ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies

Cosimo Melella | CCDCOE, Tallinn, Republic of Estonia, University of Genoa, Italy| ORCID: 0009-0009-6970-9396

Francesco Ferazza | Royal Holloway, University of London, UK | ORCID 0009-0005-3280-2678

Konstantinos Mersinas | Royal Holloway, University of London, UK | ORCID 0000-0002-4402-2987

Received: 11.06.2024

Accepted: 07.08.2024

Published: 06.09.2024

Cite this article as:
C. Melella, F. Ferazza, K. Mersinas "Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies," ACIG, vol. 3, no. 2, 2024, pp. 38–71. DOI: 10.60097/ACIG/192120

Corresponding author:
Cosimo Melella, CCDCOE, Tallin, Republic of Estonia and University of Genoa, Italy; E-mail: cosimo.melella@ccdcoe.org
0009-0009-6970-9396

Abstract

Our ongoing, descriptive study explores the intricacies of Offensive Cyber Operations (OCOs), particularly in the context of the Russian-Ukrainian conflict that began in 2022. This conflict has underscored an escalation in Russian cyber capabilities. Despite OCOs playing a role, academic research indicates a relatively limited 'spillover effect'. Our study aims to investigate this limited spillover, focusing on the lack of collaboration among Advanced Persistent Threat (APT) groups associated with Russian intelligence agencies: GRU, SVR, and FSB. By analysing the operational and technical integration among these agencies, we seek to identify factors influencing cooperation. Preliminary findings suggest that internal competition and historical disparities may have hindered effective coordination in cyber operations. We posit that this lack of coordination could potentially reduce cyberattack effectiveness and increase detection likelihood. Importantly, we recognise that behavioural aspects, such as the principal-agent problem, may contribute to the barriers preventing collaboration and coordination. These behavioural factors, alongside institutional rivalries, likely play a significant role in shaping the competitive dynamics among

Russian intelligence agencies. As our research progresses, we aim to explore the implications of this internal rivalry on the development of technical infrastructure for Russia-affiliated APT groups. We anticipate that our findings illuminate the reasons behind the apparent reduced effectiveness of cyberattacks in this scenario. This exploration of competitive dynamics, historical nuances, and behavioural factors within Russian intelligence agencies is crucial for a comprehensive understanding of the broader cyber operations landscape. We present this paper as a work in progress, aiming to contribute to the ongoing discourse in this field.

Keywords

cyber threat, intelligence, APTs, coordination, cooperation

1. Introduction

According to Damjan Štrucl, the role of Offensive Cyber Operations (OCOs) in modern conflicts has been notably heightened by the Russian invasion of Ukraine on February 24, 2022. Prior analyses, drawing from precedents like Stuxnet and NotPetya, had projected a significant impact of cyber warfare, particularly through malware distribution with potential repercussions extending beyond the immediate conflict zone to affect other nations and organisations. This expectation was underpinned by the recognition of Russia's formidable cyber capabilities. Yet, the unfolding of events presented a striking puzzle: contrary to widespread predictions, the Russian OCOs manifested limited effects on the war's outcome. This discrepancy was highlighted in several assessments that questioned the anticipated dominant role of cyber operations in the conflict. On the one hand, forecasts had envisioned a scenario where cyber operations would play a pivotal role in the warfare strategy; on the other, post-event analyses and reports underscored the surprisingly marginal impact of these operations. This apparent paradox suggests a lack of coordination among Russian intelligence agencies as a plausible explanation [1]. These empirical observations introduce a theoretical quandary: How can coordination be managed or integrated within OCOs? This is a work in progress and presents an exploratory study into a complex theoretical challenge: understanding the dynamics of coordination within OCOs, particularly in the context of Russian intelligence agencies. The study identifies a crucial observation that GRU, SVR, and FSB [2] are indeed distinct entities, each operating with unique strategies, technologies, and protocols. This differentiation is not merely organisational but extends to their approach to

cyber operations. The real puzzle, as underscored by our research, lies in the evident challenge these organisations face in coordinating their activities effectively, despite their established distinctiveness. This lack of coordination presents a significant inquiry into why these entities, known for their respective capabilities, do not achieve a unified and cohesive operational front in cyber warfare. A key observation driving this inquiry is the apparent limited effectiveness of Russian OCOs, attributed primarily to a shortfall in operational and technical integration among these agencies. This lack of coordination, especially among various advanced persistent threats (APTs), forms the central theme of our investigation. Our approach to exploring this issue is two-fold. Initially, we delve into the notion of integration at both technical and operational levels within intelligence agencies active in cyber defence. Subsequently, we empirically analyse this concept within the framework of Russia's intelligence system. This analysis aims to illuminate the roles of internal competition and political rivalry among these agencies and how these factors might influence state-sponsored cyber threats [3]. This paper aims to contribute to the broader debate on state-sponsored cyber operations. By focusing on the possible reasons for the observed lack of coordination among different hacking groups purportedly connected to Russia, the study offers insights into the impact of internal dynamics – such as competition and rivalry within the Russian government and intelligence sectors – on the nature and structure of state-affiliated cyber threats. This perspective is novel and adds a valuable dimension to our understanding of state-sponsored cyber activities. 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 [4]. Such a situation can lead to 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 [5] 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, acknowledging the historical backdrop of inter-agency rivalry in Russia, particularly between the FSB and the GRU, sheds light on the complexities of coordination within its intelligence framework. Incidents such as GRU's involvement in the 2014 Crimea annexation and the handling of Sergei Skripal's poisoning in 2018 have highlighted this friction, with the FSB expressing dissatisfaction over perceived oversteps by GRU. This longstanding political rivalry among Russia's intelligence entities, including the SVR, prior to the 2022 Ukraine conflict, suggests that the observed

lack of coordination and integration during the war was, in retrospect, an anticipated outcome. Consequently, the initial expectations of a significant cyber offensive impact, akin to spillover effects seen in previous global cyber incidents, may have overlooked the practical implications of these internal dynamics, thereby contributing to the re-evaluation of the puzzle surrounding Russia's cyber operations effectiveness [6]. The landscape of inter-agency competition, compounded by political rivalries, is full of challenges. This unstable dynamic environment can induce uncertainty and instability, hampering operational and strategic coordination. To illustrate this environment, tension has been observed within the Russian intelligence community, particularly between the FSB and the GRU, due to alleged excesses of jurisdiction and operational abuse. This study adds to the talk of state-sponsored cyber operations by providing an explanatory lens for coordination deficiencies observed among hacking groups allegedly linked to Russia [7]. Furthermore, we seek to answer two central research questions (RQs) regarding the degree of integration between cyber defence agencies' operational and technical/tactical levels and the factors contributing to any observed lack of integration:

- RQ1: To what extent does integration occur between the technical and operational divisions within intelligence agencies when executing government-offensive policies in cyberspace?
- RQ2: What factors impede the integration between technical and operational divisions within intelligence agencies in the implementation of government-offense strategies in cyberspace?

In doing so, we emphasise the critical role of the technical and operational 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 can lead to a significant disconnect between strategic objectives and their operational execution. This disjunction often stems from the divergence between technical capabilities and operational planning – wherein the technological approaches do not align with operational plans. Such misalignment threatens to widen the gap between what is strategically decided and what is practically implemented, resulting in technical inefficiencies, leading to operational inefficacies [8]. Our 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. 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 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 [9]. 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 technical and operational levels. We hope to contribute to the broader discourse on offensive state-sponsored cyber operations through this lens. The methodology used to answer RQs and better understand such operations is multifaceted, in the following order:

- We conduct a literature review on cyber operations, intelligence agency structures, and inter-agency dynamics.
- We analyse open-source intelligence (OSINT) data related to Russian cyber activities during the Ukraine conflict.
- We employ a case study approach, examining the activities of three main Russian intelligence agencies: GRU, SVR, and FSB, along with their associated APTs.
- We analyse the tactics, techniques, and procedures (TTPs) of specific APTs linked to these agencies, such as Sandworm, Fancy Bear, Cozy Bear, Turla, Callisto, and Gamaredon.

2. The Challenges of Coordination

In the complex landscape of OCO, the effective management of challenges heavily relies on the robust establishment of cooperation and coordination principles. Cooperation refers to sharing resources, information, or skills to achieve common goals or tackle shared challenges. Coordination refers to the organisation of the efforts of the various actors, aimed at ensuring the efficient and effective achievement of the shared objectives. At the strategic level, which involves long-term planning and decision-making aimed at achieving overarching goals, cooperation is the key. It involves a concerted effort among various organisations and entities, bridging their resources and capabilities. This level of

operation is crucial in conflict situations, requiring not just strong political determination but also a unified strategic vision to address broad, often long-term objectives. In contrast, coordination is critical at both operational and technical levels. The operational level refers to the execution of strategies, focusing on how different components of an organisation or entities work together to implement the strategic plan. This might involve day-to-day management of resources, decision-making regarding specific cyber operations, and real-time responses to evolving situations. The technical level, on the other hand, delves into the specificities of cyber warfare, dealing with the actual tools, tactics, and procedures used in cyber operations. It includes hands-on tasks, such as software development, system penetration, data analysis, and other technical aspects of cyber warfare. Coordination at this level ensures that the technical actions align with the strategic objectives and operational plans. It involves synchronising cyber operations, sharing crucial intelligence, and modifying tactics and techniques as needed to effectively counteract adversaries' defensive measures or react to their coordinated activities on the battlefield. Understanding and integrating these levels of operation is essential in managing the dynamic and intricate nature of cyber conflicts and the activities of APTs. Such an integrated approach ensures that strategic decisions are effectively translated into operational success and technical precision, a critical factor in the domain of OCOs. Referring to what has been written about the importance of coordination in OCO, the academic studies of McNeil [10], Hernandez-Ardieta, Tapiador, Suarez-Tangil [11], Heuvel, Baltink [12], and Liebetrau [13] provide further insights into this essentiality of coordination in cyberspace. These academic works reinforce the idea that to successfully face the challenges of cyberspace and effectively manage cyber operations; it is fundamental to establish solid principles of cooperation at the strategic level and coordination at all levels: strategic, operational, and technical. McNeil highlights the need for strategic international cooperation, emphasising how its absence can limit offensive and defensive capabilities in cyberspace. It reflects the importance of lower-level coordination among nations to achieve long-term objectives. The article by Hernandez-Ardieta, Tapiador, and Suarez-Tangil sheds light on the importance of information-sharing models for coordinated cyber defence, recognising the essentiality of coordination at the operational and technical levels to ensure alignment between technical actions and strategic objectives. Finally, Liebetrau, in his article, examines how different countries organise their cyber capabilities, identifying various organisational models and emphasising the importance of coordination between military and intelligence

entities, which is essential for addressing cyber conflicts. These studies emphasise that information sharing and coordination are crucial for improving operational capabilities and security in cyberspace. They highlight the importance of continuous efforts to develop effective frameworks, agreements, and protocols, ensuring that strategic decisions are translated into operational success and technical precision in OCOs. Coordination between different 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 [14]. Conversely, if the operation is aimed at stealth, cyber-espionage, or evasion of detection, it is more appropriate to target different targets simultaneously [15]. 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 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 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 [16]. 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 [17]. 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 cyberattack on the DNC. However, this lack of coordination may have led to overlooked opportunities or inefficiencies [18]. In recent decades, and before the invasion of Ukraine, Russia has leveraged sophisticated cyber capabilities to conduct

global disinformation campaigns, propaganda, espionage, and destructive cyberattacks. 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: GRU, SVR, and FSB [19]. The distribution of responsibilities between 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. 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, counterintelligence, and maintaining control over Russia's information space. However, the FSB has also been associated with OCOs, particularly those targeting dissidents, activists, and other alleged threats to 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 [20]. A brief graphical representation of this section is shown in Figure 1.

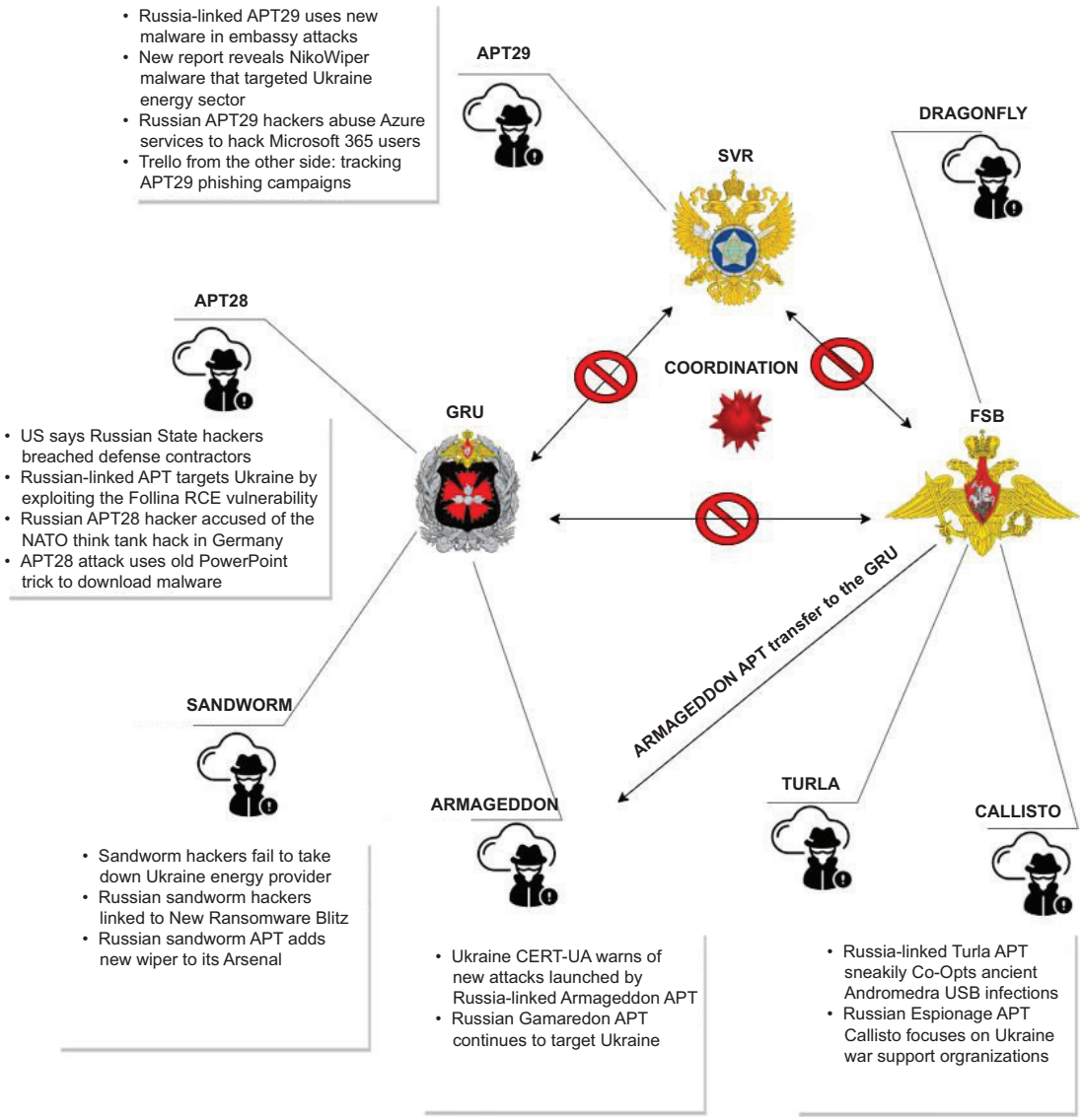

Figure 1. Coordination amongst Russian intelligence agencies and related APTs.

3. Factors Impacting Coordination

Coordination between technical and operational layers in cyberspace faces several challenges affecting the efficiency, security, and reliability of communication and collaboration. Firstly, 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 [21]. Furthermore, for the above reasons, coordination fails between intelligence agencies in cyberspace (for offensive or defensive purposes [22]). The lack of coordination between the operational and technical/tactical layers of these organisations can make it more challenging to carry out attacks with a destructive effect. The lack of coordination between operational and strategic levels among cyber threat groups can lead to counterproductive outcomes, significantly hampering their collective effectiveness. When these layers fail to share information and align their efforts, they risk not only diminishing the impact of their operations but also increasing the likelihood of detection by cyber security defences. This misalignment can result in operational redundancies, conflicting actions, undermining the overarching objectives of the cyber campaign. To enhance operational security and effectiveness, establishing robust communication channels and coordination mechanisms is essential, ensuring that all actions are synergistic and strategically aligned. 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 and share information creates technical limitations. This competition creates disjointed efforts, undermining the efficiency of cyberattacks. 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 [23]. 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 unauthorised access to targeted computer systems and networks [24]. 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 unauthorised access to targeted computer systems and networks. 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 [25]. On a technical level, the operators use various tools and techniques to gain unauthorised 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 key logging software, to capture passwords and other sensitive information or malware to monitor the target's activities and communications [26]. 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 cyber espionage operations require high technical and tactical sophistication and a deep understanding of the target's motivations, behaviours, and vulnerabilities. The integration of technical and operational levels is essential for the success of these operations and requires a high degree of skill and coordination between the operators involved.

4. Objectives, Skills, and Culture as Coordination Challenges

While intra-agency coordination remains achievable despite challenges in melding technical and operational levels, inter-agency collaboration presents a more complex scenario due to divergent organisational cultures, conflicting priorities, infrastructural disjunctions, and varying degrees of technical and operational expertise. These dynamics underscore the need for refined RQs that capture both internal and external integration facets within intelligence agencies' cyber operations. Thus, we propose an updated framing of RQs:

- RQ1: To what extent does integration occur between the technical and operational divisions within intelligence agencies, specifically

when executing government-offensive policies in cyberspace? This question aims to explore the depth and effectiveness of internal coordination efforts, shedding light on the synergy between technological innovations and operational strategies.

- RQ2: What factors impede the integration between technical and operational divisions within intelligence agencies, particularly in the context of implementing government-defensive strategies in cyberspace? This inquiry seeks to identify and analyse the barriers to effective collaboration, focusing on the internal dynamics that challenge the alignment of cyber defence objectives with operational execution. These updated questions aim to provide a comprehensive understanding of both internal integration within agencies and complexities of inter-agency cooperation, reflecting the multifaceted nature of cyber operations in the intelligence community [27]. 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 [28]. 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 modus operandi on how to approach the task [29]. Another challenge is that different agencies may have different technical and operational expertise levels. For example, one agency may be more proficient at developing and executing complex cyberattacks. At the same time, another may have skill sets for gathering information from various sources and deploying psychological operations [30].

5. The Principal-Agent Dynamic

Furthermore, there may be a disruption in the principal-agent dynamic between the technical/tactical 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 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 monitor closely the actions

of the agents, and agents have motivations which might not serve the principal's goals. In our 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 for 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 prioritising 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, that is, the agencies. Thus, in lack of a '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. In summary,

the principal-agent dynamic highlights significant coordination and information-sharing challenges within and between intelligence agencies operating APTs. These challenges stem from information asymmetries and conflicting interests, where technical teams may lack insight into broader strategic goals and decision-makers may not grasp operational technicalities. Such disparities hinder effective cooperation and can compromise operational success. Overcoming these obstacles requires improved communication, mutual understanding of goals and methodologies, and a commitment to aligning actions with overarching strategic objectives.

6. Cultural Differences

Different organisational 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 organisations, and, for our purposes, can indicate how differences in these dimensions can impair coordination between them. While there are many of these dimensions, proposed by different researchers [31, 32], 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 our purposes, we 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 organisational 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 (relationship-based trust), while the other group might find higher trust in performance, or a long successful career with achievements (task-based trust). Another important cultural aspect is that of leadership; some organisations 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 organisation can tolerate is also a very important dimension. Some organisations require everything to be normed, and deviation from these norms is often a cause of 'neuroticism', conflict, and confusion. Other organisations might be more flexible, being less focused on inflexible principles,

and more open to opportunity and change. Last, but not least, another relevant cultural aspect is that of decision-making; some organisations might favour a top-down approach, where leading individuals make decisions and impose these to subordinates, while others take a consensus-based approach. In the light of the above, it appears that motivations and access to information of agency entities in the form of principal-agent dynamics, or cultural differences between agencies, can amplify or diminish coordination challenges between agencies. In the next section, we present the case studies of GRU, SVR, and FSB, along with their indicative corresponding APTs. The choice to focus on GRU, SVR, and FSB agencies for the case study portion of our OCO study was driven by several significant factors. Firstly, the context of the recent Russian-Ukrainian conflict at the centre of this paper, which has seen a marked increase in Russian cyber capabilities, makes these agencies particularly relevant. The GRU, SVR, and FSB have been protagonists in various cyber operations in this context. These agencies have distinct but complementary roles in intelligence and cyber operations. The GRU deals primarily with military intelligence, the SVR with foreign intelligence, and the FSB with internal security and counter-intelligence. By analysing the interactions between these agencies, we can gain greater insight into Russia's internal dynamics in cyber operations. Another critical aspect is the historic competition and disparities between these agencies. These internal differences offer a rich context for exploring how they influence coordination and effectiveness in cyber operations. Understanding the causes of their lack of coordination can reveal key factors that hinder or facilitate greater cooperation. Furthermore, our analysis focuses on the impact of this lack of coordination on the effectiveness of cyber operations. If these agencies fail to coordinate effectively, this could reduce the impact of their cyberattacks and increase the likelihood of detection. By examining interactions at operational and technical levels, our study seeks to identify ways to improve the overall effectiveness of cyber operations. Through this study, we intend to deeply explore the competitive and historical dynamics of Russian intelligence agencies, which are crucial to a comprehensive understanding of the broader landscape of cyber operations. In the following sections we add succinct, top-level descriptions of TTPs employed by the analysed APTs, for they serve as valuable tools in understanding their behaviour and modus operandi.

7. The Agencies Case Studies

The choice to focus on the GRU, SVR, and FSB agencies for the case study portion of our OCO study was driven by

several significant factors. Firstly, the context of the recent Russian-Ukrainian conflict at the centre of this paper, which has seen a marked increase in Russian cyber capabilities, makes these agencies particularly relevant. The GRU, SVR, and FSB have been protagonists in various cyber operations in this context. These agencies have distinct but complementary roles in intelligence and cyber operations. The GRU deals primarily with military intelligence, the SVR with foreign intelligence, and the FSB with internal security and counter-intelligence. By analysing the interactions between these agencies, we can gain greater insight into Russia's internal dynamics in cyber operations. Another critical aspect is the historic competition and disparities between these agencies. These internal differences offer a rich context for exploring how they influence coordination and effectiveness in cyber operations. Furthermore, our analysis focuses on the impact of this lack of coordination on the effectiveness of cyber operations. If these agencies fail to coordinate effectively, this could reduce the impact of their cyberattacks and increase the likelihood of detection. By examining interactions at operational and technical levels, our study seeks to identify ways to improve the overall effectiveness of cyber operations. Through this study, we intend to deeply explore the competitive and historical dynamics of Russian intelligence agencies, which are crucial to a comprehensive understanding of the broader landscape of cyber operations. In the following sections we add succinct, top-level descriptions of TTPs employed by the analysed APTs, for they serve as valuable tools in understanding their behaviour and modus operandi.

7.1. 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 [33]. 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 Unit 26165 to numerous offensive operations against public and

private sector targets in the United States and Europe [34]. Then there is Unit 74455, which is linked to some of Russia's most brazen and damaging cyberattacks. Unit 74455 was identified as responsible for the coordinated release of stolen emails and documents during the 2016 US presidential election [35]. Focusing primarily on systems penetration and intelligence gathering, Unit 74455 appears to have a significant offensive cyber capability, including developing NotPetya malware that hit multiple targets in Ukraine in June 2017, then spread globally and caused significant damage outside Ukraine [36]. Finally, there is Unit 54777, also known as the 72nd Special Service Center, which would be responsible for GRU psychological operations, including online disinformation campaigns [37].

(1) *Sandworm:* 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 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 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 neutralised in the early stages, and the second blackout researchers expected from Sandworm after targeting Ukraine's power supply in 2015 and 2016 never occurred [38]. 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 organisations affected. According to reports, Industroyer2 has been customised 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 [39]. 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 5-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 [40]. 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 organisations. Reports indicate that the exploited .NET malware is new and distributed similarly to previous campaigns linked to GRU. The ransom note (SullivanDecryptsYourFiles[.]txt) shows the authors impersonating James P. Sullivan, one of the main characters in the Pixar film Monsters & 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 attack s 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 [41]. 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 organisations 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 these tools together with POWERGAP is attributed – at the time of writing – to APT28 too, which, like Sandworm, would be under the control of GRU [42].

(2) *Fancy Bear:* The cyber espionage 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, and dissidents at the present Russian government. In recent years, Russia appears to have been using 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, whichis then leaked for other political narratives aligned with Russian interests [43]. These have included the conflict in Syria, NATO–Ukraine relations, the European Union (EU) refugee and migrant crisis, and the 2016 US presidential election [44]. 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 calculatedly propagated, almost certainly intended to further particular objectives of the Russian government [45]. In a report published on January 7, 2017, the US Office of the Director of National Intelligence (ODNI) [46] 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 modernised 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 cyberattacks against the Ukrainian government, including military targets and critical infrastructure, as well as disinformation campaigns designed to influence public opinion in the country [35]. 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, 2022, CERT-UA issued an alert highlighting that UAC-0028, the name CERT-UA gave APT28, was phishing UkrNet accounts. On March 4, 2022, 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, 2022, Fancy Bear was then observed targeting its victims with a new variant of infostealer malware, distributed via email attachments, while on May 6, 2022, 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 HTTPPOST requests to *.m.pipedream[.]nethostnames [47]. 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 (e.g. 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 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 organisations as early as December 2021 [48].

7.2. 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.[1] Most analysts conclude that SVR operates forcefully, emphasising secrecy and detection avoidance [49]. Most cyber operations related to the SVR focus on intelligence gathering [50]. The SVR 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 [45].

1———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 subcategory of intelligence involving collecting information from cyberspace for analysis and use in cyber security.

(1) *Cozy Bear:* Cozy Bear, also known as APT 29, 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, 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 organisations (NGOs). 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#, VisualBasic .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 [51]. 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 [52]. 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 SVR [53]. 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 multi-valued LDAP property containing a sizable binary object (BLOB) containing data and encrypted credentials. According to the TAG group, one of the LDAP attributes queried by APT29 concerned ms-PKI-Credential-Roaming-Tokens, which manages blob storage of encrypted user credential tokens for roaming [54].

(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 FSB. Since at least 2007, this threat actor has allegedly been responsible for high-profile cyberattacks and espionage campaigns against government, military and diplomatic entities, research and defence organisations 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 [55]. Some of the unique tools and malware used by Turla include the following:

Snake/Uroburos: A highly sophisticated root kit 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.

EpicTurla (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 [56]. In a year of conflict, Turla was observed exploiting vulnerabilities in the systems of critical Ukrainian organisations 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 military invasion 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 analysed by Mandiant, in one, an infected USB stick was used in a Ukrainian organisation 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 [57]. 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 [58].

7.3. FSB

The Federal Security Service, or FSB, is Russia's principal internal security agency, responsible for internal security and counterintelligence. 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 [59]. In recent years, the FSB has expanded its remit to include foreign intelligence gathering and OCOs. Today's state-sponsored hacker groups linked to the FSB are Callisto, EnergeticBear, Gamaredon, TeamSpy, Dragonfly, Havex, CrouchingYeti, and Koala. SBU intelligence analysts say that 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 activities. Most of the operations appear to be reconnaissance or clandestine surveillance [60]. 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 we limit our analysis to the two main APTs linked to FSB: Callisto and Gamaredon.

(1) *Callisto:* Callisto has been an APT focused on cyber espionage at least since 2015. Over the years, this group has targeted various organisations, 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 not 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 [61]. 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 we 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 [62]. In particular, the IT security company SEKOIA.IO 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 research on typosquatted domains to identify targets. Six private companies based in the United States and Eastern Europe, and four s NGOs were identified, all involved in supporting Ukraine. Most of the targeted private organisations 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 all the targets identified so far through the investigation, namely, the industrial and military entities affected and the individuals involved in Russian affairs, are 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 United Kingdom 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 [63]. Interestingly, this 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.

(2) *Gamaredon:* Gamaredon's activity as an APT has been observed since 2013. It is believed to have ties with FSB, specifically Unit 71330. Although Gamaredon and Dragonfly are two separate APTs, both may be related to Unit 71330. While Gamaredon mainly focuses on cyber espionage and intelligence gathering, Dragonfly (also known as EnergeticBear 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 that they are related or operate 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 [64]. 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 organisations, 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 characterised 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 [41] that Gamaredon is responsible for the most significant cyberattacks 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 2022, 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 [54]. Case study analysis of OCOs 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. The case study investigation not only enriches our 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.

8. Conclusions

This evolving, descriptive paper scrutinises the intricate coordination within intelligence agencies, with a particular emphasis on the Russian landscape. The study is methodically structured around two principal RQs that guide the exploration of this complex domain. RQ1 seeks to unravel: 'To what degree is integration between technical and operational levels achieved within intelligence agencies responsible for executing offensive government policies in cyberspace?' This inquiry casts light on the multifaceted nature of coordinating cyber operations that engage numerous state-endorsed APTs managed by various intelligence units. The coordination challenges identified encompass a spectrum of technical dilemmas, including system compatibility, software intricacies, network issues, and timing delays. Additionally, it examines strategic complications, such as the intersection and potential conflict of objectives and methodologies among different agencies, which could escalate into issues of territorial and power disputes. RQ2 examines: 'What elements hinder the integration between technical and operational levels in intelligence agencies tasked with enacting government defensive strategies in cyberspace?' This query delves into the impediments to effective inter-agency cooperation, highlighting factors like varying organisational cultures and operational dynamics. Issues such as disparities in trust-building, leadership styles, decision-making processes, and management of uncertainties are explored, as these can lead to misalignments in objectives and misunderstandings. The paper also addresses the critical 'principal-agent' dynamic, wherein intelligence agencies (agents) have

greater informational access than decision-makers (principals), leading to potential reluctances in information sharing and negatively impacting strategic decision-making and intelligence operations. The research uncovers the profound rivalry among Russian intelligence agencies, notably FSB, SVR, and GRU, marked by their overlapping roles and internal competitions. This environment, coupled with the necessity for cohesive coordination in cyber operations, unveils a host of technical, strategic, and human-centric challenges [65]. While this study has focused on specific organisational, cultural, and operational factors impeding coordination between intelligence agencies, it is important to acknowledge that there may be additional elements at play. These could include geopolitical considerations, budgetary constraints, and technological disparities. The rapidly evolving nature of cyber threats and technologies may also contribute to coordination challenges, as agencies may struggle to keep pace with new developments and adapt their strategies accordingly. Furthermore, the broader political landscape and national security priorities can significantly influence inter-agency dynamics. Changes in government administration, shifts in foreign policy, or emerging global threats may alter the balance of power and responsibilities among intelligence agencies, potentially exacerbating existing coordination issues or creating new ones. As a work in progress, this research paves the way for a multitude of future inquiries. These prospects span various methodologies and themes within the cyber intelligence field, encompassing the study of organisational behaviours in intelligence agencies, the analysis of collaborative mechanisms between different agencies, and the exploration of strategies to effectively navigate the complex dynamics inherent in state-sponsored cyber operations. In conclusion, while the coordination of APTs across multiple intelligence agencies holds significant potential to enhance the impact of cyber operations, it is entangled with a series of formidable challenges. Addressing these challenges necessitates an all-encompassing grasp of the nuances in cyber operations, an acknowledgment of the cultural and operational variances among agencies, and adept management of the 'principal-agent' dynamic. Only through a comprehensive approach to these factors can intelligence entities fully harness the capabilities of coordinated cyber operations [2].

References

[1] D. Štrucl, "Russian aggression on Ukraine: Cyber operations and the influence of cyberspace on modern warfare," *Contemporary Military Challenges* (*Sodobni Vojas˘Ki Izzivi*), vol. 24, pp. 103–123, 2022, doi: 10.33179/bsv.99.svi.11.cmc.24.2.6.

[2] M.S. Weiss, "Russian Military Intelligence: Background and Issues for Congress," CRS Report R46616, 2021. [Online]. Available: https://crsreports.congress.gov/product/pdf/R/R46616. [Accessed: Nov. 9, 2023].

[3] A. Smith, "Public-Private Partnerships and Collective Cyber Defence," in Proceedings of the IEEE International Conference on Cyber Security and Cybercrime (ICCSC), M. Thompson, R. Johnson, Ed. New York: IEEE, 2022, pp. 75–85, doi: 10.23919/CyCon55549.2022.9810912.

[4] F. Ebinger, S. Veit, N. Fromm, "The partisan–professional dichotomy revisited: Politicisation and decision-making of senior civil servants," Public Administration, vol. 97, no. 4, pp. 861–876, 2019, doi: 10.1111/padm.12613.

[5] M. Alderighi, C. Feder, "Institutional design, political competition and spillovers," *Regional Science and Urban Economics*, 2020, doi: 10.1016/j.regsciurbeco.2019.103505.

[6] J. Moses, "Political rivalry and conflict in Putin's Russia," *Europe-Asia Studies*, vol. 69, pp. 961–988, 2017, doi: 10.1080/09668136.2017.1364700.

[7] S. Taillat, F. Douzet, "Collective security and strategic instability in the digital domain," *Contemporary Security Policy*, vol. 40, pp. 362–367, 2019, doi: 10.1080/13523260.2019.1602693.

[8] L.M. Maguire, "Managing the hidden costs of coordination," *Communications of the ACM*, vol. 63, pp. 90–96, 2020, doi: 10.1145/3379989.

[9] J.M. Ostrow, "Conflict-management in Russia's federal institutions," *Post-Soviet Affairs*, vol. 18, pp. 49–70, 2002, doi: 10.1080/1060586X.2002.10641513.

[10] J.J. McNeil, *Maturing international cooperation to address the cyber space attack attribution problem*, PhD Dissertation, Norfolk, VA: Old Dominion University, Norfolk, VA, 2010.

[11] J.L. Hernandez-Ardieta, J. Tapiador, G. Suarez-Tangil, "Information sharing models for cooperative cyber defence," in *5th International conference on cyber conflict* (*CYCON 2013*), June 2013.

[12] E.V.D. Heuvel, G. 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*, R. Badger, P. Thompson, Eds. Berlin: Springer, 2014, pp. 35–50, doi: 10.3233/978-1-61499-372-8-118.

[13] T. Liebetrau, "Organizing cyber capability across military and intelligence entities: Collaboration, separation, or centralization," *Policy Design and Practice*, vol. 6, no. 2, pp. 131–145, 2023, doi: 10.1080/25741292.2022.2127551.

[14] A. Ahmad, J. Webb, K.C. Desouza, J. Boorman, "Strategically motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack," Computers & Security, vol. 86, pp. 402–418, 2019, doi: 10.1016/j.cose.2019.07.001.

[15] *Defending Ukraine: Early lessons from the cyber war.* [Online]. Available: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/, 2022. [Accessed: May. 15, 2023].

[16] M. Khaleefa, M. Abdulah, "Concept and difficulties of advanced persistent threat," International Journal of Computer Science and Network Security (IJCSNS), vol. 16, no. 6, pp. 29–35, 2016. [Online]. Available: https://www.semanticscholar.org/paper/Concept-and-difficulties-of-advanced-persistent-Khaleefa-Abdulah/c0e8fb235c9bdfba5a066fdbba4ae5a660dc0fa8. [Accessed: Nov, 23 2023].

[17] S. J. Shackelford, M. Sulmeyer, A.N. Craig, B. Buchanan, B. 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.

[18] R. Simonson, J.R. Keebler, M. Lessmiller, T. Richards, J. Lee, "Cyber Security Teamwork: A Review of Current Practices and Suggested Improvements," in Proceedings of the Human Factors and Ergonomics Society Annual Meeting, M. Matthews, S. Landry, A. Bisantz, Eds. Thousand Oaks, CA: SAGE Publications, 2020, vol. 64, pp. 451–455, doi: 10.1177/1071181320641101.

[19] D.V. Gioe, "Cyber operations and useful fools: the approach of Russian hybrid intelligence," *Intelligence and National Security*, vol. 33, pp. 954–973, 2018, doi: 10.1080/02684527.2018.1479345.

[20] J. Cheravitch, B. Lilly, *Russia's Cyber Limitations in Personnel Recruitment and Innovation: Their Potential Impact on Future Operations and How NATO and Its Members Can Respond*. Santa Monica, CA: RAND Corporation, 2020.

[21] F.T. Sheldon, G. Peterson, A. Krings, R. Abercrombie, A. Mili, Proceedings of the 5th Annual Workshop on Cybersecurity and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies. New York, NY: ACM Press, 2009.

[22] G. Bonnet, C. Tessier, "Coordination despite constrained communications: A satellite constellation case," in Proceedings of the 4th International Conference on Space Mission Challenges for Information Technology (SMC-IT 2008), Pasadena, CA, USA, 2008, pp. 91–98. [Online]. Available: https://www.semanticscholar.org/paper/Coordination-despite-constrained-communications-%3A-a-Bonnet-Tessier/89110ff5f7e68700bd069f197c2662d1292de0fe. [Accessed: Feb. 20, 2023].

[23] J.-H. Eom, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace," *Computer Science and Engineering*, vol. 19, no. 3, 2014, pp. 45–56.

[24] E. Iasiello, "What is the role of cyber operations in information warfare?" *Journal of Strategic Security*, vol.14, no. 4, pp. 72–86, 2021, doi: 10.5038/1944-0472.14.4.1931.

[25] J. Rollins, C. Wilson, "Terrorist Capabilities for Cyberattack: Overview and Policy Issues," Congressional Research Service, Washington, DC, USA, 2007. [Online]. Available: https://www.semanticscholar.org/paper/Terrorist-Capabilities-for-Cyberattack%3A-Overview-Rollins-Wilson/4cb91489579c09e0b191f579b4605748e2376604 [Accessed: Feb. 21, 2023].

[26] A. Samojlova, "Social engineering methods," *Scientific Development Trends and Education*, 2019, doi: 10.18411/lj-11-2019-48.

[27] R. Egnell, "Civil–military coordination for operational effectiveness: Towards a measured approach," *Small Wars & Insurgencies*, vol. 24, no. 2, pp. 237–256, 2013, doi: 10.1080/09592318.2013.778017.

[28] C. Clough, "Quid pro quo: The challenges of international strategic intelligence cooperation," *International Journal of Intelligence and Counter Intelligence*, vol. 17, no. 4, pp. 601–613, 2004, doi: 10.1080/08850600490446736.

[29] T.H. Hammond, "Why is the intelligence community so difficult to redesign? Smart practices, conflicting goals, and the creation of purpose-based organizations," *Governance*, vol. 20, pp. 401–422, 2007, doi: 10.1111/j.1468-0491.2007.00364.x.

[30] K. Kralovanszky. (2021). *Certain connections between cyber operations, artificial intelligence and operational domains*. Hadtudoma´nyiSzemle Hadmu˝ve´szet. [Online]. Available: https://orcid.org/0000-0002-5560-3525 [Accessed: Jul. 19, 2023].

[31] G. Hofstede, *Culture's consequences: International differences in work-related values*, vol. 5. Los Angeles, CA: Sage, 1984.

[32] E. Meyer, *The Culture Map: Breaking Through the Invisible Boundaries of Global Business*. New York, NY, USA: Public Affairs, 2014.

[33] K. Giles, "'Information Troops' – A Russian Cyber Command?" in *Proceedings of the 3rd International Conference on Cyber Conflict (CyCon 2011)*, Tallinn, Estonia, 2011, pp. 1–16.

[34] I. Ciosek, "Aggravating Uncertainty – Russian Information Warfare in the West," Torun International Studies, vol. 13, no. 1, 2020, pp. 75–88, doi: 10.12775/TIS.2020.005.

[35] A.J. Dawson, M. Innes, "How Russia's internet research agency built its disinformation campaign," *The Political Quarterly*, vol. 90, no. 2, pp. 245–256, 2019, doi: 10.1111/1467-923X.12690.

[36] S. Goel, "Cyberwarfare: Connecting the dots in cyberintelligence," *Communications of the ACM* , vol. 54, pp. 132–140, 2011, doi: 10.1145/1978542.1978569.

[37] K. Pynno¨niemi, *Information-psychological warfare in Russian security strategy*. London and New York: Routledge, 2019, doi: 10.4324/9781351181242-21.

[38] F.J. Egloff and M. Smeets, "Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers," *Journal of Cyber Policy*, vol. 5, no. 2, pp. 326–327, 2020, doi: 10.1080/23738871.2020.1808032.

[39] A. Greenberg. (Apr. 12, 2022). "Russia's sandworm hackers attempted a third blackout in Ukraine," *Wired* [Online]. Available: https://www.wired.com/story/sandworm-industroyer-attack-ukraine/ [Accessed: Dec. 5, 2023].

[40] A. Scroxton, "Sandworm rolls out industroyer2 malware against Ukraine," *Computer Weekly.com*, Apr. 12, 2022. [Online]. Available: https://www.computerweekly.com/news/252515855/Sandworm-rolls-out-Industroyer2-malware-against-Ukraine [Accessed: Jan. 12, 2023].

[41] D. Antoniuk. (Nov. 29, 2022). "Sandworm hacking group linked to new ransomware deployed in Ukraine," *The Record* [Online]. Available: https://therecord.media/sandworm-hacking-group-linked-to-new-ransomware-deployed-in-ukraine [Accessed: Jan. 13, 2023].

[42] R.M.A. Molina, S. Torabi, K. Sarieddine, E. Bou-Harb, N. Bouguila, C.M. Assi, "On ransomware family attribution using pre-attack paranoia activities," *IEEE Transactions on Network and Service Management*, vol. 19, pp. 19–36, 2022, doi: 10.1109/TNSM.2021.3112056.

[43] A. Lemay, J. Calvet, F. Menet, J.M. Fernandez, "Survey of publicly available reports on advanced persistent threat actors," *Computers & Security*, vol. 72, pp. 26–59, 2018, doi: 10.1016/j.cose.2017.08.005.

[44] D.L. Linvill, B.C. Boatwright, W.J. Grant, P.L. Warren, "'The Russians are hacking my brain!' investigating Russia's internet research agency twitter tactics during the 2016 United States presidential campaign," *Computers in Human Behavior*, vol. 99, pp. 292–300, 2019, doi: 10.1016/j.chb.2019.05.027.

[45] H. Mwiki, T. Dargahi, A. Dehghantanha, K.-K.R. Choo, "Analysis and Triage of Advanced Hacking Groups Targeting Western Countries' Critical National Infrastructure: APT 28, RED October, and Regin," in Handbook of Big Data and IoT Security, A. Dehghantanha, R.M. Parizi, K.-K.R. Choo, Eds. Cham: Springer, 2019, pp. 245–266, doi: 10.1007/978-3-030-00024-0_12.

[46] S. Slick, "The Role of the Director of National Intelligence as Head of the Intelligence Community," Foreign Policy Research Institute, September 2019. [Online]. Available at: https://www.fpri.org/article/2019/09/the-role-of-the-director-of-national-intelligence-as-head-of-the-intelligence-community [Accessed: Feb. 4, 2023].

[47] J. Burt, "Russia's Apt28 targets Ukraine government with bogus Windows updates," *The Register*, May 2, 2023. [Online]. Available at: https://www.theregister.com/2023/05/02/russia_apt28_ukraine_phishing/ [Accessed: May 10, 2023].

[48] V. Kumar, C. Shah, "Countering Follina Attack (CVE-2022-30190) with Trellix Network Security Platform's Advanced Detection Features," Trellix, Jul. 19, 2022. [Online]. Available: https://www.trellix.com/en-us/security-news.html. Accessed: [Accesed May 10, 2023].

[49] R.F. Staar, C.A. Tacosa, "Russia's security services," *Mediterranean Quarterly*, vol. 15, pp. 39–57, 2004, doi: 10.1215/10474552-15-1-39.

[50] I. Thornton-Trump, "Russia: The Cyber Global Protagonist," EDPACS: The EDP Audit, Control and Security Newsletter, vol. 65, no. 2, pp. 19–26, 2022, doi: 10.1080/07366981.2022.2041226.

[51] G. Brogi, V. Viet Triem Tong, "Terminaptor: Highlighting advanced persistent threats through information flow tracking," in: *8th IFIP international conference on new technologies, mobility and security (NTMS).* pp. 1–5, 2016, doi: 10.1109/NTMS.2016.7792480.

[52] E.M. Hutchins, M.J. Cloppert, R.M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation, 2010. [Online]. Available at: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Accessed: Nov. 17, 2022].

[53] R. Waters. (Nov. 10, 2022). *Apt29 using Windows credential roaming bug to target diplomats. Mandiant finds Apt29 increasingly targeting NATO and its allies in 2022.* [Online]. Available: https://www.cybercareers.blog/2022/11/apt29-using-windows-credential-roaming-bug-to-target-diplomats/ [Accessed: Dec. 20, 2023].

[54] R. Lakshmanan. (Nov. 9, 2022). *Apt29 exploited a Windows feature to compromise European diplomatic entity network.* [Online]. Available: https://thehackernews.com/2022/11/apt29-exploited-windows-feature-to.html [Accessed: Nov. 10, 2022].

[55] D. Pereira. (Jun. 7, 2023). *The origin story of the Aptturla, the hunt for' the snake' malware, and current steps for prevention.* [Online]. Available: 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/ [Accessed: Jul. 10, 2023].

[56] Securelist by Kaspersky. (Aug. 7, 2014). *The epicturla operation.* [Online]. Available: https://securelist.com/the-epic-turla-operation/65545/ [Accessed: Dec. 10, 2023].

[57] L. Gyongyosi. (Jan. 9, 2023). *Turlause sold malware infrastructure to attack Ukrainian institutions*: *Andromeda USB spreading malware used for data exfiltration.* [Online]. Available: https://heimdalsecurity.com/blog/turla-uses-old-malware-attack-ukrainians/ [Accessed: Nov . 20, 2023].

[58] B. Leonard. (Jul. 19, 2022). *Continued cyber activity in Eastern Europe observed by threat analysis group.* [Online]. Available: https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/ [Accessed: Dec. 10, 2022].

[59] L. Turkaeva, "Federal security service in the national security system," 2020, doi: 10.20310/2587-9340-2020-4-15-399-406.

[60] J. Kose, "Cyber Warfare: An Era of Nation-State Actors and Global Corporate Espionage," Semantic Scholar. [Online]. Available: https://www.semanticscholar.org/paper/Cyber-Warfare%3A-An-Era-of-Nation-State-Actors-and-Kose/d10e2841df8e35c85830d69e54fc262c4e01ebe9 [Accessed: Jan. 18, 2023].

[61] K.S.R. Rani, B.C. Soundarya, H.L. Gururaj, V. Janhavi, "Comprehensive analysis of various cyberattacks," in: *IEEE Mysore Sub-section International Conference (MysuruCon)*, 2021, pp. 255–262.

[62] F. Aimé, M.A. Togun, "Calisto Shows Interest in Entities Involved in Ukraine War Support," Cyber Threat Intelligence Bulletin, Dec. 5, 2022.

[63] I.Group®. (Sep. 19, 2022). *Russia-nexusuac-0113 emulating telecommunication providers in Ukraine* [Online]. Available: https://www.recordedfuture.com/russia-nexus-uac-0113-emulating-telecommunication-providers-in-ukraine [Accessed: April. 7, 2023].

[64] G. Tiepolo. (Feb. 14, 2023). *Russian apt'gamaredon' exploits hoax shell to target Ukrainian organizations* [Online]. Available: https://mrtiepolo.medium.com/russian-apt-gamaredon-exploits-hoaxshell-to-target-ukrainian-organizations-173427d4339b [Accessed: May 26, 2023].

[65] B. Lilly, J. Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," in Proceedings of the 12th International Conference on Cyber Conflict (CyCon), T. Minárik, R. Jakschis, L. Lindström, Eds. Tallinn: NATO CCD COE Publications, 2020, pp. 189–203, doi: 10.23919/CyCon49761.2020.9131723.