social engineering tactics to inject malware into its targets. The group has also been observed to use remote access trojans (RATs) and credential-stealing malware to exfiltrate sensitive information from their victims. Callisto (aka COLDRIVER) is suspected to be a Russian APT which – although it has not been publicly linked with any Russian intelligence service – has, in past operations, been shown to have objectives which align closely with the strategic interests of the FSB. Callisto mainly focuses on specific Western countries, namely, the United States and Eastern European countries[275].
During the conflict in Ukraine, the group masterminded several phishing campaigns aimed at stealing credentials, targeting areas of military and strategic research such as NATO entities and defence entities based in Ukraine, as well as NGOs and think tanks. Additional targets include former intelligence officials, experts on Russian affairs and Russian citizens abroad. While the SBU, the Security Service of Ukraine, has publicly associated Callisto with the Gamaredon group - which I discuss in the next section - through a set of hacks attributed to the FSB and essentially focusing on operations in Ukraine since the start of the Russian invasion in February 2022, other Security companies do not support this link[276].
In particular, the IT security company SEKOIA.IO, in particular, has conducted numerous technical investigations, not finding any overlap between the activities of Callisto and Gamaredon, nor any coordination or cooperation activity between the two APTs, indicating a lack of intra-agency coordination. They instead suggest that these are two groups operating on different targets and purposes. Based on what SEKOIA.IO investigated, domains aligned with Callisto's past activities. Further investigations resulted in a more extensive infrastructure of more than 80 domains, including domain typosquatting activities. Since many of these domains were already known and the IP address resolution was already attributed to Callisto´s activities, SEKOIA.IO only associated these domains with Callisto with high confidence.
In campaigns observed in the past, Callisto sent malicious PDF attachments to their victims. The first page of the PDF simulated an error in the PDF renderer engine, prompting the victim to open a link that led to a malicious web page. This web page was tasked with collecting the victim's credentials using EvilGinx. Placing the phishing link in a PDF rather than in the body of the email prevents the link from being parsed by email gateways and is an effective tactic to remain undetected from an attacker´s perspective. SEKOIA.IO conducted open-source

[274] Kose, Joab. “Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage.” (2021).
[275] Kavya Rani, S R, B. C. Soundarya, H. L. Gururaj and V Janhavi. “Comprehensive Analysis of Various Cyber Attacks.” 2021 IEEE Mysore Sub Section International Conference (MysuruCon) (2021): 255-262.
[276] Aimé, Felix, Maxime A., and Threat & Detection Research Team - TDR. “Calisto show interests into entities involved in Ukraine war support.” Sekoia Blog. December 5, 2022.

research on typosquat domains to identify targets. Six private companies based in the United States and Eastern Europe, and four non-governmental organizations (NGOs) were identified, all involved in supporting Ukraine. Most of the targeted private organizations engage in activities related to military equipment, military logistics, or humanitarian support for Ukraine, including a US company that supplies humanitarian logistics and possibly tactical equipment to Kyiv. Other industries include information technology and computer security. SEKOIA.IO notes that the targets identified so far through the investigation, namely, the industrial and military entities affected and the individuals involved in Russian affairs, are all in line with Calisto´s interests.

Callisto also targets support which is not directly related to Ukraine. Among Calisto´s malicious domains discovered, three have caught the attention of analysts, namely, mvd-redir[.]ru and dns-mvd[.]ru (high confidence), which are most likely a typosquatting of the Russian Interior Ministry, and lk-nalog-gov[.]ru (with low confidence) the Russian Federal Tax Service. Because Callisto has been observed to target Russian individuals overseas, SEKOIA.IO finds it plausible that Callisto also engages in domestic surveillance activities. Another, less plausible, hypothesis would be a false flag manoeuvre to raise doubts about the attribution of the infrastructure. SEKOIA.IO found another potential victim that matches Callisto's known targeting. The domains sangrail-share[.]com and sangrail-ltd[.]com are typosquatting Sangrail Inc., a private security company, registered in the UK on July 31, 2019, by Ian Walter Baharie. That name was also used to register AC21, a British private intelligence firm focused on African politics[277].

Interestingly, that name appeared in a 17-year-old data leak that exposed a list of several MI6 officers on cryptome.org, a website dedicated to information leaks. That observation matches Microsoft's assessment of Callisto targeting former intelligence officers. It should be assessed that this kind of intrusion is aimed at a targeted collection of information contributing to the Russian efforts to interrupt the supply chain of military reinforcements for Kyiv.

Nonetheless, SEKOIA.IO estimates that Callisto contributes to intelligence gathering for Russian intelligence on identified evidence related to war crimes or international justice proceedings, likely to anticipate and build a counter-narrative about future allegations. Among Callisto’s targets, there would also be NGOs, and European and international institutions, evidence that this type of activity could enter the sphere of competence of the SVR and would indicate competitive activity between this agency and the FSB.

3.3.2 Gamaredon

Gamaredon activity as an APT has been observed since 2013. It is believed to have ties to the FSB, specifically Unit 71330. Although Gamaredon and Dragonfly are two separate APTs, they may both be related to Unit 71330. While Gamaredon mainly focuses on cyber espionage and intelligence gathering, Dragonfly (also known as Energetic Bear or Crouching Yeti) is reportedly notorious for sophisticated and multi-stage attacks aimed at compromising industrial control systems (ICS) and control systems of supervision and data acquisition (SCADA). Furthermore, while both groups may share TTPs, such as the use of spear-phishing emails as an initial attack vector, there is no direct evidence to suggest they are related or that they operate

[277] Insikt Group®. “Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine.” Recorded Future, 19th September 2022.
https://www.recordedfuture.com/russia-nexus-uac-0113-emulating-telecommunication-providers-in-ukraine

jointly. Gamaredon uses a variety of techniques and tools to compromise its targets, including, as already mentioned, spear-phishing emails with malicious attachments, social engineering attacks, and exploitation of known software vulnerabilities (n-days). Some of the malware and tools used by the Gamaredon group include Pteranodon, Jupyter and PowerShell-based tools[278]. In more detail, Gamaredon uses PowerShell scripts to automate various tasks, such as malware distribution, privilege escalation and data exfiltration.

Since the Russian invasion of Ukraine, the group remains one of the critical cyber threats to Ukrainian cyberspace. Gamaredon would operate from Sevastopol in Russian-occupied Crimea, acting on orders from the FSB's Center for Information Security in Moscow. The group began operations in June 2013, just months before Russia annexed the Crimean Peninsula from Ukraine. In its recent information-gathering campaigns against Ukraine, Gamaredon used malware written in PowerShell, known as GammaLoad and GammaSteel. These data exfiltration tools manage to capture files of specific extensions, steal user credentials and take screenshots of the victim's computer. These two pieces of malware are not new and were previously used by Gamaredon to target Ukraine's government and security services. Hackers use phishing emails to gain initial access to the victim's network. These emails contain malicious LNK files distributed in RAR archives. Only users with Ukrainian IP addresses can open these files. Hackers send phishing emails from domains associated with legitimate organizations, such as the Security Service of Ukraine, and the names of the malicious files included are usually associated with the war in Ukraine. Gamaredon's recent activity is characterized by the multi-stage distribution of malware payloads used to maintain persistence. These payloads represent similar variants of the same malware, each designed to behave the same way as the others.

According to CERT-UA, Gamaredon´s TTPs would have evolved during the war, improving its tactics and retraining the malware variants used to go undetected. CERT-UA said[279] that Gamaredon is responsible for the most significant cyber-attacks in Ukraine (even higher than those carried out by Sandworm), recording more than 70 incidents related to the group in 2022. Gamaredon also attacks allies of Ukraine. Latvia confirmed a phishing attack on its defence ministry in late January, linking it to the group. Ukrainian cybersecurity officials described their attacks as intrusive and daring, and said the group's primary purpose is to conduct targeted cyber intelligence operations[280].

Case study analysis of offensive cyber operations conducted by the Russian GRU, SVR, and FSB agencies highlights a complexity and sophistication that transcends the execution of conventional cyberattacks. In the context of the Russian-Ukrainian conflict, however, it emerged how the APTs linked to these agencies exploited their distinctive skills to implement operations, highlighting a level of internal coordination which, precisely because of the inevitable tensions and divergences, significantly influenced the effectiveness and the extent of their actions in cyberspace.

---

[278] Tiepolo, Gianluca. "Russian APT 'Gamaredon' Exploits Hoaxshell to Target Ukrainian Organizations." Medium, February 14, 2023.
https://mrtiepolo.medium.com/russian-apt-gamaredon-exploits-hoaxshell-to-target-ukrainian-organizations-173427d4339b

[279] Antoniuk, Daryna. “Russian Hacking Group Armageddon Increasingly Targets Ukrainian State Services”, The Record, July 16, 2023.

[280] Lakshmanan, Ravie. "New Russian-Backed Gamaredon's Spyware Variants Targeting Ukrainian Authorities." Hacker News, Feb 02, 2023.
https://thehackernews.com/2023/02/new-russian-backed-gamaredons-spyware.html

The case study investigation not only enriches the understanding of the operational TTPs peculiar to the Russian cyber offensive but also highlights how the lack of coordination can limit the overall impact of operations in the digital domain. Due to this lack of uniform coordination, the ability to operate highlights a strategic dimension that can surprisingly work against Russian offensive capabilities in cyberspace.

4. Conclusions

In the context of advanced persistent threats (APTs) which are sponsored by a state, inter-agency collaboration can be either a potential benefit or a significant obstacle. When cooperation is effective, it can optimize resources, improve efficiency, and increase the impact of operations. However, such cooperation is often hindered by several critical elements.
Interestingly, the competition between different intelligence agencies in Russia is evident. Many agencies, including the FSB, the SVR and the GRU, have overlapping responsibilities. These agencies have historically been known for their fierce rivalry, secrecy, and involvement in internal disputes[281].
This section addresses the research questions of my thesis, serving as an offensive case study. The analysis helps understand how the lack of coordination in cyberspace can be conceptualized to better understand how cyberattacks affect national and international security. Additionally, it explores how these interactions influence the effectiveness of both offensive and defensive operations.
The study reveals that the complexity of cyber operations, particularly involving multiple APTs managed by different intelligence agencies, makes coordination an intricate and difficult task. The challenges range from technical issues, such as compatibility of systems, software, networks, and delay issues, to more strategic issues, such as duplicating goals and operating methods across agencies. These problems can eventually lead to conflicts for territorial control and power.
I also identify other challenges affecting inter-agency coordination efforts, challenges related to different internal organizational cultures and operational dynamics. Each agency is characterized by its organizational culture, specific priorities, and distinct technical skills. For example, building trust, exercising leadership, managing decision-making, and dealing with uncertainty vary greatly across entities. These differences can lead to miscommunication, misunderstandings, or goal disagreements, ultimately affecting coordination.
Another important barrier to achieving effective coordination is the so-called “principal-agent” dynamic. Information asymmetry, with intelligence agencies (the “agents”) holding more information than decision makers (the “principals”), and possible conflicts of interest can lead to a reluctance to share valuable information. It hampers effective decision-making at the strategic level and complicates the overall intelligence operation. An example that illustrates the potential consequences of such challenges is the cyber-attack on the DNC in 2016. Despite the operation's success, the lack of coordination between APT28 and APT29 could have led to inefficiencies and missed opportunities.
In conclusion, although the coordination of APTs between different intelligence agencies can greatly amplify the impact of cyber operations, such coordination is fraught with technical,

[281] Lilly, Bilyana, and Joe Cheravitch. “The Past, Present, and Future of Russia's Cyber Strategy and Forces.” Paper presented at the 2020 12th International Conference on Cyber Conflict (CyCon), May 2020.

strategic, and human-related difficulties. In order to overcome such challenges, I identify three main components. Namely, a thorough understanding of the complexities of cyber operations, an appreciation of the cultural and operational differences between different intelligence agencies, and effective strategies for managing the "principal-agent" dynamic. Intelligence actors can achieve the full potential of coordinated cyber operations only via harnessing these components.

This chapter has significant political-military implications. By addressing the structural challenges and the lack of coordination in offensive cyber operations, this chapter provides crucial insights into the dynamics of state-sponsored cyber activities. It highlights how the divergence in operational methods and organizational cultures can hinder the effectiveness of coordinated efforts. These findings contribute to the broader understanding of the complexities involved in cyber warfare and underscore the importance of developing nuanced strategies that account for these variables.

CHAPTER VI

THE VIRTUAL BLUE TEAM IN LOCKED SHIELDS EXERCISE

1. Introduction

The lack of coordination in cyberspace, a growing problem given the sophistication of cyber-attacks, requires innovative solutions to be effectively countered. In this context, the integration of artificial intelligence (AI) in cybersecurity emerges as a promising solution, capable of responding effectively to attacks and overcoming challenges related to the lack of synchronization between different entities in cyberspace. Research and development activities are intensively engaged in creating advanced tools that, thanks to AI, can automatically identify threats, analyse attack patterns and implement defensive measures in real-time. This cutting-edge approach promises to strengthen cybersecurity by offering a coordinated and timely response to the constantly evolving threat landscape[282].

In the context of using artificial intelligence (AI) to improve coordination in cyberspace and effectively counter the increasing complexity of cyberattacks, the NATO Science and Technology Organisation's IST-152 research group has developed an innovative conceptual framework. This framework was developed specifically to improve cyber defence capabilities by directly addressing the problem of lack of coordination through the implementation of AI[283]. The proposed model is divided into several essential functions, each dedicated to a particular aspect of cybersecurity, including detection, world-state identification, learning, planning, communication and negotiation, and action selection and execution. These functions, integrated into a well-structured cyber defence system, work synergistically to ensure a comprehensive and coordinated response to cyber threats. Each function is further broken down into sub-functions to ensure that operations are carried out with maximum precision and efficiency, highlighting the importance of a holistic and coordinated approach in the fight against cyberattacks.

This integrated approach to cyber defence aims to improve the ability to detect and respond to cyber-attacks, enabling organisations to protect their digital assets more robustly. Employing AI capabilities in this context presents a promising opportunity to address the ever-increasing challenges of cybersecurity. However, it is essential to note that the proposed conceptual framework is still in development and requires further research and experimentation before its full implementation.

As the development of AI-based models progresses rapidly, it is evident that ample high-quality datasets are the most crucial component supporting these efforts. A good dataset should contain accurately labelled data, have a balance between attack and benign data, include current attack types, be generated on the latest technology network infrastructure, and encompass

[282] This Article has been published by JISA Q1 in 2024
Kott, Alexander, and Paul Theron. 2020. "Doers, Not Watchers: Intelligent Autonomous Agents Are a Path to Cyber Resilience." IEEE Security & Privacy 18 (3): 62–66.

[283] Kott, Alexander, Paul Théron, Martin Drašar, Edlira Dushku, Benoît LeBlanc, Paul Losiewicz, Alessandro Guarino, Luigi Mancini, Agostino Panico, Mauno Pihelgas, Krzysztof Rzadca, and Fabio De Gaspari. 2023. "Autonomous Intelligent Cyber-Defense Agent (AICA) Reference Architecture. Release 2.0."

attack campaigns executed over a sufficient period of time. AI models trained and tested using datasets possessing these characteristics can perform better in real-world scenarios.
There are numerous publicly available datasets, such as KDD datasets, CICIDS datasets, UNSWNB15, CIDDS, and UGR'16, but while these and other datasets cover some of the above characteristics, they do not fulfil all the desired criteria. To address this issue, the authors propose a solution. This chapter focuses on implementing this proposal and sharing the results obtained. I generated an IDS dataset called LSPR23, which contains current attack types, maintains a balance between attacks and benign data, utilizes state-of-the-art network devices and hardware found in a substantial infrastructure from the Locked Shields exercise, covers attack campaigns executed over a sufficient period, and exhibits a high level of labelling accuracy. I expect that the produced dataset will significantly contribute to developing AI-based intrusion detection systems (IDS) in academia and industry. Specifically, it will contribute in the following ways:

- Data collection during a specific iteration of Locked Shields, known as Partners Run
- Preliminary analysis of the collected data, accompanied by a public release of the dataset
- Outlining a research agenda toward a fully automated defender

2. Background on Locked Shields

Locked Shields is an annual live-fire cybersecurity exercise organized by the NATO CCDCOE since 2010.

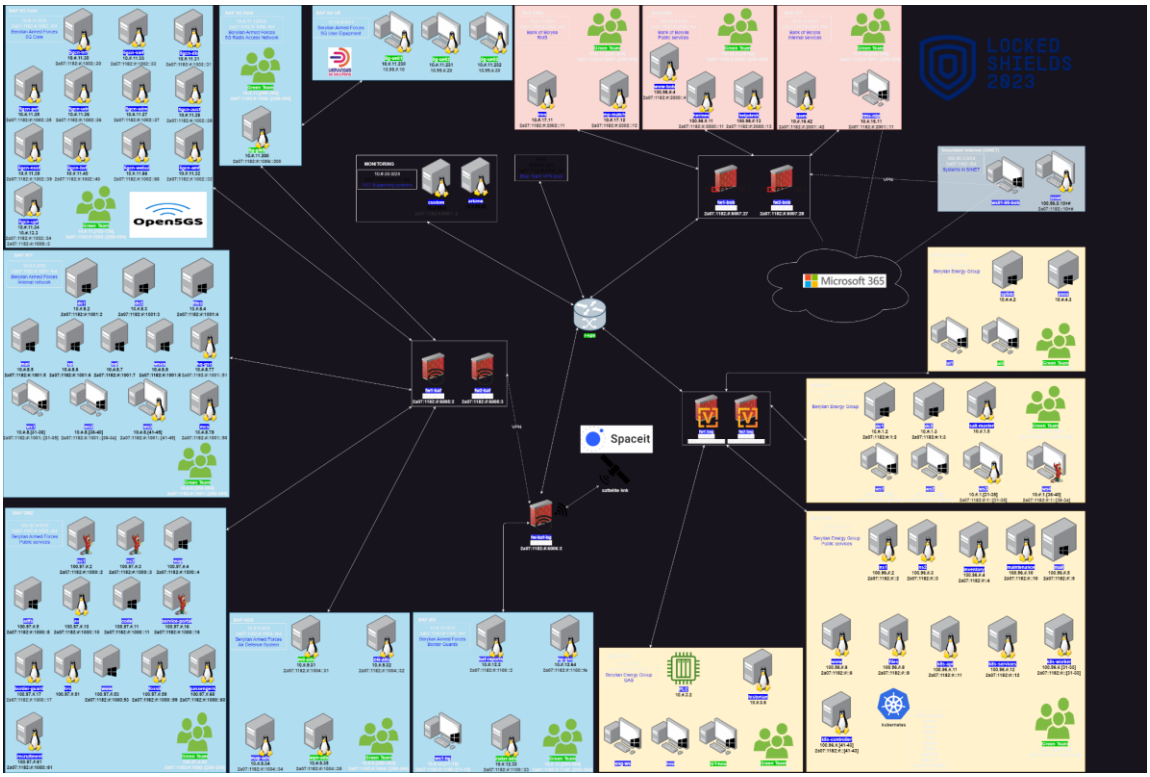


FIGURE 1. Locked Shields 2023 network map for the virtual blue team

It serves as a platform for blue teams to enhance their skills across various interdisciplinary categories, including real-time cyberattack defence, situation assessment, incident response, scenario handling, and ensuring the functionality of their computer systems. While the defence-oriented Locked Shields exercise primarily focuses on training the blue teams, four additional teams participate in the exercise. The red team is responsible for conducting attacks; the yellow team provides intelligence situation awareness; the green team maintains the back-end infrastructure; and the multifaceted white team oversees exercise control, strategy games, legal aspects, media, special investigation, and more.

The blue teams act as rapid-reaction units dispatched to assist a fictional country, Berylia, engaged in a prolonged conflict with another fictional country, Crimsonia. The red team primarily represents Crimsonia in the exercise. The blue teams must perform system administration tasks, implement security measures, handle forensic and legal challenges, and address various other duties assigned by the white team. As a result, the participating blue teams need to consist of experts with diverse skill sets to cover all the necessary competencies. The defending teams must keep in mind that there is a dedicated user simulation team, which assumes the roles of different users working on the systems. This team not only mimics regular usage patterns but also emphasizes the need for the blue teams to maintain system functionality. While preparation for the exercise takes place well in advance, the intense live-fire gameplay unfolds over just two days.

The red team's role in the exercise involves executing various escalating attacks. Their objective is to progress through various stages, starting from initial access and moving toward gaining persistence, privilege escalation, data collection, data exfiltration, and destruction. It is

important to note that due to the limited duration of the exercise, the number and pace of these attacks are significantly higher compared to real-world scenarios. In previous iterations of the exercise, the red teams have employed various attack techniques, as classified by the MITRE ATT&CK knowledge base. These techniques include exploiting vulnerabilities in public-facing applications, compromising legitimate user accounts, leveraging vulnerabilities for privilege escalation, moving laterally using remote services, collecting and exfiltrating data from target systems, defacing systems, and launching denial-of-service attacks.
FIGURE 2. AICA high-level structure of the agent

3. Related Work

In 2019, Kott et al. introduced a reference architecture that explores the utilization of autonomous intelligent cybersecurity agents for offensive cyber defence[284]. This reference architecture, known as AICA[285], includes information on the data services associated with agents and a detailed account of the functions incorporated within the architecture.
Another notable study[286]introduces a system designed to efficiently and accurately detect command and control (C&C) channels, even without prior knowledge of the network. The central concept is to train a classifier using historical network traffic data from previous attacks and utilize it to identify C&C connections within the current traffic of different networks. The system takes advantage of malicious traffic exhibiting similar patterns across networks, regardless of the specific location or devices involved (e.g., devices within a botnet tend to behave similarly). By leveraging recorded datasets from a participating team in the Locked Shields exercise (from 2017 and 2018), the authors demonstrate that their classifier can identify C&C channels in near real-time with high precision (99%) and recall (over 90%).
The system implementation is also shown to have realistic resource requirements. Additionally, the authors note that if the team had employed their system in the 2018 exercise, it would have successfully detected 10 out of 12 C&C servers within the initial hours of the exercise. Three key features have been introduced to enhance the system's detection capability. First, they propose a deep-learning approach that uses supervised and unsupervised methods to identify complex and evolving patterns of network behaviour, enabling the system to detect new intrusion attempts. Second, they stress the importance of including context awareness in their IDS to enable the system to understand and evaluate network traffic concerning the specific context of an organization or network, enhancing its ability to differentiate normal operations from potential threats. Third, they suggest incorporating a continuous learning mechanism that allows the IDS to adapt to the ever-changing network intrusion landscape, improving its detection capabilities over time.

[284] Kott, Alexander, Paul Théron, Martin Drašar, Edlira Dushku, Benoît LeBlanc, Paul Losiewicz, Alessandro Guarino, Luigi Mancini, Agostino Panico, Mauno Pihelgas, et al. 2018. "Autonomous Intelligent Cyber-Defense Agent (AICA) Reference Architecture. Release 2.0." arXiv preprint arXiv:1803.10664.
[285] Känzig, Nicolas, Roland Meier, Luca Gambazzi, Vincent Lenders, and Laurent Vanbever. 2019. "Machine Learning-based Detection of C&C Channels with a Focus on the Locked Shields Cyber Defense Exercise." In Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon), 900:1–19. IEEE.
[286] Klein, Jan, Sandjai Bhulai, Mark Hoogendoorn, Rob Van Der Mei, and Raymond Hinfelaar. 2018. "Detecting Network Intrusion Beyond 1999: Applying Machine Learning Techniques to a Partially Labeled Cybersecurity Dataset." In Proceedings of the 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), 784–787.

In[287], The authors highlight the need for up-to-date and realistic IDS datasets for accurate security modelling and threat detection. Inspired by the Locked Shields cyber defence competition, they propose a new method for generating such datasets, which will provide a better understanding of intrusion traffic.
Their approach involves creating an intrusion-detection dataset based on real-world network traffic, incorporating unique features inspired by the Locked Shields competition. By emphasizing the need for comprehensive, up-to-date datasets that capture the evolving network intrusion landscape, their approach proves highly relevant in the face of rapidly growing cyber threats. The authors[288] present an innovative network tool, CICFlowMeter-v4.0, capable of generating and analysing bidirectional network traffic flows with a specific focus on anomaly detection. The development of the tool has been influenced by the goals and achievements of the Locked Shields competition. A key feature is the tool's focus on anomaly detection, which aligns with the Locked Shields competition's focus on identifying and mitigating cybersecurity threats. This feature enables the tool to identify erratic network behaviour, making it a valuable asset in detecting potential intrusions. Moreover, the tool provides detailed analytics, such as stream duration, protocol type, packet length, and timing, contributing to a deep and comprehensive understanding of network traffic. The CICFlowMeter-v4.0 tool, inspired by the Locked Shields contest, thus offers an enhanced perspective on network traffic analysis, making a significant contribution to network security, particularly in the field of anomaly detection.
The authors[289] highlight the challenge of obtaining high-quality datasets to develop AI-based network intrusion detection systems (IDS). They discussed the limitations of existing IDS datasets available on the internet and suggested utilizing the unique infrastructure of Locked Shields, the world's largest live-fire cybersecurity exercise, to generate high-quality datasets. The authors propose integrating a virtual blue team (VBT) with autonomous agents as a solution to address security and privacy concerns. They also suggest utilizing network traffic directed toward the VBT, which operates independently of any specific blue team, as an effective resource for producing IDS datasets. These recommendations could offer valuable insights into enhancing the quality of datasets in IDS development.

4. Challenges

Building an IDS dataset is a challenge with many hurdles. First, it requires an extensive and realistic infrastructure that reflects the environment you want to model. It involves deploying various types of hardware and software, managing a complex network with different types of traffic, and maintaining a large user base. Building and managing such a large and complex infrastructure requires significant financial and personnel resources and advanced technical skills.

[287] Sharafaldin, Iman, Arash Habibi Lashkari, and Ali Ghorbani. 2018. "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization." Pages 108–116. January 2018.
[288]Lashkari, Arash Habibi, Gerard Draper Gil, Mohammad Mamun, and Ali Ghorbani. 2016. "Characterization of Encrypted and VPN Traffic Using Time-Related Features." February 2016.
[289] Halisdemir, Maj. Emre, Hacer Karacan, Mauno Pihelgas, Toomas Lepik, and Sungbaek Cho. 2022. "Data Quality Problem in AI-Based Network Intrusion Detection Systems Studies and a Solution Proposal." In Proceedings of the 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), 700:367–383.

Moreover, producing high-quality datasets entails going beyond automated script-generated malicious activity and incorporating realistic malicious activity. Replicating the tactics, techniques, and procedures used by natural and sophisticated attackers often requires involving cybersecurity experts or even ethical hackers. Locked Shields represents a perfect environment for this. Another challenge involves gathering information about attackers. To accurately label data and understand the attackers' motivations and techniques, the attackers must provide this information. In many cases, obtaining such details can be daunting, as attackers may be reluctant to share their strategies, or it may be challenging to acquire this information ethically and legally.

Furthermore, the dataset must be handled with extreme care to ensure that it does not contain sensitive information that could compromise the privacy or security of individuals or organizations. This entails implementing careful data collection and manipulation methods and may require anonymization or pseudogamication procedures. A smaller selection of the total raw collected data is created to be included in the public LSPR23 dataset. To address the concern of sharing potentially sensitive information contained in the log files, the current release of the dataset only includes flow-based information, as I continue to strive to overcome this hurdle.

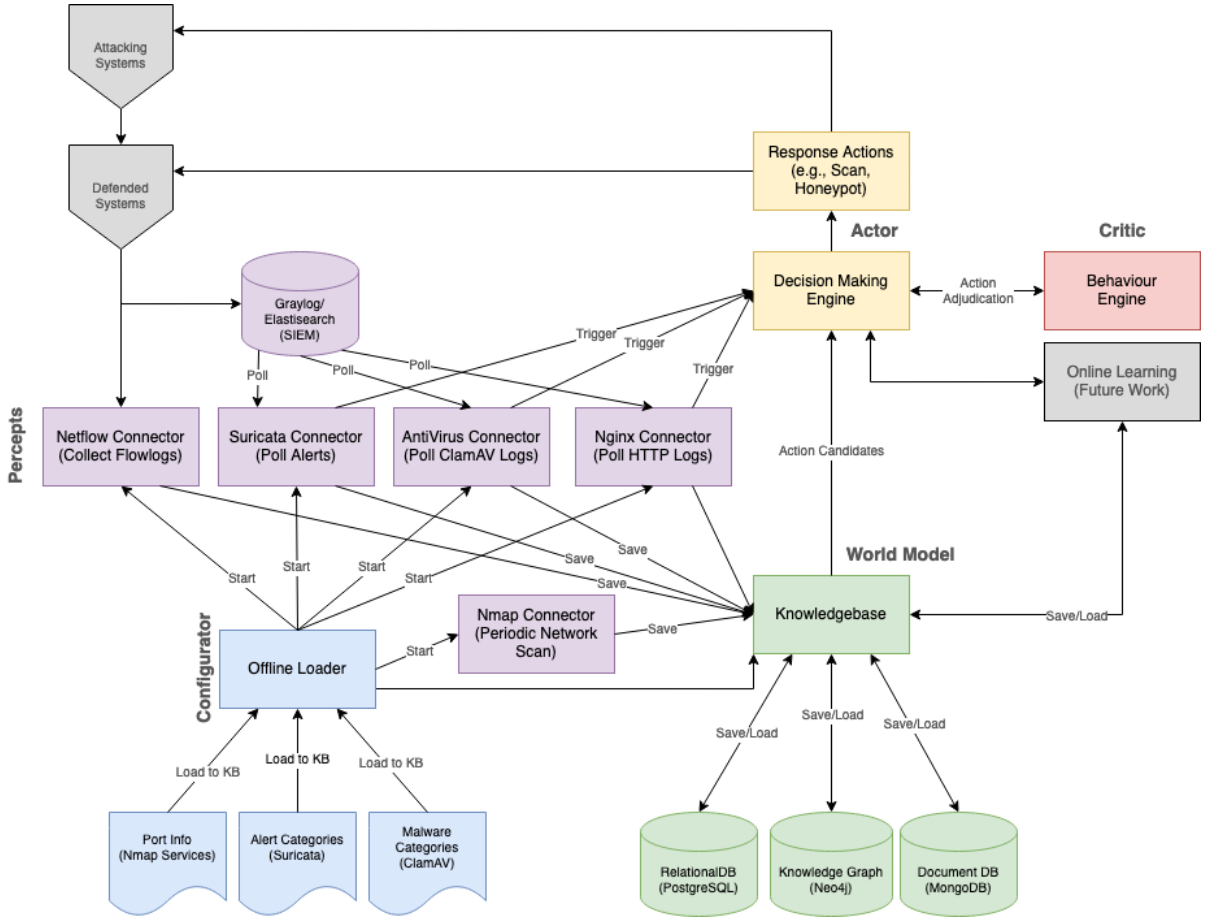
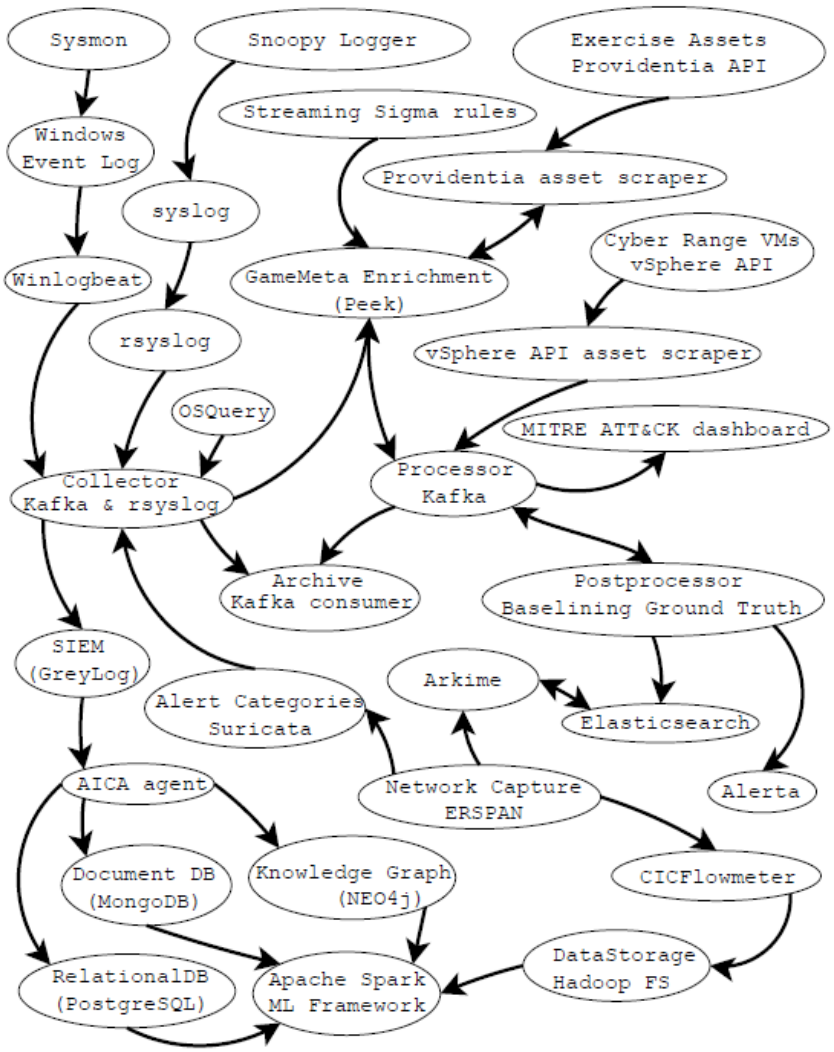


FIGURE 2. Virtual blue team data collection flow

Finally, the dataset must include a large and balanced sample of both benign and malicious events. This prevents the model from overfitting to malicious events and improves its ability

to generalize to new data. However, generating or collecting a substantial sample of benign events can be challenging, as it requires simulating or recording a wide range of everyday activities. These are just a few challenges that underscore the intricate and precise nature of creating a high-quality dataset for machine learning.

5. Data Collection



An overview of the Virtual Blue Team data collection flow in Figure 3.

For the collection and storage of the raw data, I made use of AICA and Frankenstack[290], merging them together in the overview figure. Frankenstack, a framework originally designed for monitoring red teams, is scalable for network environments like Locked Shields. On top of Frankenstack and AICA, I included OSQuery[291] for additional host-based logging and also

[290] Kont, Markus, Mauno Pihelgas, Kaie Maennel, Bernhards Blumbergs, and Toomas Lepik. 2017. "Frankenstack: Toward Real-Time Red Team Feedback." In MILCOM 2017 - 2017 IEEE Military Communications Conference, 400–405.

[291] Park, So-Hyun, Sun-Woo Yun, So-Eun Jeon, Na-Eun Park, Hye-Yeon Shim, Yu-Rim Lee, Sun-Jin Lee, Tae-Rim Park, Na-Yeon Shin, Min-Jin Kang, and Il-Gu Lee. 2022. "Performance Evaluation of Open-Source Endpoint

added a distribution system to orchestrate the automated installation of logging clients and to configure logging for all the VBT hosts on several network segments.

5.1 Network Traffic Collection

The architecture of the Locked Shields environment facilitated the remote capturing of traffic from multiple network segments. I used an encapsulated remote switched port analyzer (ERSPAN) to mirror the network traffic of all VBT hosts to an Arkime[292] instance. Using this Arkime instance, I captured network traffic and conducted exploratory data analytics (EDA). I took advantage of the meta information in the Locked Shields exercise that is only available to the green team. This information included the MAC and IP addresses of the VBT's virtual machines and the complete internal infrastructure that supports the exercise, like a virtual internet service provider. I also had access to the list of all possible network segments, IP addresses, and domain names that the attacking red teams, the defending blue teams, and the organizing green team could use. While the red team is required to use the preset IP addresses, they are allowed lateral movement from previously compromised hosts to any blue team. During EDA, I implemented the first attempt at labelling the data in Arkime by matching known benign and malicious IP addresses and network segment names to the active network flows. I observed network traffic with misconfigured, dynamic, or unusual IP addresses that would make it difficult to label the IP address without further knowledge of the external MAC address. During an earlier Locked Shields exercise, Arkime did not offer support for decoding encapsulated packets to show or filter the external MAC address.

In[293] and[294], I contributed to the development of generic routing encapsulation (GRE) support in Arkime. This enabled us to filter network traffic with dynamic and local fallback IP addresses that previously could not be matched to known IP addresses.

5.2 Intrusion Detection

The intrusion detection system (IDS) information in the LSPR23 dataset shows what is detected without machine learning. This baseline is crucial for analysing the impact of machine learning. I selected Suricata[295] as the anti-intrusion system to be implemented during the Locked Shields exercise. Configured as an IDS, Suricata can monitor network traffic to identify potential security threats or attacks. In this mode, Suricata works as a passive monitoring system that does not interfere with the traffic being monitored. I used port mirroring, a network setup that

Detection and Response Combining Google Rapid Response and Osquery for Threat Detection." IEEE Access: 20259–20269.

[292] Uramová, Jana, Pavel Segeč, Marek Moravčík, Jozef Papán, Tomáš Mokoš, and Marek Brodec. 2017. "Packet Capture Infrastructure Based on Moloch." In Proceedings of the 2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA), 1–7. IEEE.

[293] Dijk, Allard. 2022. "Fixed the Issue with the GRE IPs Not Showing Up in the Viewer." Arkime Pull Request on GitHub.

[294] Dijk, Allard. 2022. "Add Inner Mac Address to the Session for Encapsulated Protocols Like: GRE, Geneve, VXLAN." Arkime Pull Request on GitHub.

[295] Day, David, and Benjamin Burns. 2011. "A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines." In Proceedings of the Fifth International Conference on Digital Society, 187–192, Gosier, Guadeloupe.

allows all network traffic passing through a specific port (or VLAN) to be copied and routed to another port attached to Suricata's sensor. This configuration allows Suricata to monitor all network traffic passing through the mirror port, looking for potential security threats, known attack patterns or signatures, and traffic anomalies that could indicate a potential attack or threat.
During the Partner's Run, only the network segments protected by the VBT were reflected in a single interface, ensuring that other teams' network traffic was not intercepted. By integrating Suricata into the environment, I was able to monitor network traffic in real-time and detect various network-based threats, such as malware and phishing. In addition, I implemented a Suricata-based intrusion detection system to improve security during the exercise. Suricata allowed us to closely monitor network traffic in real-time, identifying various threats and promptly alerting us in case of incidents. It gave us greater visibility into network security and helped us prevent potential system damage or compromise.
Only publicly available generic rule sets were used, and no custom rules were added. The following ruleset sources were employed:

- Emerging Threats Open Ruleset: This open-source and publicly available[296] set of IDS rules is designed to detect a broad range of threats, including malware and phishing.
- Suricata Traffic ID Rule Set: This is a default open-source rule set delivered with Suricata and is primarily used for identifying and classifying social-media traffic.
- Threat Hunting Rules: The "hunt.rules" file[297] in the GitHub repository contains a set of threat-hunting rules written in the Snort IDS rules language. These rules can be used with various IDS systems, including Snort and Suricata, to identify potential threats within the network and systems.
- Core Malware Rules: The "malsilo.rules.tar.gz" file[298] in the GitLab repository contains a set of core malware rules written in the YARA rules language. These rules can be used with various security tools, including antivirus software, IDS systems, and threat-hunting platforms, to detect known malware families and variants.
- Stamus Networks Lateral Movement Rules: The "status-lateral-rules.tar.gz" file[299] on the Stamus Networks Threat Intelligence platform contains a set of lateral movement rules that detect potential lateral movement within a network's organization. The rules, written in the Suricata IDS rules language, can be used with Suricata IDS systems.

By utilizing these publicly available rule sets, I benefited from a comprehensive set of detection rules without the need to develop and maintain custom rule sets. Detected alerts were sent to a Kafka binder via Syslog. The Kafka collector received Syslog messages and transmitted them to the Kafka message broker for further analysis and processing. In the scenario, the alerts were sent in JSON format using an Extensible Event Format (EVE) event log. EVE is a structured log format used by Suricata IDS to record security events and is designed to be easily scanned and analysed by security tools and platforms.
With a centralised and scalable logging system like Kafka, I collected and archived security event logs from multiple sources in one place. This approach can help detect and respond to security incidents faster and more effectively. Moreover, using a standardized format like EVE

[296] EmergingThreats. 2023. "Emerging Threat Rules." Emerging Threats Rules Website.
[297] Green, Travis. 2023. "Threat Hunting Rules." Threat Hunting Rules on GitHub.
[298] Malsilo. 2023. "Threat Hunting Rules." Malsilo Rules on GitLab.
[299] Stamus Networks. 2023. "Stamus Networks Lateral Movement Rules." Stamus Rules on Their Website.

makes it easier to integrate various security tools and platforms, such as AICA, enabling analysis and reporting on the collected data.
Reducing false positive alarms was essential to optimizing an intrusion detection system like Suricata. To achieve this, I reviewed alert logs during a familiarization period and identified frequently encountered signatures that may generate excessive noise or false positives. Once identified, these signatures can be disabled or filtered to establish a more stable baseline of alerts with less noise. By carefully filtering out frequently encountered signatures that produced false positives, I reduced the noise in the alert logs and focused on alerts that were more likely to indicate genuine security threats. During the experiment, the following Suricata signatures were disabled by ID to reduce false positives:

- 2200073, 2200074, 2200075, 2200077, and 2200078: These signatures detect invalid checksums for various transport and IP protocols. While they can help detect specific attacks, they can also produce false positives due to legitimate traffic with invalid checksums. Disabling these signatures can reduce the number of false positive alerts related to check-sum errors.
- 2210044: This signature detects packets with invalid timestamps, which can indicate potential attacks. However, it can also produce false positives due to clock sync issues or other factors. Disabling this signature can help reduce false positives related to invalid timestamps.
- 2210010: This signature detects three-way hand-shake problems with incorrect sequence or acknowledgement numbers, which may indicate TCP session hijacking attacks. However, it can also produce false positives due to legitimate network behaviour. Disabling this signature can help reduce false positives related to handshake issues.
- 2033713: This signature detects Cobalt Strike Beacon traffic, a common indicator of malware activity. However, it can also produce false positives due to legitimate use of the Cobalt Strike tool. Disabling this signature can help reduce false positives related to Cobalt Strike traffic. I decided to disable this signature because the rule was fired many times during testing before Day 1 and was believed to be a false positive alert, but in hindsight, this was an incorrect decision. The red team was also testing their Cobalt Strike setup, resulting in the firing of this rule.
- 2018358: This signature detects suspicious POST requests to a quadruple IP address pointed using a fake browser user agent. While it can assist in detecting specific attacks, it can also produce false positives due to legitimate web traffic. Disabling this signature can help reduce false positives related to suspicious POST requests.
- 2260001: This signature detects the first data in the wrong direction for an application layer protocol. While it can assist in detecting specific attacks, it can also produce false positives due to legitimate network behaviour. Disabling this signature can help reduce false positives related to application-level issues.

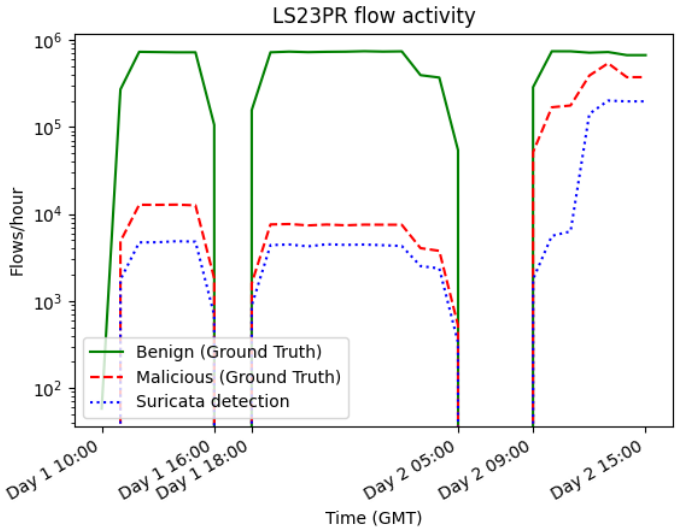


FIGURE 4. LSPR23 flow activity over time

6. Description Of The Public Locked Shields PR Dataset (LSPR23)

The Partner's Run edition of Locked Shields spanned two days. Day 1, known as the familiarization period, involved the defending blue teams studying the network they were tasked with defending. On Day 1, there were no active attacks from the red team, although non-destructive malware beaconing was allowed. Day 2, starting at 09:00 GMT, marked the commencement of active attacks by the red team, as indicated by the peak of malicious activity in Figure 4.

The gaps observed on Day 1 (16:00-18:00) and Day 2 (05:00-09:00) were unintentional. The server was responsible for recording the network traffic experienced a full disk, rendering it unable to record network traffic during those time ranges. However, as Locked Shields blue and red teams are only allowed to connect to their networks during office hours, and the issues were resolved before the official start of the red team, the resulting dataset is not missing important information, such as active attacks.

The disk-space failure occurred during overnight idle time, and from 18:00 on Day 1 to 05:00 on Day 2, the dataset still provides all the necessary information to study network behaviour outside of office hours. Starting from 09:00 GMT on Day 2, the red team launched attacks employing various techniques, including:

- Implanted vulnerabilities in network services
- System backdoors
- Network Attacks on BGP & ISP
- APT-like C2 using custom malware

For the extraction of time-based features, I used CI- CFlowMeter. After the exercise, I analysed the captured traffic with Arkime to identify the most frequently used application protocols. I modified CICFlowMeter to dissect network packets for 26 application protocols used in Locked Shields, incorporating this as the (indexed) Service feature. The list of protocols included in the dataset can be found at the end of this section. For all indexed features in the dataset, lookup tables are provided to reverse the indexed features back to their original values before indexing.

I added the two features introduced by Kanzig et al.[300]for Locked Shields data and used their methods for machine learning and evaluating the trained model. Additionally, I included the Zeek connection state feature, also used in a previous study[301] on Locked Shields data.
From the Suricata EVE source, I extracted the signature ID along with its revision, enabling the community to precisely identify and reproduce the rules I used. I also included the category, severity, and type of anomaly detected by Suricata. All the features in the dataset are indexed and ready to use for machine learning, with the ability to reverse their original values using the available index tables.
Each line of CICFlowMeter's output represents a net-workflow and is matched to the Suricata EVE log using an Apache Spark SQL join 1. The join shows matching sources from Table C to destinations in Table E, and vice versa. Due to the functioning of CICFlowMeter, the source and destination are also matched against the swapped flow. As CICFlowMeter accumulates network statistics of flows and stores them on disk after the connection is closed, or maximum flow time is reached, it can swap the source and destination if the next network packet starting after the timeout is received. While the issue could be addressed by keeping track of the source and destination fields after the flow timeout, I accepted this limitation for the study. I resolved the problem using both a normal and swapped match of CICFlowMeter and the Suricata EVE log.

6.1 Matching CICFlowMeter with Suricata

Every flow in the dataset is labelled as either benign or malicious. A flow is considered malicious if the source or destination IP in the flow originates from or connects to the red team infrastructure; all other flows are labelled as benign. Currently, I cannot label stepping-stone attacks as malicious. Therefore, when the red team compromises a blue-team host and uses it to attack another blue-team host, this is labelled as benign. The specific attack type used by the red team is not included in the labelling. However, the Suricata EVE information merged with the flow features can be used for research on specific attack types. The LSPR23 dataset combines features with and without Suricata information. The default combination I use for statistics is merged with the open-source Suricata IDS rules using the SQL query as seen in 1. I also included closed-source "Suricata Emerging Threat Pro-rules"[302] in the LSPR23 dataset as a separate file.
Although the segmentation of the network for a specific flow is not merged with the main flow features as a separate network-segment feature, the IP ranges of the used network segments are included as a separate file. Researchers can use this information to study specific segments of interest in adding the network-segment feature using the source and/or destination IP addresses available in the dataset. For processing this dataset, I recommend using a big-data framework like Apache Spark with a distributed file system such as Hadoop. Pre-processing millions of records in this dataset using Spark can be done in a matter of seconds, compared to hours when using traditional Pandas or Numpy.

[300] Känzig et al. 2019
[301] Klein, Jan, Sandjai Bhulai, Mark Hoogendoorn, Rob Van Der Mei, and Raymond Hinfelaar. 2018. "Detecting Network Intrusion Beyond 1999: Applying Machine Learning Techniques to a Partially Labeled Cybersecurity Dataset." In Proceedings of the 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), 784-787.
[302] Stamus. Stamus networks lateral movement rules, 2023. Stamus Rules on their website.

The Locked Shields network is segmented into various separate networks, as depicted in Figure 1 and listed below:

Simulated Internet (SINET)
Berylian Armed Forces
5G Core
5G Radio Access Network
5G User Equipment
Internal network
Public Services
Border Guard (radar)
Air Defense System (satellite)
Bank of Berylia
Risk Management System
Public Services
Internal Services
Berylia Energy Group
Internal Services
Public Services (DMZ)
SCADA sp5dc psos
PLC/HMI/historian

I experimented with the following feature combinations and will refer to the top-listed combination for the statistics of LSPR23 in this chapter:

- Suricata with Open Emerging rules (used in this chapter as statistical reference)
- Suricata with Open Emerging rules, including a selection of open-source rules
- Suricata with Pro-rules
- Suricata with Pro-rules, including a selection of open-source rules

The following features are available in the LSPR23 public dataset:

- 84 CICFlowMeter features[303]
- 5 Suricata features: signatureID_revision, category, severity, confidence, and anomaly_event
- 2 Features from Kanzig et al.[304]: int_ext and l3_l4
- 1 Bro/Zeek connection state feature[305]
- 1 Service feature, showing one of the de- tected protocols: UNKNOWN, DNS, TLS, HTTP, SSH, ICMPv6, SMB, DCERPC, RDP, SMTP, NTP, LDAP, KRB5, ICMP, SIP, RTP, SCTP, BGP, RTCP-RRRTCP-SR, RTCP-RR, DHCPv6, SIP, RTCP-SR, RTCP-APP, RTCP-SDES, RTCP- SRRTCP-RR, or MYSQL

7. Data Analysis

By comparing Suricata's detection accuracy and recall to the actual ground truth without machine learning, I gain valuable insights for blue teams. From this perspective, the blue teams can use Suricata to build their own ground truth labels. Since blue teams often start from scratch without access to pre-existing ground truth, having reliable ground truth data becomes significant for their decision-making process. In this context, Suricata can serve as a tool for blue teams to establish their own ground truth labels. By integrating Suricata, blue teams can benefit from its ability to follow the curves of the malicious ground truth.
Precision and recall scores estimate the accuracy and completeness of the Suricata labels compared to the actual ground truth. These metrics help blue teams understand the reliability and effectiveness of Suricata in correctly identifying and classifying network flows.
Suricata can generate alerts based on signatures and anomalies. When examining the outcomes, it is evident that the Suricata signatures exhibit a remarkable maximum accuracy of approximately 0.9107, indicating their effectiveness in correctly identifying positive cases. However, their recall rate of 0.3268 suggests a limitation in capturing all positive cases, resulting in missed detections. On the other hand, the Suricata anomalies demonstrate a much lower precision value of 0.4431 and a recall of 0.0169, indicating decreased precision and recall metrics.

[303] Lashkari, Arash Habibi. 2018. "CICFlowMeter-V4.0 (formerly known as ISCXFlowMeter) is a Network Traffic Bi-flow Generator and Analyser for Anomaly Detection." Accessed August 2018.
[304] Känzig, Nicolas, Roland Meier, Luca Gambazzi, Vincent Lenders, and Laurent Vanbever. 2019. "Machine Learning-based Detection of C&C Channels with a Focus on the Locked Shields Cyber Defense Exercise." In Proceedings of the 11th International Conference on Cyber Conflict (CyCon), 1-19. IEEE.
[305] Paxson, Vern. 1999. "Bro: A System for Detecting Network Intruders in Real-Time." Computer Networks 31, no. 23-24: 2435-2463.

It is important to highlight the significance of precision over recall in this context. Given the vast number of network actions, even with relatively high precision, the abundance of false positives can overwhelm the system's resources and hinder a timely response by the security team. Considering the limited time available, it becomes crucial to prioritize the reported activities effectively. These observations further emphasize the need for advancing automation techniques or developing an autonomous system in the future. Analysing the results, I observe that the Suricata signatures achieve an estimated maximum accuracy of about 0.9107 and a recall of 0.3268. This indicates that Suricata signatures accurately identify positive cases but have limited recall, meaning they may miss some positive cases. On the other hand, the Suricata anomalies have an estimated maximum precision of 0.4431 and a recall of 0.0169, suggesting lower precision and recall values. Considering the entire set of Suricata labels, the estimated maximum precision is about 0.8657, while the recall is 0.3438. These scores indicate that the Suricata labels show reasonably good accuracy and recall rates compared to the ground truth.
In summary, incorporating Suricata as a tool for constructing ground truth labels is essential for blue teams, as it provides a reliable starting point in the absence of ground truth data. By understanding the accuracy and recall of the IDS of Suricata labels and comparing them to the green team's ground truth, blue teams can gain insight into Suricata's performance and potential limitations in accurately labelling network flows. These results highlight the importance of Suricata in constructing ground truth labels for analysing blue team networks.
I conclude this section with a statistical overview of the LSPR23 dataset using the open-source IDS rules combination of features:

Statistical overview of the LSPR23 dataset	
Benign Flows	14.363.892
Malicious Flows	1.989.484
Scoring Bot Flows (Benign)	420.479
True Positive IDS Alerts	650.219
False Positive IDS Alerts	63.745
5G Flows	167.774
Bank Swift Flows	98.551
Air Defense / Border Guard Flows	1.162.082
Gas/Power Flows	138.618

Estimated max precision using IDS signatures	0.911
Estimated max recall using IDS signatures	0.327
F1/Recall score using Random Forest trained on ground truth	0.997
AUC score using Random Forest trained on ground truth	0.9999

8. Evaluation

I evaluated the LSPR23 dataset based on the criteria outlined by Sharafaldin et al.[306]:

- Complete Network Configuration: The Locked Shields 2023 Partners Run infrastructure is highly comprehensive, consisting of a mix of information technology (IT) and operational technology (OT). The network topology encompasses various IT systems, such as internet service provider (ISP) technology, simulated internet with internal hijacked IP addresses, redundant routers, switches, firewalls, and VPNs. The topology also includes IT/OT systems such as military 5G communication, SCADA/ICS for a power plant, SWIFT banking, military board guard, and satellite communications. Notably, the operating systems used are not limited to Ubuntu and Windows but encompass a wide range of systems.
- Complete Traffic: The dataset contains traffic from all teams, including the defenders (blue teams), attackers (red teams), organisers (green team, white team, and yellow team), and the user simulation team.
- Labeled Dataset: Each flow in the dataset is labelled with the ground truth and the Suricata signature and anomaly IDs.
- Complete Interaction: The dataset covers all the systems shown in Figure 1, including systems used for scoring by the green team. It encompasses communication between internal LANs and internal ISP communication. For example, this enabled the capture of border gateway protocol (BGP) attacks on the ISP.
- Complete Capture: All system network traffic was recorded using ERSPAN. After the conclusion of Day 1, the blue teams could not interact with their systems, and the red teams were also prohibited from doing so. During this game-closed period, traffic was not captured for about six hours. However, this should not pose a problem for the dataset because many more hours of "idle" data is available during this period. And most importantly, no attacks took place during this period.
- Available Protocols: In Section VII, I provided an overview of the protocols I dissected by modifying CICFlowMeter. In addition to commonly available IT protocols, the

[306] Sharafaldin, Iman, Arash Habibi Lashkari, and Ali Ghorbani. 2018. "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization." 108-116

dataset includes a broad spectrum of special systems such as 5G, Kubernetes, Satellite, radar, SWIFT, and SCADA/ICS protocols.

- Attack Diversity: The red team comprises subteams focusing on client networks, the web, and special systems. All current technologies are targeted. The red team aims to avoid disrupting the blue teams' systems so they can continue their attacks. Once the red team achieves their initial objectives, they move to more disruptive attacks. The red team can instruct the user simulation team to click on a URL and execute malware.
- Heterogeneity: I captured network traffic from all machines using ERSPAN during the execution of the attacks. I also obtained all host-based logs for future analysis. However, the current LSPR23 dataset does not contain host-based logs at the time of publication of the first version. Before publishing the host-based logs, I need to address the challenge of removing private information while maintaining the data's value for model development.
- Feature Set: I extracted more than 16 million net-workflows, each with 93 features, from the Locked Shields network traffic. The dataset is provided as a CSV file, including lookup tables for the indexed features and additional metadata.
- Metadata: I captured and stored all available metadata from the exercise's supporting system. I selected the relevant metadata for inclusion in the LSPR23 dataset. This includes information such as network segment, MAC and IP addresses, host and domain names, the responsible team name for each system, and the services running on the hosts.

9. Conclusion

This chapter presents a publicly available IDS dataset derived from the network infrastructure of Locked Shields, which is recognized as the world's largest live-fire cybersecurity exercise. To address the challenge of dataset confidentiality, a virtual blue team was implemented during the exercise, resulting in the LSPR23 dataset derived from the team's network traffic. This allows researchers involved in the Locked Shields Exercise to conduct reproducible research, which was previously not possible. Given the unique infrastructure of the Locked Shields exercise, utilization of state-of-the-art network devices and hardware components, and inclusion of the latest attack types executed by the red team, I believe that the generated dataset will make a significant contribution to IDS research and development efforts in academia and industry.

RESULTS AND CONCLUSIONS

This dissertation presents a comprehensive analysis of the coordination dynamics in defensive and offensive cyber operations. The research delves deeply into the context of cyber operations in contemporary conflict scenarios, focusing on complex landscape of cyber threats. These three case studies provide a more comprehensive view and in-depth understanding of the challenges and needs for coordination in high tension and geopolitical uncertainty, underlining the importance of this research.

Through advanced technical tools, targeted surveys and in-depth interviews, this research comprehensively explored the challenges, opportunities and various perceptions that emerge in the coordination and collaboration between crucial operational units in the field. The work aimed to identify the need to reformulate operational strategies and tactics to maximise effectiveness. Furthermore, concrete solutions were proposed to address and solve the identified coordination problems.

The study used advanced technical tools, targeted surveys and comprehensive interviews to examine the challenges and opportunities in coordinating cyber operations, focusing on the dynamics between the Offensive Cyber Unit (OCU) and the Command and Control Headquarters (CHQ).

Much of the research scrutinised the interaction between the OCU (Offensive Cyber Unit) and the CHQ (the Cyber Headquarter). This examination revealed both strengths and weaknesses in their operational performance. By analysing how communication and decision-making processes influence the efficiency of coordination, the study provides a clearer understanding of the factors contributing to cyber operations' success or failure. The results emphasise the importance of effective communication channels and sound decision-making frameworks to improve coordination. The research also explored the role of technology in solving coordination problems. Using the Virtual Blue Team and artificial intelligence (AI) proved crucial. These technologies facilitated simulations and learning algorithms, which uncovered previously invisible operational dynamics. By revealing these hidden dynamics, the research offers new perspectives on how to improve coordination. In particular, AI integration has improved the ability to predict and mitigate coordination challenges.

The research also provides practical guidance for optimising coordination strategies. These strategies are designed to enhance the responsiveness and resilience of cyber units against sophisticated cyber threats. By focusing on creating a seamless operational environment, the study suggests tangible ways to increase the collective effectiveness of defensive and offensive cyber operations.

The dissertation documented several case studies in detail. These case studies offered valuable insights into coordination strategies in different geopolitical contexts. The detailed analysis of these operations highlighted different state actors' diverse approaches and tactics, providing a nuanced understanding of how geopolitical factors influence coordination in cyber operations.

The research emphasised the importance of advanced analytical tools in understanding cyber threats. The integration of the MITRE ATT&CK framework, the Malware Information Sharing Platform (MISP) and the Yara rules was crucial in analysing the tactics, techniques and procedures (TTPs) of Advanced Persistent Threats (APTs). These tools helped decipher the complex interactions and coordination challenges between APT groups, providing a detailed understanding of their operational methodologies. Using these tools has enhanced the ability

to identify and address gaps in coordination, thus improving the overall effectiveness of cyber defence strategies.

Theoretically, the research systematically explored the concept of coordination in cyber operations, an area that has been relatively underexplored in the literature. A key strength of this thesis is its multidisciplinary approach, integrating theoretical strands from international relations, security and strategic studies, and computer science. This comprehensive theoretical analysis provided a clearer view of the factors contributing to the success or failure of cyber operations, emphasizing practices to improve coordination. Furthermore, integrating offensive and defensive cyber operations within a single research project represents an innovative approach that recognizes the symbiotic relationship between attack and defence in cyber warfare.

This holistic strategy simultaneously considers and aligns both aspects, offering a significant theoretical contribution to the existing literature on cyber operations. By drawing on diverse academic fields, the research not only enhances the understanding of cyber coordination but also proposes practical strategies for improving cyber defence and offence coordination.

From an empirical standpoint, this thesis employs a mix of case studies, targeted surveys, and in-depth interviews to explore the intricacies of coordinating cyber operations. The documented case studies, including operations involving Chinese APTs and Russian APTs, as well as NATO-organized cyber exercises, offer practical insights into coordination strategies in various contexts. The detailed analysis of these operations reveals the diverse approaches and tactics of different state actors, providing a nuanced understanding of how geopolitical factors impact coordination in cyber operations.

Furthermore, the research explored the crucial role of advanced technologies, such as the Virtual Blue Team and artificial intelligence (AI), in solving coordination problems. These technologies have facilitated simulations and learning algorithms that have uncovered previously invisible operational dynamics, offering new perspectives on improving coordination. In particular, integrating AI has improved the ability to predict and mitigate coordination challenges.

The methodological approach adopted for data collection and analysis in this research played a crucial role in precisely delineating critical areas requiring improvement and recognising some highly effective practices already in use. Prominent among these, as highlighted in the third case, is the use of the Virtual Blue Team and the application of artificial intelligence, which have proven to be critical tools in mitigating coordination problems. These advanced technologies, through sophisticated simulations and learning algorithms, made it possible to identify operational dynamics otherwise not evident, thus offering new perspectives on the effectiveness of coordination.

During the conclusion of the results, special attention was paid to developing practices geared towards direct implementation in the field. The aim has been to facilitate better integration and promote optimised operational synergy between the different units involved and between the operational and tactical levels, thereby improving their responsiveness and resilience in the face of increasingly sophisticated and pervasive cyber threats.

In light of the analyses and conclusions that emerged from this research, it is essential to provide concrete policy recommendations to improve cyber operations' coordination and effectiveness. This study has highlighted several critical areas that need targeted action to

optimize operational strategies and ensure greater resilience of cyber units against increasingly sophisticated and pervasive threats.

- Proactive measures must be taken to strengthen the resilience of computer networks: investing in research and development, promoting cyber awareness and education, and cultivating a cybersecurity culture within government organisations are vital steps to reduce vulnerabilities and improve resilience to emerging threats.
- Field research has shown the importance of coordination between the Offensive Cyber Unit (OCU) and the Command and Control Headquarters (CHQ): developing clear and well-defined protocols for information sharing and rapid decision-making is imperative. Advanced technologies such as artificial intelligence and the Virtual Blue Team can facilitate this, and they have been shown to significantly improve coordination effectiveness.
- It is of utmost importance that coordination strategies are continuously monitored and adapted as cyber threats evolve: this dynamic approach is not just a recommendation but necessary to ensure that cyber operations remain effective and resilient in the face of a constantly changing threat landscape.

These policy recommendations are designed to provide a solid basis for developing up-to-date coordination strategies capable of responding effectively to emerging challenges in the evolving cyber landscape. Implementing these recommendations will help improve the security and effectiveness of cyber operations globally.

In light of the findings and policy recommendations, there are several promising avenues for future research in cyber defense, particularly focusing on maritime security from a Cyber Threat Intelligence (CTI) perspective. Future research should expand data collection beyond network traffic to include host logs, security appliance alerts, and user interactions, enhancing the ability to detect and analyze cyber threats comprehensively.

Developing sophisticated AI models capable of leveraging this diverse data is crucial. Research should refine supervised and unsupervised machine learning techniques to identify malicious activities and anomalies across different data layers. Additionally, implementing effective actions based on gathered intelligence, such as system restoration and traffic blocking, is essential. By advancing these areas, researchers can work towards the vision of an automated and intelligent cybersecurity agent, enhancing the resilience of maritime infrastructure against evolving threats.

A key area of interest is the development of advanced methodologies for threat information analysis and sharing (CTI) geared explicitly towards maritime security. Maritime infrastructures, vital to global trade and national security, are desirable targets for cyber espionage and sabotage operations. Future research should focus on creating coordination models that improve the resilience of these infrastructures through the timely and accurate exchange of threat data, the adoption of common security standards and the implementation of joint cyber defence exercises.

Excitingly, the application of emerging technologies such as artificial intelligence and machine learning holds great potential to enhance the ability to detect and respond to cyberattacks in real-time. The ability to predict adversaries' moves and dynamically adapt defensive strategies is a crucial element in protecting maritime infrastructure. Future research should explore how these technologies can be integrated into existing cyber defence systems, significantly improving the effectiveness of both defensive and offensive operations.

In conclusion, this dissertation offers an in-depth and detailed examination of the complexities and challenges inherent to coordination in cyber operations, emphasising the importance of a holistic and integrated approach to address these issues effectively. The study highlights the crucial importance of understanding and managing coordination dynamics in the cyber domain, analysing critical scenarios such as the cases between China and Russia or the inherent dynamics of Russian intelligence agencies and their APTs.

The dissertation outlines key challenges and offers valuable lessons directly applicable to modern operational contexts, contributing significantly to the academic corpus on cyber defence and cyberwarfare. These recommendations are not just theoretical constructs but practical guidelines designed to guide the development of more robust and informed operational strategies. They aim to strengthen response capabilities in the face of increasingly sophisticated and rapidly evolving threats.

The work confronts previously underestimated issues and advocates for innovative solutions in a globalized and highly digitized environment, thereby guiding future policies and operational practices towards more effective management of cyber operations. In this way, the research not only contributes to cybersecurity theory, but also provides a practical and applicable framework for enhancing security strategies globally, underscoring the direct relevance of this research to real cyberdefence challenges.

REFERENCES

- Ahmad, Atif, Jeb Webb, Kevin C. Desouza and James Boorman. “Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack.” Comput. Secur. 86 (2019): 402-418.
- Aiyanyo, Imatitikua D., Hamman Samuel, e Heuiseok Lim. "A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning." Applied Sciences 10, no. 17 (2020): 5811.
- Al-Shamisi, Ahmed. "Active Offensive Cyber Situational Awareness: Theory and Practice." PhD diss., Brunel University, 2014.
- Antoniuk, Daryna. “Russian Hacking Group Armageddon Increasingly Targets Ukrainian State Services”, The Record, July 16, 2023.
- Antoniuk, Daryna. “Sandworm hacking group linked to new ransomware deployed in Ukraine.” The Record. November 29, 2022.
- Arata, Harold J., and Brian L. Hale. “Smart Bases, Smart Decisions.” The Cyber Defense Review 3, no. 1 (2018): 69–78.
- Arquilla, John, and David Ronfeldt. “Cyberwar is Coming!” Comparative Strategy 12, no. 2 (1993): 141-165.
- Arquilla, John, and David Ronfeldt. "The Advent of Netwar." Rand, 1996.
- Austin, G., K. Lin Tay, and M. Sharma. "Great-Power Offensive Cyber Campaigns: Experiments in Strategy." Tech. Rep. https://www.iiss.org/blogs/research-paper/2022/02/great-power-offensive-cyber-campaigns.
- Bateman, Jon. “Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications.” Carnegie Endowment Paper, December 16, 2022. https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.
- Bennett, Andrew, and Colin Elman. "Qualitative Research: Recent Developments in Case Study Methods." Annual Review of Political Science 9, no. 1 (2006): 455-476.
- Biderman, Stella, Hailey Schoelkopf, Quentin Anthony, Herbie Bradley, Kyle O’Brien, Eric Hallahan, Mohammad Aflah Khan, Shivanshu Purohit, USVSN Sai Prashanth, Edward Raff, et al. 2023. "Pythia: A Suite for Analyzing Large Language Models Across Training and Scaling." arXiv preprint arXiv:2304.01373.
- Bienstock, D., M. Derr, J. Madeley, T. McLellan, and C. Gardner. "UNC3524: Eye Spy on Your Email." https://www.mandiant.com/resources/blog/unc3524-eye-spy-email.
- Bonnet, Grégory and Catherine Tessier. “Coordination despite constrained communications: a satellite constellation case.” (2008).
- Borghard, Erica D., and Shawn W. Lonergan. “The Logic of Coercion in Cyberspace.” Security Studies 26 (2017): 452 - 481.
- Brogi, Guillaume and Valérie Viet Triem Tong. “TerminAPTor: Highlighting Advanced Persistent Threats through Information Flow Tracking.” 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (2016): 1-5.
- Buchanan, Ben. “The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.” Oxford University Press, 2017.
- Buchanan, Ben. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge, MA: Harvard University Press.
- Burt, Jeff. “Russia's APT28 targets Ukraine government with bogus Windows updates.” The Register, 2 May 2023.

- Byman, Daniel, and Jeremy Shapiro. The Challenge of Defeating the Islamic State: Report of a Workshop on “Fighting ISIS: Measures and Models.” Brookings Institution, 2011.
- Calcara, Antonio, Andrea Gilli, Mauro Gilli, and Ivan Zaccagnini. "Will the Drone Always Get Through? Offensive Myths and Defensive Realities." Security Studies 31, no. 5 (2022): 791-825. Routledge.
- Carly, P. "US, UK and EU Blame Russia for ‘Unacceptable’ Viasat Cyberattack." TechCrunch. https://techcrunch.com/2022/05/10/russia-viasat-cyberattack/.
- Chaudhary, Sunil, Vasileios Gkioulos, e Sokratis Katsikas. "Developing metrics to assess the effectiveness of cybersecurity awareness program." Journal of Cybersecurity 8, no. 1 (2022).
- Chaudhary, Tarun, Jenna Jordan, Michael Salomone, and Phil Baxter. "Patchwork of Confusion: The Cybersecurity Coordination Problem." Journal of Cybersecurity 4, no. 1 (2018).
- Cheravitch, Joe and Bilyana Lilly. “Russia´s Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond.” (2020); Zoller, Richard G.. “Russian Cyberspace Strategy and a Proposed United States Response.” (2010).
- Chinese State-Sponsored Group 'RedDelta' Targets the Vatican and Catholic Organizations." Recorded Future, 2020. https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf.
- Clarke, Richard A., and Robert K. Knake. "The Rise of Active Defense in Cybersecurity." Foreign Affairs 94, no. 2 (2015): 84-93.
- Clingendael Report October 2021. 'EU-NATO cooperation: what has been achieved so far?' Countering Hybrid Threats. Accessed. https://www.clingendael.org/pub/2021/countering-hybrid-threats/3-eu-nato-cooperation-what-has-been-achieved-so-far/.
- Clough, Chris. “Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation.” International Journal of Intelligence and CounterIntelligence, vol. 17, no. 4, 2004, pp. 601-613.
- Côté Cyr, A. "Mustang Panda’s Hodur: Old Tricks, New Korplug Variant." Section: ESET Research, March 2022. https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/.
- Courtney, W., and P. A. Wilson. "If Russia Invaded Ukraine." December 2021. https://www.rand.org/blog/2021/12/if-russia-invaded-ukraine.
- Crocker, Andrew, e Bill Budington. "NSA’s Failure to Report Shadow Broker Vulnerabilities Underscores Need for Oversight." Electronic Frontier Foundation, 23 settembre 2016. https://www.eff.org/deeplinks/2016/09/nsas-failure-report-shadow-broker-vulnerabilities-underscores-need-oversight.
- Cyber Warfare." RAND Corporation. https://www.rand.org/topics/cyber-warfare.htm
- D'Encausse, Hélène Carrère. La Gloire des Nations: Ou La Fin de l'Empire Soviétique. Fayard, 2014.
- Dawson, Andrew J and Martin Innes. “How Russia's Internet Research Agency Built its Disinformation Campaign.” The Political Quarterly (2019).
- Day, David, and Benjamin Burns. 2011. "A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines." In Proceedings of the Fifth International Conference on Digital Society, 187–192, Gosier, Guadeloupe.
- DeSombre, W., and D. Byrnes. "Thieves and Geeks: Russian and Chinese Hacking Communities," 2018. https://go.recordedfuture.com/hubfs/reports/cta-2018-1010.pdf.
- DiResta, Renee, e Shelby Grossman. "Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019." Cyber Policy Center, Freeman Spogli Institute for International

Studies, Stanford University, 12 novembre 2019. https://cyber.fsi.stanford.edu/io/publication/potemkin-think-tanks.

- Dijk, Allard. 2022. "Add Inner Mac Address to the Session for Encapsulated Protocols Like: GRE, Geneve, VXLAN." Arkime Pull Request on GitHub.
- Dijk, Allard. 2022. "Fixed the Issue with the GRE IPs Not Showing Up in the Viewer." Arkime Pull Request on GitHub.
- Dunn Cavelty, Myriam and Andreas Wenger. “Cyber security meets security politics: Complex technology, fragmented politics, and networked science.” Contemporary Security Policy 41 (2020): 32 - 5.
- Dykstra, Josiah, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. "Maximizing the Benefits from Sharing Cyber Threat Intelligence by Government Agencies and Departments." Journal of Cybersecurity 9, no. 1 (2023).
- Ebinger, Falk, Sylvia Veit, and Nadin Fromm. “The partisan–professional dichotomy revisited: Politicisation and decision-making of senior civil servants.” Public Administration (2019).
- Egloff, Florian J. and Max Smeets. “Sandworm: a new era of cyberwar and the hunt for the Kremlin’s most dangerous hackers.” Journal of Cyber Policy (2020).
- Egnell, Robert. “Civil–military coordination for operational effectiveness: Towards a measured approach.” Small Wars & Insurgencies, vol. 24, no. 2, 2013, pp. 237-256. 30 Apr 2013.
- EmergingThreats. 2023. "Emerging Threat Rules." Emerging Threats Rules Website.
- Eun, Yong-Soo, and Judith Sita Aßmann. "Cyberwar: Taking Stock of Security and Warfare in the Digital Age." International Studies Perspectives 17, no. 3 (2016): 343-360.
- Fanelli, Robert L. and Gregory J. Conti. “A methodology for cyber operations targeting and control of collateral damage in the context of lawful armed conflict.” 2012 4th International Conference on Cyber Conflict (CYCON 2012) (2012): 1-13.
- Fanelli, R. “Cyberspace Offense and Defense.” Journal of Information Warfare 15, no. 2 (2016): 53–65. https://www.jstor.org/stable/26487531.
- Fischerkeller, Michael P., and Richard J. Harknett. “Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation.” The Cyber Defense Review, 2019, 267–87.
- Fidler, David P. "Cyberspace, Terrorism and International Law." Journal of Conflict and Security Law 21, no. 3 (Winter 2016): 475–493.
- Foote, Colin, et al. "CYBER CONFLICT AT THE INTERSECTION OF INFORMATION OPERATIONS." Information Warfare in the Age of Cyber Conflict (2020).
- Frederick T. Sheldon, G. Peterson, A. Krings, R. Abercrombie, A. Mili. Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies. April 13, 2009.
- Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." International Security 38, no. 2 (2013): 41-73.
- Gatlan, Sergiu. "Microsoft: State-backed Hackers Are Targeting the 2020 US Elections: https://www.bleepingcomputer.com/news/security/microsoft-state-backed-hackers-are-targeting-the-2020-us-elections/.
- Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. "A retrospective impact analysis of the WannaCry cyberattack on the NHS." npj Digital Medicine 2, Article number: 98 (2019). https://www.nature.com/articles/s41746-019-0161-6.
- Giles, Keir. ““Information Troops” - A Russian Cyber Command?” 2011 3rd International Conference on Cyber Conflict (2011): 1-16.
- Gioe, David V.. “Cyber operations and useful fools: the approach of Russian hybrid intelligence.” Intelligence and National Security 33 (2018): 954 - 973.

- Glaser, Charles L., and Chaim Kaufmann. "What Is the Offense-Defense Balance and How Can We Measure It?" Belfer Center for Science and International Affairs.
- Glaser, Charles L., and Chaim Kaufmann. “What Is the Offense-Defense Balance and How Can We Measure It?” International Security 22, no. 4 (1998): 44–82.
- Goel, Sanjay. “Cyberwarfare: connecting the dots in cyber intelligence.” Commun. ACM 54 (2011): 132-140.
- Goldsmith, Jack, and Tim Wu. Who Controls the Internet?: Illusions of a Borderless World. Oxford: Oxford University Press, 2006.
- Gomez, Miguel Alberto, and Christopher Whyte. "Unpacking Strategic Behavior in Cyberspace: A Schema-Driven Approach." Journal of Cybersecurity 8, no. 1 (2022).
- Gordon, L.A., M.P. Loeb, and W. Lucyshyn, et al. "The Impact of Information Sharing on Cybersecurity Underinvestment: A Real Options Perspective." Journal of Accounting and Public Policy 34, no. 5 (2015): 509–519.
- Green, Travis. 2023. "Threat Hunting Rules." Threat Hunting Rules on GitHub.
- Greenberg, Andy. "How Russian Hackers Aimed at Viasat, Causing Chaos in Ukraine and Beyond." MIT Technology Review, May 10, 2022. https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.
- Greenberg, Andy. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers. Anchor Books, 2020.
- Greenberg, Andy. "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine." Wired, April 12, 2022.
- Graber, Scott. "Defend Forward: Adapting Offense and Defense Strategy to Cyberspace." Yale Cyber Leadership Forum, 20 luglio 2021.
- Halevi, T., Memon, N., Levis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F., e Chen, J. "Cultural and Psychological Factors in Cyber-Security." 2017.
- Hammond, T. H. “Why Is the Intelligence Community So Difficult to Redesign? Smart Practices, Conflicting Goals, and the Creation of Purpose-Based Organizations.” Governance, vol. 20, 2007, pp. 401-422.
- Harknett, Richard J., and Max Smeets. “Cyber campaigns and strategic outcomes.” Journal of Strategic Studies, vol. 45, no. 4, pp. 534–567, Jun. 2022, publisher: Routledge eprint: https://doi.org/10.1080/01402390.2020.1732354.
- Healey, Jason and Neil Jenkins. “Rough-and-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing.” 2019 11th International Conference on Cyber Conflict (CyCon) 900 (2019): 1-20.
- Healey, Jason, Patricia Mosser, Katheryn Rosen, and Alexander Wortman. 2021. "The ties that bind: A framework to assess the linkage between cyber risks and financial stability." Journal of Financial Transformation 53: 94-107. Capco Institute.
- Heuvel, Elly Van Den, e Gerben Klein Baltink. "Coordination and Cooperation in Cyber Network Defense: The Dutch Efforts to Prevent and Respond." In Best Practices in Computer Network Defense: Incident Detection and Response, 35, 121. 2014.
- Hegel, T. "Chinese Threat Actor Scarab Targeting Ukraine." March 2022. https://www.sentinelone.com/labs/chinese-threat-actor-scarab-targeting-ukraine/.
- Hernandez-Ardieta, J. L., Tapiador, J., and Suarez-Tangil, Guillermo. "Information Sharing Models for Cooperative Cyber Defence." Paper presented at the 2013 5th International Conference on Cyber Conflict (CYCON 2013), June 4.
- Hofstede, Geert. Culture's consequences: International differences in work-related values. Vol. 5. sage, 1984.

- Holubčík, Martin, Jakub Soviar, and Viliam Lendel. 2023. "Through Synergy in Cooperation towards Sustainable Business Strategy Management" Sustainability 15, no. 1: 525. https://doi.org/10.3390/su15010525.
- Huntley, S. "An Update on the Threat Landscape." March 2022. https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/.
- Hutchins, Eric Michael, Michael J. Cloppert and Rohan M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." (2010).
- Hutchins, E. M., M. J. Cloppert, and R. M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," 2011.
- Iasiello, Emilio. "What is the Role of Cyber Operations in Information Warfare?", Journal of Strategic Security 14, no. 4 (2021): 72-86.
- Jacobsen, Jeppe T. "Cyber offense in NATO: challenges and opportunities." International Affairs 97, no. 3 (May 2021): 703-720.
- Jasper, Scott. Strategic Cyber Deterrence: The Active Cyber Defense Option. Rowman & Littlefield, 2017.
- Jensen, Benjamin. "The Cyber Character of Political Warfare." Brown Journal of World Affairs 24, no. 1 (Fall/Winter 2017–18): 159–171.
- Jiang, Chaoyi. "Decoding China's Perspectives on Cyber Warfare." Chinese Journal of International Law 20, no. 2 (June 2021): 257–312.
- Johnson, Emily, Michael Brown, and Sarah Davis. 2020. Enhancing Cyber Defense Coordination through Integrated Command and Control Systems. Boston: Tech Defense Press.
- Kahana, Ephraim. "Israeli Intelligence: Organization, Failures, and Successes." In The Oxford Handbook of National Security Intelligence, edited by Loch K. Johnson, Oxford Handbooks, 2010; online edn, Oxford Academic, 2 Sept. 2010.
- Känzig, Nicolas, Roland Meier, Luca Gambazzi, Vincent Lenders, and Laurent Vanbever. 2019. "Machine Learning-based Detection of C&C Channels with a Focus on the Locked Shields Cyber Defense Exercise." In Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon), 900:1–19. IEEE.
- Katagiri, Nori. "Two explanations for the paucity of cyber-military, cross-domain operations." Journal of Cybersecurity 8, no. 1 (2022).
- Katagiri, Nori. "Why international law and norms do little in preventing non-state cyber attacks." Journal of Cybersecurity 7, no. 1 (2021).
- Keir, G. "Putin Does Not Need to Invade Ukraine to Get His Way." December 2021. https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way.
- Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." International Security 38, no. 2 (2013): 7-40.
- Kello, Lucas. "The Virtual Weapon and International Order." Yale University Press, 2017.
- Klein, Jan, Sandjai Bhulai, Mark Hoogendoorn, Rob Van Der Mei, and Raymond Hinfelaar. 2018. "Detecting Network Intrusion Beyond 1999: Applying Machine Learning Techniques to a Partially Labeled Cybersecurity Dataset." In Proceedings of the 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), 784-787.
- Knox, MacGregor, and Williamson Murray, eds. The Dynamics of Military Revolution, 1300–2050. Cambridge: Cambridge University Press, 2001.
- Kont, Markus, Mauno Pihelgas, Kaie Maennel, Bernhards Blumbergs, and Toomas Lepik. 2017. "Frankenstack: Toward Real-Time Red Team Feedback." In MILCOM 2017 - 2017 IEEE Military Communications Conference, 400–405.

- Kott, Alexander, and Paul Theron. 2020. "Doers, Not Watchers: Intelligent Autonomous Agents Are a Path to Cyber Resilience." IEEE Security & Privacy 18 (3): 62–66.
- Kott, Alexander, Paul Théron, Martin Drašar, Edlira Dushku, Benoît LeBlanc, Paul Losiewicz, Alessandro Guarino, Luigi Mancini, Agostino Panico, Mauno Pihelgas, Krzysztof Rzadca, and Fabio De Gaspari. 2023. "Autonomous Intelligent Cyber-Defense Agent (AICA) Reference Architecture. Release 2.0."
- Kott, Alexander, Paul Théron, Martin Drašar, Edlira Dushku, Benoît LeBlanc, Paul Losiewicz, Alessandro Guarino, Luigi Mancini, Agostino Panico, Mauno Pihelgas, et al. 2018. "Autonomous Intelligent Cyber-Defense Agent (AICA) Reference Architecture. Release 2.0." arXiv preprint arXiv:1803.10664.
- Krepinevich, Andrew F. "Cavalry to Computer: The Pattern of Military Revolutions." The National Interest, no. 37 (Fall 1994): 30-42.
- Krepinevich, Andrew F. "The Unfinished Revolution in Military Affairs." Issues in Science and Technology 19, no. 4 (2003): 58-66.
- Kushner, David. "The Real Story of Stuxnet." IEEE Spectrum 50, no. 3 (2013): 48-53.
- Lakshmanan, Ravie. “APT29 Exploited a Windows Feature to Compromise European Diplomatic Entity Network.” The Hacker News, 9 November 2022.
- Lakshmanan, Ravie. "New Russian-Backed Gamaredon's Spyware Variants Targeting Ukrainian Authorities." Hacker News, Feb 02, 2023. https://thehackernews.com/2023/02/new-russian-backed-gamaredons-spyware.html.
- Lakshmanan, Ravie. “Another Chinese Hacking Group Spotted Targeting Ukraine Amid Russia Invasion.” Section: Article. https://thehackernews.com/2022/03/another-chinese-hacking-group-spotted.html.
- Lashkari, Arash Habibi. 2018. "CICFlowMeter-V4.0 (formerly known as ISCXFlowMeter) is a Network Traffic Bi-flow Generator and Analyser for Anomaly Detection." Accessed August 2018.
- Lashkari, Arash Habibi, Gerard Draper Gil, Mohammad Mamun, and Ali Ghorbani. 2016. "Characterization of Encrypted and VPN Traffic Using Time-Related Features." February 2016.
- Lilli, Eugenio. "How Can We Know What We Think We Know about Cyber Operations?" Journal of Global Security Studies 8, no. 2 (June 2023).
- Lin, Herbert, and Jaclyn Kerr. "On Cyber-Enabled Information Warfare and Information Operations." In The Oxford Handbook of Cyber Security, edited by Paul Cornish. Oxford Handbooks, 2021; online edn, Oxford Academic, December 8, 2021.
- Lindsay, Jon R. “Stuxnet and the Limits of Cyber Warfare.” Security Studies 22, no. 3 (2013): 365-404.
- Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction.” International Security 39, no. 3 (2014/2015): 7-47.
- Lindsay, Jon R., and Lucas Kello. “Correspondence: A Cyber Disagreement.” International Security 39, no. 2 (2014): 181-207.
- Linvill, Darren L., Brandon C. Boatwright, Will J. Grant and Patrick L. Warren. “"THE RUSSIANS ARE HACKING MY BRAIN!" investigating Russia's internet research agency twitter tactics during the 2016 United States presidential campaign.” Comput. Hum. Behav. 99 (2019): 292-300.
- Liu, M. "Inter-temporal Incentives in Security Information Sharing Agreements." In Workshops at the Thirtieth AAAI Conference on Artificial Intelligence, 1-8. La Jolla, CA, March 2016.
- Malsilo. 2023. "Threat Hunting Rules." Malsilo Rules on GitLab.

- Mandiant Analysts: Russia-backed APTs Likely to Ramp up Attacks." Computer Weekly. https://www.computerweekly.com/news/252512299/Mandiant-analysts-Russia-backed-APTs-likely-to-ramp-up-attacks.
- Mazarr, Michael J., Bryan Frederick, Emily Ellinger, and Benjamin Boudreaux. Competition and Restraint in Cyberspace: The Role of International Norms in Promoting U.S. Cybersecurity. Santa Monica, CA: RAND Corporation, 2022.
- McNeil, Jeff J. 2010. "Maturing International Cooperation to Address the Cyberspace Attack Attribution Problem." Doctor of Philosophy (PhD), Dissertation, Political Science & Geography, Old Dominion University.
- Meyer, E. (2014). The culture map: Breaking through the invisible boundaries of global business. Public Affairs.
- Microsoft. "An Overview of Russia's Cyberattack Activity in Ukraine." Tech. Rep., 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
- Miller, M. "Russian Invasion of Ukraine Could Redefine Cyber Warfare." January 2022. https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051.
- Molina, Ricardo Misael Ayala, Sadegh Torabi, Khaled Sarieddine, Elias Bou-Harb, Nizar Bouguila and Chadi M. Assi. "On Ransomware Family Attribution Using Pre-Attack Paranoia Activities." IEEE Transactions on Network and Service Management
- Moore, Daniel. Offensive Cyber Operations: Understanding Intangible Warfare. Oxford: Oxford University Press, 2022.
- Morgan, Adam S., and Steve W. Stone. 2019. "Command and Control for Cyberspace Operations - A Call for Research." Military Cyber Affairs 4, no. 1 (Article 4).
- Moses, Joel. "Political Rivalry and Conflict in Putin's Russia." Europe-Asia Studies 69 (2017): 961 - 988.
- Mueller, Milton L. "Against Sovereignty in Cyberspace." International Studies Review, Volume 22, Issue 4, December 2020, Pages 779–801.
- Mustang Panda, TA416, RedDelta, BRONZE PRESIDENT, Group G0129." MITRE ATT&CK®. https://attack.mitre.org/groups/G0129/
- Nakasone, Paul M. 'A Cyber Force for Persistent Operations.' In Joint Force Quarterly 92, no. 1 (1st Quarter, 2019).
- National Security Archive. 'The CIA and Signals Intelligence.' Last modified March 20, 2015. https://nsarchive.gwu.edu/briefing-book/cyber-vault-intelligence/2015-03-20/cia-and-signals-intelligence
- Nocetti, Julien. "Review of The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age, by Adam Segal, and Internet Wars: The Struggle for Power in the 21st Century, by Fergus Hanson." International Affairs 92, no. 5 (2016): 1263–1266.
- Nye, Joseph S. "Public Diplomacy and Soft Power." The Annals of the American Academy of Political and Social Science 616 (2008): 94–109. http://www.jstor.org/stable/25097996.
- Ostrow, Joel M.. "Conflict-Management in Russia's Federal Institutions." Post-Soviet Affairs 18 (2002): 49 - 70.
- Park, So-Hyun, Sun-Woo Yun, So-Eun Jeon, Na-Eun Park, Hye-Yeon Shim, Yu-Rim Lee, Sun-Jin Lee, Tae-Rim Park, Na-Yeon Shin, Min-Jin Kang, and Il-Gu Lee. 2022. "Performance Evaluation of Open-Source Endpoint Detection and Response Combining Google Rapid Response and Osquery for Threat Detection." IEEE Access: 20259–20269.
- Paxson, Vern. 1999. "Bro: A System for Detecting Network Intruders in Real-Time." Computer Networks 31, no. 23-24: 2435-2463.
- Persoglia, Davide. "Between Defence and Offence: An Analysis Of The US' Cyber Strategic Culture.", 2018.

- Pinto, C. Ariel, e Matthew Zurasky. "Systemic Methodology for Cyber Offense and Defense." In Proceedings of the 15th International Conference on Cyber Warfare and Security: ICCWS 2020, 380-390. 12-13 Marzo 2020, Norfolk, Virginia. Academic Conferences & Publishing International Limited, 2020.
- Priebe, Miranda, Douglas C. Ligor, Bruce McClintock, Michael Spirtas, Karen Schwindt, Caitlin Lee, Ashley L. Rhoades, Derek Eaton, Quentin E. Hodgson, e Bryan Rooney. "Multiple Dilemmas: Challenges and Options for All-Domain Command and Control." RAND Corporation, 2020.
- Pynnöniemi, Katri. "Information-psychological warfare in Russian security strategy." Routledge Handbook of Russian Security (2019).
- Raggi, M. "The Good, the Bad, and the Web Bug: TA416 Increases Operational Tempo Against European Governments as Conflict in Ukraine Escalates." Proofpoint US, March 2022. https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european.
- Ravie, L. "Another Chinese Hacking Group Spotted Targeting Ukraine Amid Russia Invasion." Section: Article. https://thehackernews.com/2022/03/another-chinese-hacking-group-spotted.html.
- Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." Paper presented at the International Studies Association Annual Convention, San Diego, CA, April 1, 2012.
- Reykers, Yf, John Karlsrud, Malte Brosig, Stephanie C Hofmann, Cristiana Maglia, and Pernille Rieker. "Ad hoc coalitions in global governance: short-notice, task- and time-specific cooperation." International Affairs 99, no. 2 (March 2023): 727–745.
- Rid, Thomas. "Cyber War Will Not Take Place." Journal of Strategic Studies 35, no. 1 (2012): 5-32.
- Rid, Thomas. "The Challenges of Cyberwarfare." RUSI Journal 157, no. 5 (2012): 22-29.
- Rid, Thomas. 2013. Cyber War Will Not Take Place. Oxford: Oxford University Press.
- Rollins, John W. and Clay Wilson. "Terrorist Capabilities for Cyberattack: Overview and Policy Issues." (2005).
- Sanger, David E. "12. A New Age Of Cyberwarfare" In Journalism After Snowden: The Future of the Free Press in the Surveillance State edited by Emily Bell and Taylor Owen, 186-196. New York Chichester, West Sussex: Columbia University Press, 2017. https://doi.org/10.7312/bell17612-015
- Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance." Contemporary Security Policy 34, no. 1: 40-41.
- Schneier, Bruce. "The Threat of Cyber War Has Been Grossly Exaggerated." CNN, July 31, 2012.
- Schmitt, Michael N. "Rewired Warfare: Rethinking the Law of Cyber Attack." International Review of the Red Cross 96, no. 893 (2014): 189-206.
- Schoka, Andrew. "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat." War on the Rocks, April 3, 2019. https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/.
- Scroxton, Alex. "Sandworm rolls out Industroyer2 malware against Ukraine." ComputerWeekly.com. April 12, 2022
- Scroxton, A. "Mandiant Analysts: Russia-backed APTs Likely to Ramp up Attacks." Computer Weekly.
- Segal, Adam. "The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age." PublicAffairs, 2016.

- Segal, Adam. “Why Digital Pearl Harbor Makes Sense...and Is Possible.” Carnegie Endowment for International Peace, 2017.
- Sepielli, Andrew. "Cooperation." Stanford Encyclopedia of Philosophy. Stanford University, 2021.
- Shackelford, Scott J., Michael Sulmeyer, Amanda N. Craig, Ben Buchanan and Brian Micic. “From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do about It.” Conflict Studies: Terrorism eJournal (2017).
- Sharafaldin, Iman, Arash Habibi Lashkari, and Ali Ghorbani. 2018. "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization." 108-116.
- Sharafaldin, Iman, Arash Habibi Lashkari, and Ali Ghorbani. 2018. "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization." Pages 108–116. January 2018.
- Smeets, Max. "A Matter of Time: On the Transitory Nature of Cyberweapons." Journal of Strategic Studies 41, no. 1-2 (2018): 6-32.
- Smeets, Max. "Cyber Arms Transfer: Meaning, Limits, and Implications." Security Studies 31, no. 1 (January 2022): 65–91. https://doi.org/10.1080/09636412.2022.2041081. Publisher: Routledge.
- Smeets, Max. “The Strategic Promise of Offensive Cyber Operations.” Strategic Studies Quarterly 12, no. 3 (2018): 90–113.
- Smeets, Max. 2022. No Shortcuts: Why States Struggle to Develop a Military Cyber-Force. London: Hurst.
- Smeets, Max, and Richard J. Harknett. “Cyber Campaigns and Strategic Outcomes.” Journal of Strategic Studies, 2022.
- Smith, John, and Priya Patel. 2019. The Role of International Cyber Alliances in Improving Defense Posture. New York: Cybersecurity Publishing.
- Smeets, Max, and Richard J. Harknett. “Cyber campaigns and strategic outcomes,” Journal of Strategic Studies, vol. 45, no. 4, pp. 534–567, Jun. 2022, publisher: Routledge eprint: https://doi.org/10.1080/01402390.2020.1732354.
- Stamus Networks. 2023. "Stamus Networks Lateral Movement Rules." Stamus Rules on Their Website.
- Staar, Richard Felix and Corliss Anne Tacosa. “Russia's Security Services.” Mediterranean Quarterly 15 (2004): 39 - 57.
- Štrucl, Damjan. “Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare.” CONTEMPORARY MILITARY CHALLENGES/SODOBNI VOJAŠKI IZZIVI 24 (2022): 103 - 123.
- Taillat, Stéphane and Frédérick Douzet. “Collective security and strategic instability in the digital domain.” Contemporary Security Policy 40 (2019): 362 - 367.
- Tanmay, K. “DECODED - Did China Help Moscow Hack Ukraine & Share Critical Intelligence Before The Russian Invasion?” Apr.2022. [Online]. Available: https://eurasiantimes.com/decoded-did-china-help-moscow-hack-ukraine-russian-invasion/
- Teraoka, A. "Chinese Hackers Launch Cyberattacks Against Ukraine Amid War." https://asia.nikkei.com/Politics/Ukraine-war/Chinese-hackers-launch-cyberattacks-against-Ukraine-amid-war.
- Tiepolo, Gianluca. "Russian APT 'Gamaredon' Exploits Hoaxshell to Target Ukrainian Organizations." Medium, February 14, 2023.
- Thornton-Trump CD, Ian. “RUSSIA: THE CYBER GLOBAL PROTAGONIST.” EDPACS 65 (2022): 19 - 26.

- Truong, Thanh Cong, Quoc Bao Diep, e Ivan Zelinka. "Artificial Intelligence in the Cyber Domain: Offense and Defense." Symmetry 12, no. 3 (2020): 410.
- Turkaeva, Laura. “Federal Security Service in the national security system.” (2020).
- Uramová, Jana, Pavel Segeč, Marek Moravčík, Jozef Papán, Tomáš Mokoš, and Marek Brodec. 2017. "Packet Capture Infrastructure Based on Moloch." In Proceedings of the 2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA), 1–7. IEEE.
- Valeriano, Brandon, and Benjamin Jensen. “The Myth of the Cyber Offense: The Case for Restraint.” Policy Analysis no. 862, Cato Institute, January 15, 2019.
- Valeriano, Brandon, and Ryan C. Maness. “The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11.” Journal of Peace Research 51, no. 3 (2014): 347-360.
- Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. Cyber Strategy: The Evolving Character of Power and Coercion. Oxford: Oxford University Press, 2018.
- Valeriano, Jensen, and Maness, Cyber Strategy, 2018.
- Van Creveld, Martin. The Transformation of War. New York: Free Press, 1991.
- Ventre, Daniel, ed. Cyberwar and Information Warfare. John Wiley & Sons, 2012.
- Vicic, J., and R. N. Metha. "Why Russian Cyber Dogs Have Mostly Failed to Bark." March 2022. https://warontherocks.com/2022/03/why-cyber-dogs-have-mostly-failed-to-bark/.
- Vyas, K. “China accused of hacking Ukraine days before Russian invasion,” The Times, Mar. 2023. [Online].
  Available: https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf.
- Wadhwani, S. "Russian Darknet Forum RAMP Reemerges With Chinese-speaking Hackers At the Wheel. https://www.spiceworks.com/tech/security/news/russian-darknet-forum-ramp-reemerges-with-chinese-speaking-hackers-at-the-wheel/.
- Waters, Rob. "APT29 using Windows Credential Roaming bug to target diplomats. Mandiant finds APT29 increahttps://www.cybercareers.blog/2022/11/apt29-using-windows-credential-roaming-bug-to-target-diplomats/singly targeting NATO and its allies in 2022." Cybercareers, 10 November 2022.
- Warner, Michael. “Cybersecurity: A Pre-history.” Intelligence and National Security 27, no. 5 (2012): 781-799.
- Weaver, Nicholas. "Shadow Brokers Redux: Dump of NSA Tools Gets Even Worse." Lawfare April 14, 2017.
- Wiener, Craig. “Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation.” (2016).
- Wilner, A. S., et al. "Offensive Cyber Operations and State Power: Lessons from Russia in Ukraine," International Journal, no. 0 (2024).
- World’s Most Dangerous Malware EMOTET Disrupted Through Global Action." Europol. Accessed January 27, 2021.
- Wright, Steve. "Cyberwarfare, Netwar & The Revolution in Military Affairs." In Edited by Halpin, E., Webb, D., Trevorrow, P., and Wright, S., Palgrave, 2006.
- Zhang, Wei, and Li Wang. 2021. Blockchain and Cybersecurity: A Symbiotic Relationship. San Francisco: Blockchain Security Institute.
- Zhang, Wei, and Li Wang. 2021. Blockchain and Cybersecurity: A Symbiotic Relationship. San Francisco: Blockchain Security Institute.
- Zoller, Richard G.. “Russian Cyberspace Strategy and a Proposed United States Response.” (2010).