ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

The Russia-Ukraine Conflict from 2014 to 2023 and the Significance of a Strategic Victory in Cyberspace

Dominika Dziwisz | Jagiellonian University, ORCID: 0000-0002-5837-3446
Błażej Sajduk | Jagiellonian University, ORCID: 0000-0002-2974-8173

Abstract

The article explores Russian engagement in cyberspace during the conflict with Ukraine. Many experts have been surprised not only by the lack of coordination between offensive military operations in cyberspace and other domains, but also by the absence of significant cyberattacks. The central argument revolves around the perceived inadequacy of Russian capabilities. However, the authors contend that such an assessment is flawed and stems from the imposition of Western expectations onto a non-Western actor. They argue that the Russians' employment of cyberspace not only aligns with their strategic culture but also represents a continuation of their utilisation of cyber as a tool for disinformation, which was previously observed during the war with Georgia in 2008 and the initial phase of the conflict with Ukraine in 2014. The aim of the article is threefold. Firstly, it discusses the Western strategic discourse regarding the potential use of cyberspace in warfare. In contrast to the position of Western experts, the second part of the article presents the Russian approach. The third section describes how the application of Russian cyber warfare concepts has played out in practice during the conflict in Ukraine.

Keywords

Cyberspace, Russia, Ukraine, war, strategy

Received: 23.08.2023

Accepted: 5.12.2023

Published: 28.12.2023

Cite this article as:
D. Dziwisz, B. Sajduk "The Russia-Ukraine conflict from 2014 to 2023 and the significance of a strategic victory in cyberspace," ACIG, vol. 2, no. 1, 2023, DOI: 10.60097/ACIG/162842.

Corresponding author:
D. Dziwisz, Jagiellonian University; ORCID: 0000-0002-5837-3446; E-MAIL: dominika.dziwisz@uj.edu.pl

Introduction

During the 2013 gathering of high-ranking Russian and US defence officials, General Nikolai Makarov derided the absence of information warfare in the mission of US Cyber Command (USCYBERCOM) [1]. In a bold speech, he told his counterparts, "One uses information to destroy nations, not networks" and suggested that the Americans' lack of emphasis on information warfare demonstrated their ignorance. This incident served as a clear indication of Russia's cyberspace priorities, as subsequently reflected in their strategic documents and implemented during the Ukraine conflict in 2022.

Despite the ongoing war in Ukraine, significant breakthroughs on the battlefield resulting from cyberattacks have yet to materialise. During the Russian-Ukrainian conflict, many experts have expressed surprise at the lack of offensive cyber actions. However, an analysis of cyberattacks since 2014 indicates that the Russians never considered cyberspace as a decisive domain for offensive actions [2], [3], [4]. From 2000 to 2020, Russia primarily focused on intelligence activities. Approximately 61% of attributed incidents were centred on the acquisition of information rather than disruption or degradation of adversary systems [5]. Furthermore, coordination between cyber operations and military actions has not unfolded as expected. In contrast to initial attempts to synchronise cyber and kinetic forces at the beginning of the war, we now observe the independent use of these two Russian capabilities [2]. This discrepancy may be attributed to the different objectives assigned to Russian cyber operations and kinetic invasions. Cyber operations focus on information warfare, including disinformation, propaganda, and subversion, while kinetic actions aim to acquire territory. As a result, it can be deduced that the highly anticipated "cyber Pearl Harbor" event is unlikely, and Russia's performance in cyber warfare is not worse than expected. This is primarily due to the fact that cyber weapons are not suited to circumstances in Ukraine.

The article reviews opinions regarding the role of cyberspace in Russian strategy. Attention was drawn to the divergent understanding among Western experts regarding the strategic utilisation of cyberspace by the Russians. This discrepancy contradicted both earlier assessments and actual Russian actions, starting from the attacks on Estonia in 2007.

Consequently, the following research hypotheses have been adopted:

- **H1:** A different understanding of the use of cyberspace for strategic purposes, compared to the Russian perspective,

led to the formation of numerous inaccurate expectations and forecasts regarding cyberspace use during the war in Ukraine.

H2: Cyberspace did not effectively serve Russia's objective of territorial acquisition in Ukraine, because it is better suited as a domain for operating in the grey zone, specifically for informational purposes.

H3: Cyberspace was mostly utilised by the Russians in the initial phase of the war to deploy offensive weapons against Ukrainian command and control systems, as well as massive malware attacks.

To investigate these hypotheses, the authors conducted a detailed analysis of assumptions and predictions on significance of cyberspace use for strategic objectives.

To conduct the study, a registry and database were developed, containing scientific articles, public writings, as well as reports from official think tanks and governments concerning the strategic use of cyberspace by the Russian Federation, with particular emphasis on publications related to cyber activities accompanying the conflicts in 2014 and 2022. Based on this, a study of source material was carried out using a critical analysis method.

This paper will proceed as follows: The first section describes Western perceptions of cyberspace use during conflicts, starting from the cyber Pearl Harbor and ending with actions below the threshold of war. The second section discusses the Russian strategic discourse on the role of cyberspace during conflict and warfare. The third part deals with the issue of Russian offensive actions in cyberspace and their role in achieving strategic victory.

Western Strategic Discourse: From Cyber Pearl Harbor to the Cyber Grey Zone

War is a legally and morally exceptional state of affairs, well defined on the grounds of international law. However, predictions about the future of war follow narratives and intellectual trends. Various manifestations of war, e.g. hybrid war, cyberwar, grey zone confrontation, come to the forefront of academic debate when social circumstances become favourable. Moreover, the development of cyberwar-related topics has resulted in a division within the field

between "alarmists" who view cyber power as crucial in modern strategic affairs and "sceptics" who believe that cyber power possesses less potency. The multitude of views regarding the potential use of cyberspace in warfare, as well as the ambiguity surrounding the terminology employed, may lead to, among others, a misunderstanding of Russian operational concepts.

The warning issued by US Defence Secretary Leon E. Panetta in 2012 about an unavoidable "cyber Pearl Harbor", an attack that would cause physical destruction and loss of life, influenced the understanding of conflicts in the digital realm, where the sole alternative to cyberwar is cyberpeace [1]. Since then, "exaggeration" has become an important characteristic of the cyberwar discourse (for example, exaggerating the effect of cyberattacks on Estonia in 2007 or the Russian invasion of Georgia in 2008) [6]. This concept found fertile ground, especially among high-ranking US military officials, particularly as a means to rationalise heightened investment in cybersecurity. In an unclassified memorandum dated 23 March 2012, General Keith Alexander provided a strategic assessment for operating in cyberspace and "Preventing a Pearl Harbor Environment" [7]. He shared his viewpoint on the potential occurrence of a cyber "Pearl Harbor" and delved into the perils associated with failures in the realm of cyberspace. This analogy and metaphor quickly caught on, not only in official speeches by government officials but also in media coverage, where they were uncritically repeated. It also heavily influenced the global discourse on cybersecurity and strategic planning in the early 2000s [8]. However, this circumstance was not without adverse repercussions. The ease of using catchy metaphors in discussions about war encouraged the unquestioned expansion of a reasoning that appears effective in theory but lacks explanatory capability in practice. Those who overlook this tendency are prone to rely on metaphors to do their thinking for them [9].

The widespread adoption of terminology such as "cyber-doom", "power grid shutdown", "shock and awe", and "worst-case scenarios" also garnered support from some researchers, particularly leading up to and during the onset of the Russian-Ukrainian war. Jason Healey, the former Director of the Atlantic Council's Cyber Statecraft Initiative, predicted that "it will be the first time a state with real capabilities is willing to take risks and put it all on the line" [10], and that "a Russian cyber offensive might have far more impact on the battlefield, more coercive power, more lethal and widespread effect than many doubters would expect" [11]. William Courtney and Peter A. Wilson of the RAND Corporation wrote that a Russian invasion would "likely employ massive cyber and electronic warfare tools and long-range

PGMs to create 'shock and awe,' [and] causing Ukraine's defences or will to fight to collapse" [12]. Keir Giles of Chatham House believes that "a destructive cyber onslaught could target military command and control systems or civilian critical infrastructure and pressure Kyiv into concessions and its friends abroad into meeting Russia's demands" [13]. NATO analysts David Cattler and Daniel Black assert that "cyber-operations have been Russia's biggest military success to date in the war in Ukraine" [14]. Despite some limitations, Russian cyberattacks on Ukrainian government and military command centres, logistics, emergency services, and crucial facilities such as border control stations were completely aligned with a strategy known as "thunder run", aimed at generating chaos, confusion, and uncertainty, and ultimately to prevent a costly and prolonged war in Ukraine. It is worth noting that Russian cyber-units have showcased their capability to achieve success with minimal prior warning and guidance, despite the significant challenges impeding Russia's military endeavours [14].

Despite these radical predictions, cyber operations don't appear to be playing a decisive role on the Russian-Ukrainian battlefield. Since the beginning of the war, various, sometimes contradictory, analyses have been published regarding use of the cyberspace in this conflict. However, most experts agree on one aspect – cyber operations did not significantly contribute to achieving Moscow's campaign objectives. James Lewis from CSIS writes that "the so-far inept Russian invasion, where cyber operations have provided little benefit, raises questions about the balance between defence and offense in cyberspace, the utility of offensive cyber operations, and the requirements for planning and coordination" [3]. Jon Bateman from the Carnegie Endowment for International Peace states that "Russia's cyber operations in Ukraine have apparently not had much military impact", and even goes so far to describe it as "Russia's humbling experience" [15]. On the other hand, John Hultquist from Mandiant points out that "many of these attacks carried out were designed to affect the civilian populace rather than any military targets" [16]. Marcus Willetta from IISS was surprised that "Russia's invasion of Ukraine in 2022 did not appear to be accompanied from the outset by Russian cyber operations aimed at extensively disabling Ukraine's critical national infrastructure" [4].

Microsoft wrote about the "limited impact" of cyber operations and the sharp decline in their intensity and pace already at the beginning of March 2022 [4]. Researchers Nadiya Kostyuk and Erik Gartzke say that "while Russia has conducted some cyber operations in Ukraine, both in the lead-up to and after the February invasion, these have

neither supplanted nor significantly supplemented conventional combat activities" [2].

There are several factors that can explain the lack of spectacular successes by the Russians in cyberspace, including a lack of flexibility in army management, the desire to avoid risks associated with the uncontrolled spread of attacks to other countries, the plan for a swift victory in the early weeks of the war without the need to utilise cyber capabilities [18], as well as the lack of coordination between cyber and kinetic operations [2]. There are also voices suggesting that Russian military strategists set the bar too high for cyber operations, basing their planning on observations from wars fought in the 1990s and the beginning of the current century, without adapting them to the conditions of total war [19]. There was a lack of ideas (and possibly processing power or capability) for coordinating actions across different domains of warfare. Despite attempts in the early weeks of the invasion, currently, we can only observe independent utilisation of Russian capabilities [17].

However, another explanation for the absence of a cyber Pearl Harbor cannot be ruled out. Namely, that from the very beginning, the Russians did not plan for wide-scale use of direct cyber capabilities against critical infrastructure objects, not due to a lack of such capabilities, but rather because of other strategic assumptions that perceive the cyberspace as most useful for achieving informational objectives. If this is the case, Russia may have different strategic goals for the use of cyberspace. This also fits into the current decline in popularity of the term "cyberwar", as multiple non-military perspectives on understanding cyberpower are emerging. A review of the state of the art has shown that competition below the threshold of armed aggression is constantly gaining in importance. The emphasis on activities in the grey zone appears in, e.g. strategic documents of the largest cyber rivals – the US, Russia and China – but also in national security strategies of other countries, including Australia, Germany, Great Britain, and Indonesia [20]. The most contemporary approach perceives cyberpower mostly as a form of intelligence activity [21] and cyberpower exercises as a state of "unpeace" [22], an equivalent of the terms: "grey zone" between war and peace [23], [24] (the most popular), "non-war military activities" [25],"warfare during peacetime" [26], [27], "subliminal aggression", "persistent cyberspace confrontation", or "non-war" [20], [28]. All these terms refer to actions below the threshold of armed aggression and usually cover the entire spectrum of possible actions, not only those in cyberspace. Therefore, besides deriving offensive and defensive strategies from the study of war, in practice, cyber conflict has been low in intensity, remaining below the threshold of armed conflict [21].

However, the ongoing war confirms that the unquestionable benefits of cyber operations during a conflict below the threshold of war lose significance when the conflict becomes "hot". The key advantage of cyber actions, or attribution – the clear indication of the attacking entity in cyberspace – loses significance when both sides are already in physical confrontation, and their mutual intentions are clear. In other words, deniability and ambiguity, which define grey zone conflicts, do not apply during times of war.

One of the advantages of conducting hostile operations in cyberspace is the ease of disrupting enemy information exchange, which can be more effectively achieved, for example, through missile attacks on telecommunication infrastructure elements. The third advantage is their non-territorial nature, meaning they can be carried out from any location on Earth, but this loses significance when kinetic targets can be attacked throughout the enemy's territory, as the Russians are doing by targeting objectives across Ukraine. In the current phase of the war, Russia continues to utilise cyberspace to conduct operations in the grey zone against states supporting Ukraine. As a result, one can expect an intensification of disinformation and intelligence activities. This is reflected in opinions from Microsoft experts, who indicate that hostile Russian actions aimed at states supporting Ukraine primarily have an intelligence character. For instance, the attacks targeting Polish entities were not intended to damage systems as much as to gather information about the logistics process related to providing assistance to Ukraine.

Despite the aforementioned factors, which prevent categorising current cyber activities of the war as "grey zone" actions, the techniques employed in Ukraine remain similar to those utilised prior to 24 February 2022, once the element of surprise is excluded.

Russian Strategic Discourse – Information as a Weapon

To comprehensively grasp the broader context of Russian activities in cyberspace during the war with Ukraine, it becomes imperative to delve into how Russia defines and assigns significance to these activities at a strategic level. Undoubtedly, perception of this role is influenced by a longstanding tradition rooted in the development of doctrines pertaining to the active utilisation of intelligence and subversive operations, tracing back to the eras of Tsarist Russia and the Soviet Union. Russia's modern armed forces exhibit a creative continuity of this tradition. The very notion of "information

warfare" can be viewed as a natural extension of concepts formulated in the 1920s regarding active intelligence and counterintelligence. As posited by Jolanda Darczewska, this concept signifies "not so much a change in the theory of its conduct (the changes mainly relate to the form of its description, and not the content), but rather a clinging to old methods (sabotage, diversionary tactics, disinformation, state terror, manipulation, aggressive propaganda, exploiting the potential for protest among the local population)" [29].

Historical heritage played a significantly larger role in contemporary Russian military strategic thought. This is because it is influenced by two conflicting perspectives. According to Dimitri Minic, on one hand, it is shaped by arguments advocating the traditional definition of war as "the direct and open use of armed violence". The opposing view posits that the central issue is the "bypassing of armed struggle" through the use of "indirect, non-armed violence", including activities in the cyber sphere [30]. This duality in defining the role of non-kinetic actions conducted in cyberspace (as well as the infosphere) at the strategic level may explain the limited role of cyber offensive actions during the hot phase of the conflict with Ukraine.

In addition to considering the historical context and distinctive strategic culture, the Russian approach to information and its role in achieving objectives within international politics and internal security is shaped and refined through numerous official documents [31]. These documents unequivocally indicate Russia's awareness of being perceived as a threat by numerous countries. Concurrently, Russia is cognizant of its relatively disadvantaged position in the event of a confrontation with NATO. This is particularly evident in the 2021 National Security Strategy of the Russian Federation, wherein explicit mention is made of foreign global internet companies that disseminate disinformation and orchestrate social protests based on "the objective social and economic difficulties in the Russian Federation" [32]. Moreover, the Russian strategic culture perpetually portrays Russia as a besieged fortress [33], with the country's power elite steadfastly believing that it faces an incessant threat of cyberattacks from the West, particularly NATO [34].

These factors create a foundation for the underlying assumptions of the Russian strategy in global competition, wherein continuous competition in the information domain is viewed as a permanent aspect of Russia's exertion of pressure on Western states [35]. As a comparatively weaker actor, Russia must maintain a persistent and proactive approach in influencing other countries. This strategic outlook is operationalised at the military level through a collection

of concepts known as "Gerasimov's Doctrine" [36], which was largely a reaction to US offensive actions, according to Moscow [37]. A crucial component of this doctrine is the belief in the necessity of conducting "active defence", which entails employing non-military means and indirect approaches to maintain constant pressure on adversaries [38]. The concept of "active defence" encompasses a wide array of activities aimed at systematically destabilising the social, political, and military systems of the opponent over an extended period, preceding any kinetic actions. Key elements for exerting this pressure involve non-military means utilised below the threshold of war, such as psychological warfare and subversion.

When discussing the evolution of warfare, Russian sources indicate that the current sixth generation of warfare involves "high-precision weapons based on land-air-sea", with cyberspace assuming a reduced role as "informational-space support" [38]. The Russians classify information warfare activities into two interconnected and complementary categories: information operations and cyber operations (i.e. offensive operations in cyberspace as defined by NATO) [39]. The latter further encompasses two distinct strands: cyber-psychological and cyber-technical operations. Cyber-psychological operations primarily leverage platforms, such as social media, to disseminate disinformation and propaganda, intending to exert long-term influence on societies and potentially destabilise hostile states. On the other hand, cyber-technical operations include a broad range of activities targeting enemy infrastructure. In the Western paradigm, however, greater emphasis is placed on destructive offensive cyber operations targeting critical infrastructure, rather than information operations [40]. It is essential to note that Russian military terminology distinguishes their approach to information warfare, which extends beyond activities conducted solely during or immediately preceding kinetic warfare, in contrast to the Western approach that focuses on the tactical utilisation of information warfare during ongoing conflicts [41]. In this regard, Keir Giles astutely observed that the Russian term "kibervoyna" (cyber war) is only used when referencing Western thinking rather than Russian approaches [42].

During a conflict, Russia focuses on enhancing its armed forces to conduct strikes against critical infrastructure. However, the primary role of this task falls under long-range strike capabilities, specifically cruise and ballistic missiles, with cyber capabilities providing supporting roles [43]. It is worth noting that "It remains unclear how cyber weapons fit into Russian thinking on strategic operations and SODCIT (*Strategic Operation for the Destruction of Critically Important Targets*) in particular" [43]. Despite this, artillery remains a significant

component in Russia's "non-contact warfare" [38] approach, relegating cyberspace to a secondary position. According to a report from the RAND Corporation, "Russian military officers and analysts believe that augmenting capabilities in EW, space, and cyber could fully compensate for a lack of conventional theatre strike capacity" [44]. In the Russian armed forces, cyberspace is not regarded as a novel weapon category that fundamentally alters the nature of temporal activities on the battlefield. Instead, it is viewed as a tool primarily for subversion and enhancing its effectiveness. This perspective has guided the approach of the Russian Federation's armed forces in recent years.

Russia's Utilisation of Cyberspace During an Armed Conflict

When examining the utilisation of cyberspace in warfare, a crucial aspect pertains to its application during military interventions conducted by Russia against neighbouring countries. The Russian power elite justified these interventions as defensive actions aimed at safeguarding Russia through what they perceived as limited-scale defensive wars [45]. In this regard, the actions taken against Estonia in 2007 are particularly important, but did not cross the threshold of physical interference by armed forces. Additionally, the armed conflicts with Georgia in 2008 and Ukraine in 2014 exemplify Russia's approach.

In Estonia, the pressure exerted was primarily achieved through successful yet temporary distributed denial-of-service (DDoS) attacks targeting government IT systems. However, no substantial cyberattacks have been officially confirmed, and experts have noted the absence of such attacks in Moscow's arsenal. During the war with Georgia, cyber activities were predominantly ancillary to kinetic operations. Similar to the cyberattack on Estonia, instances of DDoS attacks and website defacements against official institutions were reported. Nonetheless, the Georgia conflict in 2008 demonstrated that offensive operations in cyberspace need not occur at the "speed of cyber" [46]. The coordination of such operations with other domains poses a challenge that is difficult for most armed forces worldwide to manage. In the context of the Georgia conflict, Erik Gartzke astutely noted that Russia relied on conventional forces rather than cybernetic forces to achieve success [47].

In a similar vein, during the initial phase of the conflict with Ukraine in 2014, the utilisation of offensive actions in cyberspace did not

hold significant importance in warfare [48]. Researchers and analysts posed the question: "Why was there no cyberwar in Ukraine?" [49]. James A. Lewis, when evaluating Russian offensive activities in cyberspace targeting Ukraine in 2015, observed "Cyberattacks are a support weapon and will shape the battlefield, but by themselves they will not produce victory" [50]. Subsequent cyberattacks on the Ukrainian power grid in 2015 and 2016 were primarily employed to exert pressure on Ukrainian society and the government in Kiev [51]. The NotPetya attack in 2017 aligns with the same logic of activities in the grey zone. It is important to emphasise that none of these actions changed the course pursued by authorities in Tallinn, Tbilisi, or Kiev. This fact certainly did not escape the attention of the Kremlin's ruling elite. Hence, it appears that Russian expectations regarding activities in cyberspace are much more modest than assumed in the West, a notion seemingly substantiated by the progression of the Russian invasion of Ukraine in 2022. This is consistent with the conclusions drawn by analysts at CSIS in 2023: "Moscow appears to view using cyber operations more as a means of harassing Ukraine and supporting information operations than as a war-winning weapon indicative of the thunder run strategy (...) Cyber operations remain a weak coercive instrument for Moscow despite their frequent use" [52].

The shift by Russia from operations in the grey zone to a kinetic military operation can be explained not only by the ineffectiveness of such actions but also by Russia's increased assertiveness in international relations over the past decade and Vladimir Putin's growing acceptance of higher risk levels, particularly in actions directed against Russia's immediate surroundings [53]. Additionally, Tor Bukkvoll highlights that Putin's willingness to take on more risk stems from the "prospect theory", which posits that individuals who fear losses are more inclined to engage in risky actions compared to those pursuing profit [54]. Consequently, it can be assumed that the fear of conflict escalation did not constrain Russian activities in cyberspace, and if Russia possessed effective cyber weapons, they would have undoubtedly been employed already. The level of tactical planning is evident in Russian actions, as the dominant attack tools were modified and gradually adapted in preparation for the impending invasion. Kenneth Geers noted in this regard that the beginning of 2022 witnessed a prevalence of defacement attacks, followed by intensified distributed denial-of-service (DDoS) attacks just before the invasion, and massive-scale malware usage during the kinetic phase of the operation [55].

Equally important in understanding the role of cyberspace activities in kinetic conflicts is Russia's extensive employment of malware.

Microsoft has identified at least eight families of malware utilised in the initial weeks of the attack [56]. However, determining the extent of their coordination with kinetic assaults poses challenges [15]. This aligns with the fact that cyberspace activities are subject to limitations that require a choice between mutually exclusive attributes such as speed, intensity, or control. Lennart Maschmeyer referred to this predicament as the subversive trilemma [57]. It appears that Russia, in this trilemma, prioritised intensity at the expense of the other factors, recognising that leaving the grey zone would hinder their ability to maintain coordinated speed between cyberspace activities and operations in other domains. Similarly, they relinquished the control component. Nonetheless, these limitations restrict the ability of cyber operations to successfully produce independent strategic utility. Herbert Lin suggests that a potential solution could involve increasing the scale of cyberattacks at the expense of quality, selecting tactics that "go forth and damage Ukrainian institutions that provide government, military, and economic functions, that inform the Ukrainian public, or that constitute Ukrainian critical infrastructure" [58]. However, this approach has its limitations, as the Russians were unable to sustain the same intensity after the initial phase of cyberattacks from January to April 2022 [59]. The offensive role of cyberspace activities was likely constrained, partly because the Russians focused on psychological impact and information warfare, inadvertently exposing their covert access to Ukrainian IT systems, which could have adverse consequences for future offensive cyber operations. This suggests that this strategy might make it impossible to reue vulnerabilities and accesses gained during grey zone operations in a full-scale war, as the adversary may update their systems and bolster defences [61]. However, this may indicate a deliberate Russian prioritisation of grey zone conflict characteristics in cyberspace. The extensive use of malware resulted in some targets being infected with both malware and subjected to kinetic attacks, which could create the illusion of a partial correlation between offensive cyberspace and kinetic actions. This raised doubts among certain Western experts [17]. Nevertheless, it is evident that even if highly coordinated, the impact of cyberspace activities on the overall course of the war has thus far been limited. Despite the increased number of Russian cyberattacks in the initial phase, most proved unsuccessful: "only 29 percent of the attacks breached the targeted networks – in Ukraine, the United States, Poland and the Baltic nations (...) only a quarter of those resulted in data being stolen" [62].

It is noteworthy that the Russians did not show significant interest in synchronising their state-of-the-art electronic warfare systems with

other types of weapons. Jack Watling and Nick Reynolds observed that "Interestingly, there is minimal interest among Russian crews in synchronising these effects with other activities or with deconflicting their effects" [63]. This lack of synchronisation may have followed a similar logic in the use of offensive cyberspace activities. The objective was to deploy malware extensively without attempting to achieve deep synchronisation across different domains. Such a course of action aligns with the principles of Russian warfare, which place importance on the initial phase of war, preemptive measures [64], and information operations conducted in the grey zone.

Conclusions

The shortcomings of the Russian army during the so-called Special Operation against Ukraine launched in February 2022 can be observed with the naked eye. However, in the cyber domain, there was one exception, indirectly indicating Russia's high offensive capabilities. Expert attention focused on the sole officially confirmed and successful offensive cyberattack on Viasat, a satellite internet provider. The objective of this attack was to undermine the Ukrainian military's command and control system (C2). Notably, this attack occurred just hours before the invasion commenced, garnering interest from Western analysts as an example of cross-domain coordination. While the internet blockade posed difficulties in defending Kiev during the early days of the war, it did not grant Russia enough of a military advantage to capture the Ukrainian capital or significantly influence the course of the conflict. The absence of other documented instances of effective Russian cyber operations during this conflict makes it easier to interpret Russian failures in cyberspace as part of the overall *bardak* within Russia. However, it appears that Russian strategic goals in cyberspace were much more modest than what Western experts had imagined.

The text argues that this is because the Russians acted in accordance with their strategic culture, wherein information warfare is crucial for hybrid warfare, but not instrumental in gaining territory. Offensive actions in cyberspace may hold tactical significance but lack strategic importance. The concept of cyberwar, as envisioned by Western analysts, involving offensive actions against the enemy's critical infrastructure during kinetic warfare, did not materialise. This was evident not only in 2022 but also in earlier conflicts such as the 2008 war with Georgia and the 2014 armed conflict with Ukraine. Russian offensive activities in cyberspace aimed at achieving strategic victory primarily involved mass malware attacks in the initial phase, but later

shifted towards intelligence activities and disinformation campaigns. Decisive cyberattacks are not the most important element of this strategy. It seems that Russia acknowledges the limited role of cyberspace in kinetic warfare, primarily focusing on intelligence and subversion, assigning more significance to it. And it will most likely stay that way in the future.

Acknowledgements

The publication has been supported by a grant from the Faculty of International and Political Studies under the Strategic Programme Excellence Initiative at Jagiellonian University.

Bibliography

[1] S. Gordon, E. Rosenbach. (Dec. 14, 2021). "America's Cyber-Reckoning," *Foreign Affairs*. [Online]. Available: https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning [Accessed: May 01, 2023].

[2] N. Kostyuk. (Jun. 23, 2022). "Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine," *Texas National Security Review*. [Online]. Available: https://tnsr.org/2022/06/why-cyber-dogs-have-yet-to-bark-loudly-in-russias-invasion-of-ukraine/ [Accessed: May 01, 2023].

[3] J. Lewis. (Jun. 16, 2022). "Cyber War and Ukraine," Center for Strategic and International Studies. [Online]. Available: https://www.csis.org/analysis/cyber-war-and-ukraine [Accessed: May 01, 2023].

[4] M. Willett. (Oct. 06, 2022). "The Cyber Dimension of the Russia – Ukraine War," *IISS*. [Online]. Available: https://www.iiss.org/blogs/survival-blog/2022/10/the-cyber-dimension-of-the-russia-ukraine-war [Accessed May 01, 2023].

[5] R. C. Maness, B. Valeriano, K. Hedgecock, J. Macias, B. Jensen. (2022, Sep. 22). "Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID): Cyber Conflict from 2000," *The Cyber Defense Review*. [Online]. Available: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/3500241/expanding-the-dyadic-cyber-incident-and-campaign-dataset-dcid-cyber-conflict-fr/ [Accessed Nov. 03, 2023].

[6] M. Hasian, S. T. Lawson, M. McFarlane, *The Rhetorical Invention of America's National Security State*. Lanham, MA: Lexington Books, 2015.

[7] K. Alexander. (Mar. 23, 2012). "Keith B. Alexander, Commander, U.S. Cyber Command, Memorandum for Record, Subject: United States Cyber Command

(USCYBERCOM) Commander's Strategic Assessment for Operating in Cyberspace – Preventing a Pearl Harbor Environment. Unclassified. National Security Archive," *nsarchive.gwu.edu*. [Online]. Available: https://nsarchive.gwu.edu/document/21531-document-2-7 [Accessed: Nov. 03, 2023].

[8] S. Lawson, M. K. Middleton, "Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991–2016," *First Monday*, vol. 24, no. 3, 2019, doi: 10.5210/fm.v24i3.9623.

[9] M. Libicki. (1997). "Defending Cyberspace and Other Metaphors". [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a368431.pdf [Accessed: Nov. 03, 2023].

[10] "What the Heck Is Threatcasting?". (Sep 15, 2017). *Army Cyber Institute*. [Online]. Available: https://cyber.army.mil/Library/Media-Coverage/Article/1342180/what-the-heck-is-threatcasting/ [Accessed: May 01, 2023].

[11] J. Marks. (Feb. 24, 2022). "Here's what cyber pros are watching in the Ukraine conflict," *Washington Post.* [Online]. Available: https://www.washingtonpost.com/politics/2022/02/24/heres-what-cyber-pros-are-watching-ukraine-conflict/ [Accessed: Aug. 02, 2023].

[12] W. Courtney, P. Wilson. (Dec. 08, 2021). "Expect 'shock and awe' if Russia invades Ukraine," *The Hill*. https://thehill.com/opinion/international/584805-expect-shock-and-awe-if-russia-invades-ukraine/ [Accessed: Aug. 03, 2021].

[13] K. Giles. (Dec. 21, 2021). "Putin does not need to invade Ukraine to get his way," *Chatham House – International Affairs Think Tank*. [Online]. Available: https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way [Accessed: May 01, 2023].

[14] D. Cattler, D. Black. (Apr. 06, 2022). "The Myth of the Missing Cyberwar," *Foreign Affairs*. [Online]. Available: https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar?check_logged_in=1#author-info [Accessed: May 01, 2023].

[15] J. Bateman. (Dec. 16, 2022). "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," *Carnegie Endowment for International Peace*. [Online]. Available: https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657 [Accessed: Nov. 15, 2023].

[16] M. Miller. (Jan. 11, 2023). "Russia's cyberattacks aim to 'terrorize' Ukrainians," *Politico*. [Online]. Available: https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561 [Accessed: Dec. 02, 2023].

[17] Microsoft. (Jun. 22, 2022). "Defending Ukraine: Early Lessons from the Cyber War." [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK [Accessed: Nov. 07, 2023].

[18] J. Marks. (Mar. 03, 2022). "11 reasons we haven't seen big Russian cyberattacks yet," *Washington Post*. [Online]. Available: https://www.washingtonpost.com/politics/2022/03/03/11-reasons-we-havent-seen-big-russian-cyberattacks-yet/ [Accessed: Jun. 03, 2023].

[19] J. Bateman, N. Beecroft, G. Wilde. (Dec. 19, 2022). "What the Russian Invasion Reveals About the Future of Cyber Warfare," *Carnegie Endowment for International Peace*. [Online]. Available: https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667 [Accessed: Jul. 23, 2023].

[20] D. Dziwisz, "Cyber Pearl Harbor is Not Coming: US Politics Between War and Peace," *Politeja*, vol. 19, no. 4 (79), 2022, doi: 10.12797/politeja.19.2022.79.07.

[21] L. Maschmeyer, "A new and better quiet option? Strategies of subversion and cyber conflict," *Journal of Strategic Studies*, vol. 29, no. 1, pp. 1–25, 2022, doi: 10.1080/01402390.2022.2104253.

[22] S. Zilincik, I. Duyvesteyn, "Strategic studies and cyber warfare," *Journal of Strategic Studies*, vol. 11, pp. 1–22, 2023, doi: 10.1080/01402390.2023.2174106.

[23] L. Morris, M. Mazarr, J. Hornung, S. Pezard, A. Binnendijk, M. Kepe. (2019). "Gaining Competitive Advantage in the Gray Zone Response Options for Coercive Aggression Below the Threshold of Major War," RAND Corporation. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf [Accessed: Nov. 03, 2023].

[24] G. Popp, S. Canna. (2016). "The Characterization and Conditions of the Gray Zone A Virtual Think Tank Analysis (ViTTa) Prepared for Strategic Multi-Layer Assessment Gray Zone Conflicts, Challenges, and Opportunities: A Multi-Agency Deep Dive Assessment," NSI, Inc. [Online]. Available: https://nsiteam.com/social/wp-content/uploads/2017/01/Final_NSI-ViTTa-Analysis_The-Characterization-and-Conditions-of-the-Gray-Zone.pdf [Accessed: Nov. 03, 2023].

[25] Office of the Secretary of Defense. (2020). "Office of the Secretary of Defense Annual Report to Congress: Military and Security Developments Involving the People's Republic of China." [Online]. Available: https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF [Accessed: Nov. 03, 2023].

[26] S. Takashi. (2020). "Overview of current research," Nakasone Peace Institute, [Online]. Available: https://www.npi.or.jp/en/research/NPI_Research_Note_20201005.pdf [Accessed: Nov. 03, 2023].

[27] J. R. Van der Velde. (Jul. 23, 2018). "Make Cyberspace Great Again Too!," *Real Clear Defense*, https://www.realcleardefense.com/articles/2018/07/23/make_cyberspace_great_again_too_113634.html [Accessed: Jul. 23, 2023].

[28] G. Casey. (Aug. 15, 2007). "Aug. 14, 2007 – Remarks at the National Press Club," https://www.army.mil/article/4436/aug_14_2007_remarks_at_the_national_press_club [Accessed: Jul. 15, 2023].

[29] J. Darczewska. (2015). "The devil is in the details. Information warfare in the light of Russia's military doctrine". Warsaw: Centre for Eastern Studies. May 2015. [Online]. Available: https://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf [Accessed: Nov. 03, 2023].

[30] D. Minic, "How the Russian army changed its concept of war, 1993–2022," *Journal of Strategic Studies*, pp. 1–35, 2023, doi: 10.1080/01402390.2023.2199445.

[31] "Doctrine of Information Security of the Russian Federation". (Dec. 05, 2016). http://www.scrf.gov.ru/security/information/DIB_engl/ [Accessed: Nov. 02, 2023].

[32] "Strategy of National Security of the Russian Federation". (2021). [Online]. Available: https://paulofilho.net.br/wp-content/uploads/2021/10/National_Security_Strategy_of_the_Russia.pdf [Accessed: Oct. 10, 2023].

[33] M. Skak, "Russian strategic culture: the role of today's *chekisty*," *Contemporary Politics*, vol. 22, no. 3, pp. 324–341, 2016, doi: 0.1080/13569775.2016.1201317.

[34] C. Pursiainen, "Russia's Critical Infrastructure Policy: What do we Know About it?," *European Journal for Security Research*, vol. 6, 2020, doi: 10.1007/s41125-020-00070-0.

[35] K. B. Payne, J. S. Foster, "Russian strategy Expansion, crisis and conflict," *Comparative Strategy*, vol. 36, no. 1, pp. 1–89, 2017, doi: 10.1080/01495933.2017.1277121.

[36] S. Fabian, "The Russian hybrid warfare strategy – neither Russian nor strategy," *Defense & Security Analysis*, vol. 35, no. 3, pp. 308–325, 2019, doi: 10.1080/14751798.2019.1640424.

[37] J. A. Kerr, "Concept Misalignment and Cyberspace Instability: Lessons from Cyber-Enabled Disinformation," in *Cyberspace and Instability*, R. Chesney, J. Shires, M. Smeets, Eds: Edinburgh University Press, 2023, pp. 99–126.

[38] M. Kofman, A. Fink, D. Gorenburg, M. Chesnut, J. Edmonds, J. Waller. (2021). "Russian Military Strategy: Core Tenets and Operational Concepts," [Online]. Available: https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf [Accessed: May 01, 2023].

[39] R. Thornton, M. Miron. (2022). "Winning Future Wars: Russian Offensive Cyber and Its Vital Importance," [Online]. Available: https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/09_Thorton_Miron_CDR_V7N3_Summer_2022.pdf?ver=0LhzDv4-cUkzkAqiTz401g%3D%3D [Accessed: May 01, 2023].

[40] J. Hakala, J. Melnychuk. (2021). "Russia's Strategy in Cyberspace," NATO Strategic Communications Centre of Excellence, [Online]. Available: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf [Accessed: Jul. 12, 2023].

[41] K. Giles, A. Seaboyer. (2019). "The Russian Information Warfare Construct," Defence Research and Development Canada, [Online]. Available: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc341/p811007_A1b.pdf [Accessed: Oct. 10, 2023].

[42] K. Giles. (2016). "Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power Russia's 'New' Tools for Confronting the West," [Online]. Available: https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf [Accessed: Sep. 09, 2023].

[43] C. Reach, A. A. Blanc, E. Geist. (2022). "Russian Military Strategy Organizing Operations for the Initial Period of War Research Report," Santa Monica: RAND Corporation, [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1200/RRA1233-1/RAND_RRA1233-1.pdf [Accessed: Jun. 12, 2023].

[44] C. Reach, A. Demus, M. Grisé, K. Holynska, C. Lynch, D. Massicot, D. Woodworth. (2023). "Russia's Evolution Toward a Unified Strategic Operation. The Influence of Geography and Conventional Capacity Research Report," RAND Corporation, Santa Monica. [Online]. Available: https://apps.dtic.mil/sti/trecms/pdf/AD1193347.pdf [Accessed: Nov. 03, 2023].

[45] M. J. Kari, K. Pynnöniemi, "Theory of strategic culture: An analytical framework for Russian cyber threat perception," *Journal of Strategic Studies*, vol. 46, no. 1, pp. 56–84, 2019, doi: 10.1080/01402390.2019.1663411.

[46] S. P. White. (Mar. 20, 2018). "Understanding Cyberwarfare: Lessons from the Russia-Georgia War," *Modern War Institute*, https://mwi.westpoint.edu/understanding-cyberwarfare-lessons-russia-georgia-war/ [Accessed: Oct. 06, 2023].

[47] E. Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, vol. 38, no. 2, pp. 41–73, 2013, doi: 10.1162/ISEC_a_00136.

[48] K. Giles, P. Hanson, R. Lyne, J. Nixey, J. Sherr, A. Wood. (2015). "Chatham House Report: The Russian Challenge," London: Chatham House. [Online]. Available: https://www.chathamhouse.org/sites/default/files/field/field_document/20150605RussianChallengeGilesHansonLyneNixeySherrWoodUpdate.pdf [Accessed: Oct. 10, 2023].

[49] P. Tucker. (Apr. 28, 2014). "Why Ukraine Has Already Lost the Cyberwar, Too," *Defense One*. [Online]. Abailable: https://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350/ [Accessed: Oct. 03, 2023].

[50] J. A. Lewis, "Compelling Opponents to Our Will': the Role of Cyber Warfare in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, K. Geers, Ed. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015, pp. 39–47.

[51] J. J. Driedger, "Russian Active Measures against Ukraine (2004) and Estonia (2007)," in *Russian Active measures – yesterday, today, tomorrow*, O. Bertelsen, Ed. Stuttgart: Columbia University Press, 2021, pp. 177–213.

[52] G. B. Mueller, B. Jensen, B. Valeriano, R. C. Maness, J. M. Macias. (Jul. 13, 2023). "Cyber Operations during the Russo-Ukrainian War," *Center for Strategic and International Studies.* [Online]. Available: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war [Accessed: Nov. 03, 2023].

[53] J. J. Driedger, "Risk acceptance and offensive war: The case of Russia under the Putin regime," *Contemporary Security Policy*, vol. 44, no. 2, pp. 199–225, 2023, doi: 10.1080/13523260.2023.2164974.

[54] T. Bukkvoll, "Why Putin Went to War: Ideology, Interests and Decision-making in the Russian Use of Force in Crimea and Donbas," *Contemporary Politics*, vol. 22, no. 3, pp. 267–282, 2016, doi: 10.1080/13569775.2016.1201310.

[55] K. Geers. (Aug. 11, 2022). "Computer Hacks in the Russia-Ukraine War," DEFCON Conference. [Online]. Available: https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Kenneth%20Geers%20-%20Computer%20Hacks%20in%20the%20Russia-Ukraine%20War%20-%20paper.pdf [Accessed: Oct. 10, 2023].

[56] "An Overview of Russia's Cyberattack Activity in Ukraine Special Report: Ukraine Digital Security Unit". (Apr. 27, 2022). Microsoft Digital Security Unit. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd [Accessed: Oct. 10, 2023].

[57] L. Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security*, vol. 46, no. 2, pp. 51–90, 2021, doi: 10.1162/isec_a_00418.

[58] H. Lin. (2022). "Russian Cyber Operations in the Invasion of Ukraine," *The Cyber Defense Review*, vol. 7, no. 4, pp. 31–46. [Online]. Available: https://www.jstor.org/stable/48703290.

[59] S. J. Freedberg Jr. (May 01, 2023). "Cyber lessons from Ukraine: Prepare for prolonged conflict, not a knockout blow," *Breaking Defense*. [Online]. Available: https://breakingdefense.com/2023/05/cyber-lessons-from-ukraine-prepare-for-prolonged-conflict-not-a-knockout-blow/ [Accessed: Jul. 07, 2023].

[60] T. Starks, A. Schaffer. (Sep. 04, 2022). "Did Russia Mess up Its Cyberwar with Ukraine before It Even invaded?," *Washington Post*. [Online]. Available: https://www.washingtonpost.com/politics/2022/08/04/did-russia-mess-up-its-cyberwar-with-ukraine-before-it-even-invaded/ [Accessed: Sep. 10, 2023].

[61] A. Levite. (Apr. 18, 2023). "Integrating Cyber into Warfighting: Some Early Takeaways from the Ukraine Conflict," *Carnegie Endowment for International Peace*, https://carnegieendowment.org/2023/04/18/integrating-cyber-into-war-fighting-some-early-takeaways-from-ukraine-conflict-pub-89544 [Accessed: Jul. 07, 2023].

[62] D. E. Sanger, J. E. Barnes. (Jun. 22, 2022). "Many Russian Cyberattacks Failed in First Months of Ukraine War, Study Says," *The New York Times*. [Online]. Available: https://www.nytimes.com/2022/06/22/us/politics/russia-ukraine-cyberattacks.html [Accessed: Jun. 10, 2023].

[63] J. Watling, N. Reynolds. (May 19, 2023). "Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine," *Royal United Services Institute for Defence and Security Studies.* [Online]. Available: https://www.rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine [Accessed: Oct. 10, 2023].

[64] T. Thomas. (2019). "McLean, VA Russian Military Thought: Concepts and Elements," MITRE CORP MCLEAN VA. [Online]. Available: https://www.mitre.org/sites/default/files/2021-11/prs-19-1004-russian-military-thought-concepts-elements.pdf [Accessed: Oct. 11, 2023].