ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

The Use of Cyber Tools by the Russian Military: Lessons from the War against Ukraine and a Warning for NATO?

Marina Miron | War Studies, King's College London, UK |
ORCID: 0000-0003-3695-6541

Rod Thornton | Defence Studies, King's College London, UK |
ORCID: 0000-0002-9566-8956

Abstract

This article examines the Russian military's Information Warfare (IW) activities. The particular focus here is on the use by this military of operations in cyberspace as a strategic force-multiplier. It seeks to shed light on why such operations are so important to this military and what goals it hopes to achieve through their use. In particular, this article highlights the role played by what Russian analysts refer to as cyber-psychological and cyber-technical operations. Having established the background to the Russian military's IW thinking, this article then goes on to examine the application of its cyberspace operations against Ukraine: both before the 2022 invasion and as part of it. It is from this examination of the cyber-attacks conducted against Ukraine that a better understanding of the potential of Russian IW can be generated. As such, lessons can be drawn from this conflict as to how, in the future, the Russian military might employ IW specifically against NATO states as part of a major kinetic confrontation. But, as this article notes, drawing lessons as to the actual strength of Russian IW capabilities from the Ukraine conflict may be a flawed process. It may be the case that the Russian military might not have shown its true cyber hand in

Received: 21.03.2024

Accepted: 23.05.2024

Published: 08.07.2024

Cite this article as:
M. Miron, R. Thornton "The use of cyber tools by the Russian military: Lessons from the war against Ukraine and a warning for NATO?," ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190142

Corresponding author:
Marina Miron, War Studies, King's College London, UK. E-mail: marina.miron@kcl.ac.uk;
0000-0003-3695-6541

Ukraine. It may be saving its best cyber tools for any future conflict with NATO itself.

Keywords
cyberattack, cyberspace operations, information war, Ukraine, Russia

1. Introduction

It has long been understood that when it comes to its confrontation with NATO states, the Russian military has been looking to operations in cyberspace to provide for significant force-multiplier effect [1–3]. Such operations offer to have this effect in two specific areas: in the realm of ideas and that of technology. The Russian military – perhaps the most important Russian actor engaged in 'malign' cyberspace activity against NATO states – refers to these two realms as the 'cyber-psychological' and the 'cyber-technical' [4]. The former realm uses cyber means to conduct influence operations by playing on the consciousness of targets, while the latter variant aims at disrupting, degrading, or destroying the IT systems of targets. Such operations, in whatever realm – and as this article explores – are perceived by the Russian military to be vital tools in both the ongoing peacetime 'competition' [5] between Russia and NATO states and any actual kinetic operations that may at some point transpire; that is as part of major armed conflict between the two [6]. This article seeks to highlight just how important these cyberspace operations are, in particular, to the Russian military. It first provides the conceptual basis behind this military's emphasis on such operations and then goes on to discuss some specific examples of their use. The focus where the examples are concerned is on those cyberspace activities sourced to Russia that have been used against Ukraine since 2014 and specifically during the war that began in 2022. From such an analysis, this article then sheds light on the specific Russian cyber capabilities that may, in the future, threaten NATO states and the Alliance's ability to prevail in any potential future war with Russia.

2. Conceptual Basis

It can be said that in Russian thinking 'information' has a much larger role to play as a tool of 'warfare' (however understood) than it does in the West. The notion of using information for propaganda purposes during wartime dates back to Tsarist times [7]. However, the more refined idea of using information as a strategic tool to generate major effect against state rivals first really

began to be discussed in the later Soviet period. In 1960, Evgenii Messner in his book, *Myatezhvoyna* (*Rebellion war*) was one of the first to look upon 'information warfare' (IW) (or, in Russian, *informatsionnoe protivoborstvo*) as a true strategic-level weapon [8]. Mere information, applied adroitly, could be weaponised by influencing the consciousness of an adversary state's population to incite the said 'rebellion' against its own government. By such means, that government could be brought down and replaced by one more amenable to Moscow. In essence, that state would have been 'defeated'.

Of those Russian thinkers who followed in Messner's footsteps in terms of this thinking about the power of IW, Igor Panarin stands out. In 1997, Panarin obtained his doctoral degree in political science with a dissertation entitled, *Information-psychological support of Russia's national security* [9]. And while it is difficult to determine the scope of the overall influence his writings have had on the recent practice of Russian IW, it should be noted that Panarin's methodological framework for the theory of IW came to serve as the capstone for the Information Security Doctrine of the Russian Federation of 2000 [10].

It was Panarin – now operating in the era of IT systems – who first divided IW into two distinct types: the 'information-psychological' and the 'information-technical'. According to Panarin, these two forms differ in terms of their target sets. The first, the information-psychological, looks to influence two particular systems: the system of elite decision-making and the system that relates to public consciousness and thus to the forming of public opinion. This latter system can then go on to influence elite decision-making as a second-order effect. In terms of directly influencing the decision-making of state elites, the targets can range from those at the politico-strategic level right down, in the military sphere, to leaders at quite low levels in the armed forces [11]. The ultimate objective, as Panarin [11] points out, is to generate *manipulation* at the very highest level possible; that is, 'to force the leader of the opposing side to act according with the goal of information war'. This form of IW has now come to be known in Russian circles as the 'cyber-psychological'. This is because the information being supplied to generate the required manipulation will more than likely be coming across IT means.

The fact that, in theory, significant outcomes can be generated at the strategic level through the use of *mere* information has, as noted, attracted an audience in the Russian military. For this military, information appears to offer the enticing possibility of actually

winning 'wars' without kinetic engagement. This is important for a Russian military that has, certainly over the last 20 or so years, understood that it cannot hope to prevail against NATO forces in any major conflict. It is not strong enough in conventional military terms and it would have, it understands, to resort to nuclear weapons to stave off defeat by NATO [12–14]. This is viewed as distinctly undesirable [15]. Hence, the Russian military has accepted that it has to look to asymmetric means – such as IW – if not to actually win its wars with NATO, then at least to gain strategic advantage vis-à-vis the Alliance [2, 16]. The second impetus behind this focus on IW is the view that the Russian military must, as it sees it, match and defend itself against NATO's cognitive technologies which could help NATO achieve a strategic victory, as the adviser to the Russian Defence Minister, Andrei Il'nitsky has suggested [17, 18].

Very senior Russian military officers have not only come to understand the power of IW but also to actively advocate its use. General Yuri Baluyevsky, the former head of the armed forces (from 2004 to 2008), was one of the first such senior officers to stress that trying to win an information war was more important than trying to win a classical military confrontation. The fact that information could be used to produce significant effects against 'the principal organs' (the 'elite decision-makers') of an enemy state was a major attraction to him [19]. The current (as at March 2024) Chief of the General Staff, General Valerii Gerasimov, has further elevated the importance of IW as a weapon of significant influence. He first pushed its capabilities in a speech he made in 2013. This was summarised in his important article entitled, 'The value of science in foresight' [20]. Similarly, influential senior serving, or retired military officers have been repeatedly arguing in Russian military publications that the main focus of peer-state warfare should be placed on destroying adversary states from *within* using non-kinetic means, such as IW, instead of trying to achieve such destruction by kinetic means [21, 22]. Colonel (ret.) Aleksandr Barthosh [23, 24], in particular, has proved influential. He has underlined recently the importance of using information to shape the belief systems of an adversary state's population. As Bartosh [23] puts it, 'the objective is to manipulate the enemy state's population's beliefs'. Such beliefs will then go on to drive the decision-making of the aforementioned elites. He also looked at the way information could influence the 'consciousness' (i.e. the morale) of an adversary state's armed forces personnel. His ideas were building on not just those presented earlier by the likes of Messner and Panarin but also those of Sergey P. Rastorguev [25]. But Bartosh [23] has perhaps more elegantly understood that the power of IW applied at the strategic level

comes from *combining* influence operations deployed against the mindsets of an adversary's civilian population with those directed at the state's civilian and military leaders.

It is through the work of this series of influential Russian observers (and many others not mentioned here) that the power of IW as a tool of warfare has become so ingrained in Russian military thinking. And certainly, this IW tool has become a part of such military thinking in ways that are not mirrored by NATO militaries: these tend to focus almost exclusively on generating kinetic effect, rather than non-kinetic effect [26]. For instance, current Russian military doctrine refers to the important role that inciting 'the protest potential of the population' plays as a strategic tool (and it would, of course, be incited through the use of IW techniques) [27]. No NATO military doctrine would ever include reference to such a technique.

Today, of course, the inciting of such 'protest' is far more easily generated given the role that social media now play in modern societies. Misinformation and disinformation can be disseminated very easily across such media that aim to discredit western institutions (including NATO) and to sow doubt and confusion about individual western government's means of/right to control their populations. False narratives can also act to amplify the existing societal divisions that serve to create damaging schisms. Social media also represent a convenient avenue of attack to weaken the unity of NATO and ultimately to advance its own geopolitical and military interests [24, 28–30]. Moreover, all of this targeting can be done today very easily across IT systems [2].

Here then is the power of the cyber-psychological tool. However, there is also the profound power today of the cyber-technical form of attack. Such attacks target data transmission systems [11]. They can serve to disrupt, deny, or degrade information flows that enable everything from the effective functioning of adversary states' critical national infrastructures (CNIs) down to interfering with their militaries' battlefield systems at the tactical level. Russian analysts, however, tend to concentrate on the *strategic*-level application of cyber-technical means, given that they can also, like the cyber-psychological tools discussed above, generate major strategic – perhaps, indeed, war-winning – effects. Fundamentally, major cyber-technical attacks can also be used with the aim of calling into question the ability of any targeted state to be effectively governed [28, 31–33].

As several Russian sources also affirm, ideally strategic-level cyber-psychological operations should be employed in *coordination*

with strategic-level cyber-technical attacks. The hope is that synergies would be created that maximise effect. According to Panarin [11], '…sometimes the methods of information and technical influence are carried out in combination with the methods of information and psychological confrontation.' Moreover, and of course, by using cyber-based means, these effects can be generated, as the likes of Rastorguev [25] point out, in an extremely resource-lite and cost-effective way.

It is this coordination, this combination of the two forms of attack that is seen as key in generating the degree of dislocation that can actually undermine adversary state governments from 'within'. The goal is to create what Bogdanov and Chekinov [22] refer to as 'chaos' within any targeted state. Examples here might be long-term cyber-psychological activity designed to undermine a state population's faith in its own government which is then allied to and exacerbated by attacks on that state's CNI that create major disruption to everyday life (lights going out; no Internet; banks not functioning, etc.). Power grids would here be a particular focus for cyber-technical attack [34]. The popular discontent resulting from both forms of attack may then incite the 'protest potential of the population' that could bring down the government – to be replaced, of course, by one more suited to Russian strategic interests. Another example of coordinated action would be the use of cyber-technical means to undermine faith in the voting count in, say, the general election of a NATO state, while at the same using cyber-psychological means to call into question the right of the winner of that election to govern – inventing a political scandal, for instance. This may undermine freely elected governments. An example here might be the Russian coordinated cyberattacks using the two forms that sought to materially affect the French presidential election of 2017 [35].

This attack on the French election was seen to be the work of the GRU's (*Glavnoye Razvedyvatel'noye Upravleniye*) Military Unit 26165 or FancyBear [36]. The GRU is the principal intelligence arm of the military. Russian cyberspace operations against adversary states – using both cyber-psychological and cyber-technical variants of attack – are also engaged in by the internal security force, the FSB (*Federalnaya Sluzhba Bezopasnosti*), and the foreign intelligence service, the SVR (*Sluzhba Vneshney Razvedki*) [37]. The GRU, being the most potent and aggressive of these three, is seen, moreover, to be the controlling body that coordinates cyberspace operations of both FSB and SVR [38]. Obviously, and particularly when mass effect is called for (such as with distributed denial-of-service [DDoS] attacks), these

three agencies can call on assistance from Russian civilian hackers – whether voluntary or forced. Other, non-state actors, such as the Wagner Group (and its successors) can also contribute [38, 39].

Overall, when looking at this issue of Russian IW and how to operationalise it through cyber means, it needs to be understood just how much emphasis that the Russian military is putting on it as a strategic tool – and as, indeed, a potentially war-winning tool. As Margarita Simonyan, the then editor-in-chief of *Russia Today*, put it even back in 2013, '…information weapons are comparable to weapons of mass destruction' [40]. After 10 years, this mindset might be seen to apply even more, given the across-the-world increasing reliance on IT systems and the rise of social media. This said, however, the question for NATO and its constituent states – which are seemingly the main targets for Russian military IW – is, can these cyber-psychological and the cyber-technical operations really work to generate the effect that Russian analysts and observers have been advertising? Just how effective can these IW means of 'warfare' be against NATO if ever they were to be employed synergistically against NATO states at times of high geopolitical tension and particularly as part of any major kinetic conflict? This is one of the major questions that NATO countries must be asking – and are asking [41]. In light of such questions, it seems apposite to gauge some sense of the threat posed to NATO by looking at Russian activities in this IW field that have played a part in Moscow's conflict with Ukraine since 2014.

3. Russian Cyberspace Operations in Ukraine prior to the 2022 War

In the years before Russia's full-scale invasion of Ukraine in February 2022, Moscow's exponents of offensive cyber engaged in several significant operations designed to serve strategic ends and which were an adjunct to kinetic activities. For instance, the GRU's Military Unit 54777 (also known as the 72nd Special Service Centre) [42] was known to be crafting an anti-Chechen information campaign during the 1990s. There were also both cyber-psychological and cyber-technical attacks against Georgian targets conducted by GRU's Unit 74455 (Sandworm) that were part of the Russian invasion in 2008 [43]. More recently, Unit 54777 also came to be involved in shaping the information environment prior to Russia's annexation of Crimea and later seizure of the eastern Donbas in 2014. This was done using two of Unit 54777's front organisations, namely, InfoRos and the Institute of Russian Diaspora. The aim was to create an impression that Russian

speakers in the regions in question wanted Moscow to intervene to help them [44]. Thus, as expected and given the emphasis of the writings on this subject over the last several years, Russian IW – using both cyber-psychological and cyber-technical elements – has had a significant role to play as part of the kinetic conflicts being conducted in the service of Moscow's strategic interests.

However, in considering the use of IW to run alongside such kinetic operations, it must be remembered, of course, that the Russian state, before the initiation of such operations, will also have been engaging in what might be looked upon as more long-term preparatory activity in the cyber-psychological realm. There will have been a kind of 'softening-up'/'preparing the ground' process designed to reduce opposition in any targeted area/state. Such preparatory cyber-psychological operations can also, of course, be used in tandem with long-term cyber-technical attacks. Such a combination can clearly be noted when considering Russian cyberspace operations against Ukraine before 2022. There were noted to be dozens of significant cyber-psychological attacks in the months preceding the invasion [45] and several major cyber-technical attacks, chiefly targeted at Ukraine's CNI, notably its power grid [46].

Among the most significant of the pre-2022 cyber-technical operations were those conducted by the Sandworm group. This is also a GRU entity and otherwise known as Military Unit 744551 or Voodoo Bear. It works out of the GRU's Main Center for Special Technologies (*Glavnyi Tsentr Spetsial'nykh Tekhnologii* or GTsST). This unit has been linked to some of the most destructive cyberattacks worldwide [47]. It was Sandworm that stood accused, along with a range of cyber-espionage activities, of conducting the cyberattacks against Ukraine's CNI (particularly its power grid) that began soon after the Euromaidan demonstrations in Kyiv in 2014. The most prominent of these were the BlackEnergy3 attack in 2015 (exploiting Microsoft Word's macro-feature) and the Industroyer malware applied in 2016 [46, 48]. One of the best-documented instances, however, of Sandworm's activities was its deployment of the notorious NotPetya malware in 2017. Although Ukrainian CNI was the initial target, the virus involved spread to create damage to IT systems worldwide, including in Russia itself. Major financial losses were incurred both within Ukraine and internationally, most notably by the Danish Maersk shipping company [49]. The work of Sandworm demonstrated a notable level of sophistication, marked by coordination of a series of attacks and by meticulous consideration of potential mitigation activities engaged in by the targeted entity [46, 48].

The GRU's Fancy Bear group was also engaged in significant cyber operations prior to the war. Most prominent were those designed to interfere with the everyday lives of as many ordinary Ukrainians as possible. Spearphishing, brute-force, and 'password spraying' attacks targeted individuals' accounts [50]. The SVR's CozyBear unit also conducted cyber-attacks against the Ukrainian military, political parties, diplomatic agencies, think tanks, and non-profit organisations during the conflict in Ukraine.

By the beginning of 2022, it could be said that Ukraine had been subjected to a series of cyberattacks from a variety of Russian agencies that were looking to create a sense of political and societal dislocation to weaken the bonds that held the country together. To exacerbate the situation, and just before the February 2022 invasion, Russian cyber-technical attacks against Ukraine 'soared' [51]. This is what should be expected as part of any prelude to an actual Russian kinetic attack (it was the case in Georgia in 2008 as well). By the middle of February 2022 (with the invasion itself beginning on 24 February), cyberattacks were bringing down the websites of Ukrainian government departments and data-wiping malware was being used against over 100 commercial enterprises. In line with the thinking of Bogdanov and Chekinov, the aim was said to be to sow a degree of 'chaos' within the country [51].

4. Russian Cyberspace Operations during the 2022 War

According to Russian doctrinal approaches, it would, of course, be expected that the actual movement of Russian troops across the Ukrainian border on 24 February 2022 would be accompanied by significant cyberspace activity. This would contribute to the generation of disruption and dislocation – if not actual chaos – which would assist the movement of troops on the ground and the gaining of strategic objectives.

When looking specifically at Russian operations in the cyber-technical realm, it will doubtless be the case that the Ukrainian authorities (and NATO itself) would not want to advertise any successful (or even unsuccessful) hacks into Ukrainian military IT systems. This would be sensitive information that would need to be kept from the Russians in order to make, in effect, their battle-damage assessment (BDA) in this cyber-technical realm more difficult to quantify. Given this situation, providing a true analysis of actual Russian hacking activities in this field is difficult.

This said, however, there were known major cyber-technical attacks in the initial period of the invasion. Of note in this regard was the ViaSat KA-SAT hack, which could hardly be hidden. This took place just before the invasion began and was patently designed to be coordinated with it [52]. It was an attack on the downlink ground terminals of the ViaSat satellite network serving Ukraine [53, 54]. While affecting millions of civilian users in Ukraine (and across eastern Europe), it also, crucially, denied information, surveillance, command and control, and communication means to Ukrainian forces and acted to limit their operational capabilities [55]. This did create a military advantage for Russian forces [56].

The use of such cyberattacks so early in the invasion would, as can be understood, be designed to have two particular effects in the strategic realm. Both relate to the sowing of confusion, the generation of chaos. Certainly, the ability of the Ukrainian armed forces to function effectively as a counter to the invasion would be one. However, government structures would also be a target. The Kyiv authorities needed to be seen to be in control in the invasion's early stages when rumours and counter-rumours would be running rife. Slow government reaction – such as in terms of reassuring the population and to creating a sense of the state itself still actually existing – could be fatal in any invasion's first few hours. Anything, thus, that interfered with the ability of both military and government to act quickly would allow scope for a vacuum of control to exist which Russian forces could take advantage of. For in such an invasion as this, the prime goal for Moscow would be to try and have its forces seize the seat of government and impose a Moscow-appointed administration as soon as possible. Anything that would slow down the reaction of the Kyiv authorities – military and government – would work to Moscow's advantage; and here both cyber-psychological and cyber-technical attacks can be seen to have had a role to play.

As it happened, the government in Kyiv was able to maintain control. An attempted FSB *coup de main* operation to seize government structures in the centre of Kyiv on the first day of the invasion was thwarted. Also blocked in the first few days was an attempt to seize Hostomel airfield, close to Kyiv, by Russian Airborne Forces (VDV). This prevented any push by these VDV to the centre of Kyiv and thus to gain control of the capital [57]. Ukrainian forces retained enough command-and-control and coordination capacity to at least hold back this initial assault. Hence, it may be said that whatever Russian cyber-technical attacks were applied in this initial period were not successful: the degree of Ukrainian control was greater

than the degree of chaos that Russian cyberattacks attempted to generate.

In the cyber-psychological realm, there were a number of attempts, in the invasion's early days, to deploy misinformation and disinformation that targeted the consciousness of the Ukrainian population [58]. Particular aims were to undermine support for individual political and military leaders. Their reputations and their right to control the government/armed forces were called into question [59]. Note should be taken, in this regard, of one particular operation conducted by the Russians. This could have proved very telling in the conflict's initial stages. This was the creation of a deepfake of Ukrainian President Volodymyr Zelensky. It appeared on 16 March 2022 in a video on Facebook and YouTube. Deepfakes are a combination of both cyber-psychological and cyber-technical means. The idea behind them is to artificially generate an image/video of a particular leading or influential figure – one of the elite decision-makers – and to have 'them' be seen as acting in ways that suit, in this case, Moscow's ends. The deepfake of Zelensky had 'him' making a speech in which he was calling on Ukrainian troops to 'surrender' [59]. Here, writ large, is the kind of effect that the Russian proponents of IW would see as its ability, using such as this deepfake tool, to have a major strategic, indeed, war-winning effect. If this deepfake had actually gained traction among the Ukrainian population/military, then it could have led to the country's defeat. As it happens, it did not. This was, in part, down to the fact that a few days before the video appeared, Ukraine's Center for Strategic Communication had warned that a deepfake of Zelensky would appear. The authorities were thus prepared for it, and it could be countered. But what this deepfake lacked most of all was veracity; it did not look 'right'. It was clumsy and maladroit. Still, though, Zelensky was forced into making a 'real' appearance and to deny it was 'him' [59]. Beyond its clumsiness, what also seems to have been a mistake here is that this deepfake only made an appearance a few weeks into the war. If it had appeared in the first few hours, or at least the first few days when the situation was at its most 'chaotic', then it could have had more effect within the general confusion pervading at that time.

Beyond the cyberspace operations that were evident in the initial days and weeks of Moscow's 'special military operation', many more have continued throughout the conflict. A particular increase in their use was noted from January 2023 onwards [6]. The GRU's Sandworm group has resurfaced several times. Where this body is

concerned, Mandiant Intelligence has documented the consistent deployment of a standardised and replicable common set of tactics, techniques, and procedures (TTPs) employed during the conflict [60]. A GRU 'playbook' has been seen to be at work. Despite an extended period of aggressive and high-tempo operational use, this playbook appears to have exhibited remarkable resilience. There are five noted elements in this playbook:

1. *Living on the edge*: Here, there is exploitation of compromised edge infrastructure, such as routers, virtual private networks (VPNs), firewalls, and mail servers where interventions are challenging to detect.

2. *Living off the land*: In this approach, there is the employment of inherent tools, such as operating system components or pre-installed software, which can be used for activities such as reconnaissance and information theft. The malware footprint is minimal, which means detection is often difficult.

3. *Group policy objects* (GPO): Here, the policy settings within file systems are targeted, enabling the deployment of wipers through GPOs.

4. *Disrupt and deny*: With this technique, 'pure' wipers are utilised alongside other low-equity disruptive tools, such as ransomware, tailored to various contexts and scenarios to disrupt and deny targeted systems.

5. *Telegraphing success*: Where cyber-psychological operations have attained a degree of success, this tends to be amplified through a series of hacktivist personas on Telegram (widely used in Russia).[1]

1——Adapted from [60].

In terms, specifically, of cyber-technical attacks, there is also evidence of their being combined with kinetic activity. In October 2022, for instance, Sandworm orchestrated a cyber-induced blackout of Ukraine's power grid concurrently with kinetic missile strikes (from the Air Force) on elements of this same grid. Details of the cyberattack were disclosed by Mandiant, which emphasised Sandworm's use of a 'living off the land' (LotL) approach (see above) [61]. In this case, previously planted data-destroying wiper malware, which had evaded detection, was activated once the missile strikes on the grid had gone in. Sandworm's malware erased data content across the utility's network that hindered any repair of the initial damage. The blackout thus lasted longer [62].

This particular above example is indicative of the type of attack that seeks to create the synergies that Panarin first called for in his idea of fusing cyber-technical and cyber-psychological operations. What initially looks like a cyber-technical operation can be seen to morph into a cyber-psychological operation, given the effects that it subsequently can create. The overall Russian aim – where a series of attacks on CNI is involved – would be to sap civilian morale that then leads populations to look to their government to seek an end to their suffering – that is, to call an end to the war. In a similar vein, on 12 December 2023, there was a large-scale cyberattack on Ukraine's mobile phone provider Kyivstar. This left more than 24 million subscribers without cell phone services for several days [63]. Kyivstar subscribers were also unable to manually change their data connection to that of another provider, meaning they were only able to purchase SIM cards from other providers, causing large queues [63]. Around 1.1 million people live in remote locations in Ukraine where Kyivstar is the only provider available [63]. Again, creating such an outage would be geared to undermining the population's capacity to put up with the exigencies of the war.

The above Sandworm example is also indicative of the ability of Russian hackers to adapt and to evolve their forms of attack. Over the course of the conflict, Sandworm's tactics have changed from using highly customised malware (such as the Industroyer malware used to target CNI in real time) to the use of more agile LotL techniques [62]. Another example of cyberspace adaptation is that conducted by another GRU hacker entity known as Cadet Blizzard. This was first identified by Microsoft in June 2023 [64, 65]. This group, operating without bespoke malware, functions as a conventional network operator, seeking public signals to disrupt with the overall aim of generating morale-sapping intimidation. It engages in the likes of website defacements and hack-and-leak operations. It has been targeting not just Ukraine but also NATO member states supporting Ukraine [66]. Microsoft's report identifies Cadet Blizzard as a significant actor in the Russian cyber threat landscape [66]. The examples of Sandworm and Cadet Blizzard indicate that the Russian agencies involved in cyberspace operations can be seen as adaptive, as learning organisations [67].

All this said, however, when looking at Russian offensive cyber activities in the war in Ukraine, it should be noted that they have not been as devastating as might have been expected. Given the noted emphasis in Russian military circles on the importance of offensive cyber as a tool of warfare – and given the noted

capabilities that Russia appears to have in the cyber realm [68–70] – the number of hacking attempts and their sophistication during this war has been, perhaps, limited. They have not proved as damaging as was predicted by many observers before the war [71]. This may be the result of an overestimation of the likes of the GRU's capabilities. It may also be down to stronger than expected Ukrainian cyber defences (which had been honed with the assistance of NATO countries since 2014) [72]. However, there is also a further possible cause here. This is that Russia may be wanting to basically 'hide' its true cyber capabilities in this Ukraine war because it does not want to show them to its NATO adversary. It may be holding these capabilities back to save them for a much more important future conflict with NATO. If NATO were to be forearmed about the real extent of Russian cyber expertise, by witnessing them being used against Ukraine, then NATO could develop its own defences. As Kofman et al. [73] expressed it, 'high-end cyber capabilities may have been held in reserve for conflict with the United States and NATO'.

5. Cyberspace Operations against Satellites

One characteristic of Russian cyberspace activities during the war, and one which should have specific resonance for NATO planners, has been the attacks against satellite links. Such links have to pass through the IT systems of ground stations and so they can be vulnerable to hacking. Data to or from any satellite can be blocked, corrupted, or spoofed. Moreover, the actual movements of individual satellites or even whole arrays can be controlled through cyber intervention [74]. This can 'induce harmful satellite manoeuvres' [75]. As David Burbach sums up, 'an invulnerable satellite fleet [up in orbit] is irrelevant if cyberattacks can impair its ground-based control systems and user access' [76].

The Ukrainian military has made much use of western satellite feeds (for navigation, guidance, communications, etc.). The Ukrainian population has also been looking to satellite-supplied data to aid in the conduct of their everyday lives. The temptation for Russian hackers to target satellites is therefore great – resource-lite cyber-attacks can produce some profound results. It is not only the GRU involved here in such anti-satellite (ASAT) attacks but also, it seems, affiliates, such as the 'cyber troops' of the (former) Wagner organisation [77]. The ViaSat hack in the first few days of the invasion has been mentioned above but there have been other notable examples. Elon Musk's Starlink system of satellites was also, for instance, subject to hacking attempts [78].

It appears, though, and as with wider Russian cyberspace operations, that the degree of attempted hacking of satellite links during the war has not been as high as might have been expected [79]. This may, again, be a case of overestimating capabilities or that Ukrainian cyber defences are better than expected. And it may also be because Russian cyber capabilities in this field are being husbanded for use in a future major war. However, other specific issues are also involved here. Firstly, the Russian economy, at least to some degree, itself relies on the data supplied by western satellites. Russian high-tech industries look, in particular, to the Global Positioning System (GPS) to provide a very precise timing mechanism. Such a benefit appears to be restricting Russian cyber-interference with the GPS. This does mean that GPS-guided Ukrainian missiles and drones are not being prevented from hitting their targets, including within Russian territory. Additionally, the Russian military itself also looks, in part, to GPS for navigation and guidance and would be hindering its own capabilities if GPS became subject to a cyberattack [80].

This issue, though, of the hacking of satellite systems could be a major problem for NATO in any future major conflict with Russia [81]. A host of NATO capabilities that outmatch those of the Russian military (mostly related to C4ISR and weapons' guidance) rely on unfettered access to satellite signals. If these signals are interfered with, then it could profoundly affect NATO's military strength. Given what is at stake, Russia will inevitably be involved in what a leaked report from the US Central Intelligence Agency noted that China was already doing. Beijing was said to be 'building cyber weapons to hack into enemy satellites that would render them useless during wartime' [82].

6. A Warning to NATO

Beyond the issue of its satellites being potentially 'rendered useless' by Russian hacking, NATO states could (will?), in the future, be faced by much wider threats from the Russian military's use of IW applied over cyber means. This military is one, as noted, that looks upon IW as a major force-multiplier to a degree that NATO does not. The Russian military has a specific focus on how cyber-psychological and cyber-technical operations can be utilised to create strategic, perhaps even war-winning, effect. The cyber-psychological methods generally look to generate the long-term undermining of state adversaries; to weaken them from within using influence operations. The cyber-technical means will, in peacetime, largely be looking for weaknesses within western

IT systems that can be exploited later and used especially during actual kinetic conflict. Ideally, according to Russian thinking and when necessary, the two methods – cyber-psychological and cyber-technical – can be combined to create synergies of effect. This would be seen as especially productive in the very early stages of any major kinetic conflict when the coordinated activities of the two types could, at least theoretically, produce strategically important results.

There are a number of issues which NATO states should be specifically aware of in regard to future Russian offensive cyberspace operations. The first is that, because these operations are so important to the Russian military – they are deeply ingrained in its doctrinal logic – that they will doubtless be invested in and improved in the coming years. Lessons must have been learnt from experience in Ukraine. The likes of the GRU and other agencies will have understood, what works and what does not; where Ukrainian cyber defences are strong and where they might be weak. As a consequence, these Russian cyber agencies can also probably extrapolate and go on to establish where NATO cyber defences might also be strong and where weaknesses might lie.

It should be expected that, in the coming years, NATO states will experience more refined 'softening up' cyber-psychological attacks from the Russian military quarter. Western governments, elections, and even whole populations will be subjected to increased attempted 'manipulation' activities to degrees not seen before. This may result, as anticipated in the Russian military literature on this subject, in a long-term weakening of western institutions (NATO, European Union [EU], etc.) and a general undermining of the ability of individual NATO states to govern themselves effectively. Political vacuums could be created that might allow Moscow-leaning administrations to come to power. It should also be expected that cyber-technical attacks will continue against NATO states. These, though, will largely be confined to cyber-espionage activity seeking out weaknesses that can be exploited later and when necessary.

And then there is AI. AI will come to play a major part in the refining of future Russian IW activities. As its capabilities increasingly come to be utilised, AI will elevate the potency of all aspects of Russian cyberspace operations [83]. Cyber-psychological offensives that make use of social media can, with the application of AI, come to be far more targeted and more effective than hitherto. And AI-enhanced deepfakes of 'elite decision-makers' may become indistinguishable from the 'real' person and hence totally

believable [84]. Cyber-technical attacks, enhanced by AI, could potentially be of an unimagined scale and impossible to counter.

But it is, of course, at times of very high geopolitical tension, or maybe even as preparation for major kinetic conflict with NATO, that Russian cyberspace operations may provide the greatest threat to NATO states. At such a time, a host of attacks – in combination and coordinated – using both cyber-psychological and cyber-technical means can be expected – from highly believable deepfakes to attacks that cripple a range of CNI targets (probably using previously planted malware). NATO states may then be unable to function as states. And if the state cannot function, then how can its military organisations? How then can NATO 'win' in a major kinetic conflict with Russia? And it may all be down to *mere* information.

References

[1] R. Morgus, B. Fonseca, K. Green, A. Crowther. (2019). *Are China and Russia on the cyber offensive in Latin America and the Caribbean?: A review of their cyber capabilities and implications for the US and its partners in the region*. [Online]. Available: https://www.newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean [Accessed: Nov. 27, 2023].

[2] R. Thornton, M. Miron. (2022). Winning future wars: Russian offensive cyber and its vital importance in Moscow's strategic thinking, *Cyber Defense Review*, Summer, pp. 117–125. [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: Dec. 15, 2023].

[3] A. Polyakova. (Nov. 15, 2018). Weapons of the weak: Russia and AI-driven asymmetric warfare, *Brookings*. [Online]. Available: https://www.brookings.edu/articles/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/. [Accessed: Dec. 11, 2023].

[4] J. Jashibekova. (Mar. 24, 2011). *Igor' Panarin: V informatsionnykh Voynakh u Rossii Dolzhen Byt' krepkii shchit IO.* [Online]. Available: https://aif.ru/society/igor_panarin_v_informacionnyh_voynah_u_rossii_dolzhen_byt_krepkiy_schit_i_o. [Accessed: Jan. 9, 2024].

[5] M.J. Mazarr, B. Frederick, Y.K. Crane. (2022). *Understanding a new era of strategic competition.* Santa Monica, CA: RAND. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA200/RRA290-4/RAND_RRA290-4.pdf. [Accessed: Dec. 15, 2023].

[6] S. Duguin, P. Pavlova. (Sep. 2023). *The role of cyber in the Russian war against Ukraine: Its Impact and the consequences for the future of armed conflict.* [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf. [Accessed: Nov. 27, 2023].

[7] V. Medinsky. "Ivan Groznyi I informatsionnaya Voyna", *Pravmir*, 06 Oct. 2016. [Online]. Available: https://www.pravmir.ru/ivan-groznyiy-i-informatsionnaya-voyna-video. [Accessed: Jan. 9, 2024].

[8] E. Messner. *Myatezh – Imya tretei mirovoi voyny.* Moscow: Moscow Publishing House, 1960.

[9] Kommersant, "Who is Igor Panarin," Apr. 25, 2006. [Online]. Available: https://www.kommersant.ru/doc/669611. [Accessed: Dec. 11, 2023].

[10] J. Darczewska, "The anatomy of Russian information warfare. The Crimean operation, a case study," *OSW Point of View*, no. 42, 2014. [Online]. Available: https://aei.pitt.edu/57173/1/42.pdf. [Accessed: Dec. 15, 2023].

[11] I. Panarin, *Pervaya mirovaya informatsionnaya voyna: Razval SSSR.* Saint Petersburg: Piter, 2010.

[12] V.V. Selivanov, Y.D. Il'yin, "Kontseptsiya voennotekhnicheskogo asimmetrichnogo otveta po sderzhivaniyu veroyatnogo protivnika ot razvyazyvaniya voennykh konflikov," *Voennaya Mysl*, no. 2, pp. 31–47, 2022.

[13] I. Fazletdinov, V.I. Lumpov, "Rol' Raketnykh voisk strategicheskogo naznacheniya v protivodeystvii strategicheskoi mnogosfernoi operatsii NATO," *Voennaya Mysl*, no. 3, pp. 53–56, 2023.

[14] A. Mitrofanov, "Zakat yadernoi triady. Oruzhie SShA dlya naneseniya obezglavlivayushshego udara," *Voennoe Obozrenie*, 15 Jan. 2020. [Online]. Available: https://topwar.ru/166706-zakat-jadernoj-triady-oruzhie-ssha-dlja-nanesenija-obezglavlivajuschego-udara.html. [Accessed: Nov. 27, 2023].

[15] J. Foreman, "Russia will not attack NATO," *The Spectator*, 09 Mar. 2024. [Online]. Available: https://www.spectator.co.uk/article/russia-will-not-attack-nato/. [Accessed: Jan. 9, 2024].

[16] G. Austin, N. Khaniejo, "Impact of the Russia–Ukraine war on national cyber planning: A survey of ten countries," *The International Institute for Strategic Studies*, Dec. 2024. [Online]. Available: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/01/impact-of-the-russiaukraine-war-on-national-cyber-planning_a-survey-of-ten-countries.pdf. [Accessed: Dec. 15, 2023].

[17] A.V. Il'nitsky, "Mental'naya Voyna Rossii," *Voennaya Mysl*, no. 8, pp. 19–33, 2021.

[18] RBC. (Mar. 20, 2024). *Sovetnik shoygu zayavil o razrabotke NATO kognitivno-mental'nykh tekhnologiy*. [Online]. Available: https://www.rbc.ru/politics/20/03/2024/65fa3ad79a7947f594c076d6. [Accessed: Dec. 11, 2023].

[19] RIA Novosti. (Feb. 22, 2017). *Baluyevsky: Pobeda v informatsionnoi voine vazhnee, chem v klassicheskoi*. [Online]. Available: https://ria.ru/20170222/1488611839.html. [Accessed: Nov. 27, 2023].

[20] V. Gerasimov, "Tsennost' Nauki v Predvidenii," *Voenno- Promyshlenyi Kur'er*, 27 Feb. 2013. [Online]. Available: http://www.vpk-news.ru/articles/14632. [Accessed: Nov. 27, 2023].

[21] S.G. Chekinov, S.A. Bogdanov, "Vliyaniye asimmetricheskikh deystviy na sovremennuyu bezopasnost' Rossii," *Vestnik Akademii Voennykh Nauk*, no. 1, pp. 46–53, 2010.

[22] S.A. Bogdanov, S.G. Chekinov, "Asimmetrichnye deistviya po obespecheniyu voennoi bezopasnosti Rossii," *Voennaya Mysl*, no. 3, pp. 13–22, 2010.

[23] A. Barthosh. (Aug. 12, 2021). *Gibridnaya, skrytnaya, nepredskazuyemaya, Nezavisimoye Voennoye Obozreniye*. [Online]. Available: https://nvo.ng.ru/gpolit/2021-08-12/1_10_11_1153_hybrid.html. [Accessed: Dec. 15, 2023].

[24] A. Barthosh, "Informatsionno-psikhologicheskaya bor'ba obretaet novye sredstva," *Nezavisimoye Voennoe Obozreniye*, 28 Sep. 2023. [Online]. Available: https://nvo.ng.ru/concepts/2023-09-28/1_1255_propaganda.html. [Accessed: Nov. 27, 2023].

[25] S.P. Rastorguev. (1999). Informatsionnaya voyna: Problemy I modeli. Moscow: Radio and Communication. [Online]. Available: https://community.apan.org › __key › docpreview-s. [Accessed: Nov. 27, 2023].

[26] B. DeWees, T.C. Pierce, E.J. Rokke, A. Tingle, "Toward a unified metric of kinetic and nonkinetic actions," *Joint Force Quarterly*, no. 85, 2017. [Online]. Available: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-85/jfq-85_16-21_DeWees-et-al.pdf. [Accessed: Dec. 11, 2023].

[27] President of the Russian Federation. (Dec. 31, 2015). *Strategiya natsional'noi bezopasnosti Rossiiskoi federatsii,* Moscow: The Kremlin. [Online]. Available: https://rg.ru/documents/2015/12/31/nac-bezopasnost-site-dok.html. [Accessed: Dec. 15, 2023].

[28] I. Panarin, Informatsionnaya voyna i geopolitika [Information war and geopolitics], Moscow: Pokolenie, 2006.

[29] V.M. Burenok, E.V. Gorgola, S.F. Vykulov. (2015). *Natsional'naya bezopasnost' Rossii v epokhy setevykh voin*, Moscow: Granitsa. [Online]. Available: https://sc.mil.ru/files/morf/military/archive/VIE-41.pdf. [Accessed: Nov. 27, 2023].

[30] V.V. Izonov, "On the issue of political mechanisms to counter external threats to Russia' military security," *Nauka, Obshestvo, Oborona*, vol. 6, no. 1, 2016. [Online]. Available: https://www.noo-journal.ru/nauka-obshestvo-oborona/2016-1-6/article-0059/. [Accessed: Dec. 11, 2023].

[31] A.V. Manoilo, "Informatsyonno-psikhologicheskaya voyna: Faktory, opredelayushchiye format sovremennogo vooruzhennogo konflikta." Materials of the V International Scientific and Practical Conference on Information Technologies and Security, no. 8, Kyiv, 2005, pp. 73–80.

[32] S.P. Rastorguev, M.V. Litvinenko, *Informatsionnye operatsii v seti internet*. Moscow: ANO Tsentr Strategicheskikh Otsenok I Prognozov, 2014.

[33] A. Khramchikhin, "Novyi Sposob Vedeniya Voyn," *Voenno-Promyshlennyi Kur'er*, 17 Feb. 2020. [Online]. Available: https://vpk.name/news/375164_novyi_sposob_vedeniya_boya.html. [Accessed: Dec. 15, 2023].

[34] S. Shandler, M.L. Gross, D. Canetti, "Cyberattacks, psychological distress, and military escalation: An internal meta-analysis," *Journal of Global Security Studies*, vol. 8, no. 1, pp. 1–19, 2023, doi: 10.1093/jogss/ogac042.

[35] A. Greenberg, "Hackers hit Macron with huge email leak ahead of French elections," *Wired*, 05 May 2017. [Online]. Available: https://www.wired.com/2017/05/macron-email-hack-french-election/. [Accessed: Nov. 27, 2023].

[36] D.V. Gioe, "Cyber operations and useful fools: The approach of Russian hybrid intelligence," *Intelligence and National Security*, vol. 33, no. 7, pp. 954–973, 2018, doi: 10.1080/02684527.2018.1479345.

[37] H. Tanriverdi, F. Flade, L. Frey. (Feb. 17, 2022). *The elite hackers of the FSB*. [Online]. Available: https://interaktiv.br.de/elite-hacker-fsb/en/index.html. [Accessed: Dec. 11, 2023].

[38] A. Soldatov, I. Borogan, "Kibersily Rossii: Kak eto rabotayet," *Agentura.ru*, 2022. [Online]. Available: https://agentura.ru/investigations/kibersily-rossii-kak-jeto-rabotaet/. [Accessed: Jan. 16, 2024].

[39] A. Scarsi, "Prigozhin's corporate network 'aims at destabilising' the west with 'information warfare'," *Daily Express,* 26 Jul. 2023. [Online]. Available: https://www.express.co.uk/news/world/1795164/Yevgeny-Prigozhin-threat-western-democracies-information-warfare. [Accessed: Dec. 15, 2023].

[40] M. Simonyan, "Simonyan: Informatsiya kak oruzhye ispol'zuyetsya temi, kto imeet vozmozhnost'," *Rossiyskaya Gazeta,* 03 Jul. 2013. [Online]. Available: https://rg.ru/2013/07/03/simonian.html. [Accessed: Jan. 9, 2024].

[41] 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: Nov. 27, 2023].

[42] A.S. Bowen, "Russian cyber units," *Congressional Research Service*, 02 Feb. 2022. [Online]. Available: https://sgp.fas.org/crs/row/IF11718.pdf. [Accessed: Dec. 11, 2023].

[43] H. Warrell, M. Seddon, K. Manson, "Russia military unit accused of Georgia cyber attacks," *Financial Times*, 24 Feb. 2020. [Online]. Available: https://www.ft.com/content/14377b84-53e3-11ea-90ad-25e377c0ee1f. [Accessed: Dec. 15, 2023].

[44] A. Troianovski, E. Nakashima, "Russia's military intelligence agency became the covert muscle in Putin's duels with the west," *The Washington Post*, 27 Dec. 2018. [Online]. Available: https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html. [Accessed: Nov. 27, 2023].

[45] M. Roache, S. Tewa, A. Cadier, Ch. Labbe, V. Padovese, et al., "Russia-Ukraine disinformation tracking center: 470 websites spreading war disinformation and the top myths they publish," *Newsguard*, 24 May 2024. [Online]. Available: https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/. [Accessed: Dec. 11, 2023].

[46] A. Greenberg, *Sandworm: A new era of cyberwar and the hunt for Kremlin's most dangerous hackers.* New York, NY: DoubleDay, 2020.

[47] A. Greenberg, "This Is the new leader of Russia's infamous sandworm hacking unit," *Wired*, 15 Mar. 2023. [Online]. Available: https://www.wired.com/story/russia-gru-sandworm-serebriakov/. [Accessed: Dec. 11, 2023].

[48] J. Hultquist, "Sandworm team and the Ukrainian power authority attacks," *Mandiant*, 07 Jan. 2016. [Online]. Available: https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team. [Accessed: Jan. 16, 2024].

[49] United States Department of Justice. (Oct. 19, 2022). *Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace.* [Online]. Available: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and. [Accessed: Jan. 9, 2024].

[50] D.E. Sanger, N. Perlroth, "Russian intelligence hackers are back, microsoft warns, aiming at officials of both parties," *The New York Times*, 10 Sep. 2020. [Online]. Available: https://www.nytimes.com/2020/09/10/us/politics/russian-hacking-microsoft-biden-trump.html. [Accessed: Dec. 11, 2023].

[51] J. Przetacznik, S. Tarpova. (Jun. 08, 2022). *Russia's war on Ukraine: Timeline of cyber-attacks.* [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549. [Accessed: Dec. 15, 2023].

[52] M. Burgess, "A mysterious satellite hack has victims far beyond Ukraine," *Wired*, 23 Mar. 2022. [Online]. Available: https://www.wired.com/story/viasat-internet-hack-ukraine-russia. [Accessed: Jan. 9, 2024].

[53] C. Albon, "Experts say Russia's use of counterspace capabilities could make 2022 a 'pivotal' year for space security," *Defense News*, 04 Apr. 2022. [Online]. Available: https://www.defensenews.com/battlefield-tech/space/2022/04/04/experts-say-russias-use-of-counterspace-capabilities-could-make-2022-a-pivotal-year-for-space-security/. [Accessed: Nov. 27, 2023].

[54] A.J. Vicens, "UK, EU, US formally blame Russia for Viasat satellite hack before Ukraine invasion," *Cyberscoop*, 10 May 2022. [Online]. Available: https://cyberscoop.com/viasat-hack-russia-uk-eu-us-ukraine/. [Accessed: Dec. 11, 2023].

[55] V. Zhora. (May 18, 2022). *How to ride a bear – Russian cyber posture and security implications*, CyberSec Forum/Expo, Katowice, Poland. [Online]. Available: https://www.youtube.com/watch?v=lI7PQP_IcdA. [Accessed: Dec. 15, 2023].

[56] J. Bateman. (Dec. 16, 2022). *Russia's wartime cyber operations in Ukraine: Military impacts, influences, and implications*, Carnegie Endowment for International Peace, Washington, DC, Paper. Available: https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en&center=global [Accessed: Jan. 16, 2024].

[57] L. Collins, M. Kofman, J. Spencer, "The battle of Hostomel airport: A key moment in Russia's defeat in Kyiv," *War on the Rocks*, 10 Aug. 2023. [Online]. Available: https://warontherocks.com/2023/08/the-battle-of-hostomel-airport-a-key-moment-in-russias-defeat-in-kyiv/. [Accessed: Dec. 11, 2023].

[58] A. Molchanova, "V Provedenii IPsO Protiv Ukrainy Zadeystvovany GRU, FSB I Prigozhinskiye Trolli – Kak Oni Deistvuyut. Intervyu s Polkovnikom VSU," *Obozrevatel*, 14 Dec. 2022. [Online]. Available: https://war.obozrevatel.com/polkovnik-vsu-taras-dzyuba-ipso-kak-rossiya-provodit-informatsionnyie-operatsii-protiv-ukrainyi.htm. [Accessed: Jan. 16, 2024].

[59] T. Simonite, "A Zelensky deepfake was quickly defeated. The next one might not be," *Wired*, 17 Mar. 2022. [Online]. Available: https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/. [Accessed: Nov. 27, 2023].

[60] D. Black, G. Roncone, "The GRU's disruptive playbook," *Mandiant*, 12 Jul. 2023. [Online]. Available: https://www.mandiant.com/resources/blog/gru-disruptive-playbook. [Accessed: Dec. 11, 2023].

[61] K. Proska, J. Wolfram, J. Wilson, D. Black, K. Lunden, et al., "Sandworm disrupts power in Ukraine using a novel attack against operational technology," *Mandiant*, 09 Nov. 2023. [Online]. Available: https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology. [Accessed: Jan. 9, 2024].

[62] A. Greenberg, "Sandworm hackers caused another blackout in Ukraine–During a missile strikes," *Wired*, 09 Nov. 2023. [Online]. Available: https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/. [Accessed: Jan. 16, 2024].

[63] J. Pearson, "Russian spies behind cyber attack on Ukraine power grid in 2022 – Researchers," *Reuters*, 11 Nov. 2023. [Online]. Available: https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/. [Accessed: Dec. 15, 2023].

[64] P. Muncaster, "Microsoft warns of destructive malware campaign targeting Ukraine," *Infosecurity Magazine*, 17 Jan. 2022. [Online]. Available: https://www.infosecurity-magazine.com/news/microsoft-destructive-malware/. [Accessed: Dec. 11, 2023].

[65] Microsoft Threat Intelligence. (Jun. 14, 2023). *Cadet Blizzard emerges as a novel and distinct Russian threat actor.* [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/. [Accessed: Nov. 27, 2023].

[66] A.J. Vincens, "Microsoft identifies new hacking unit within Russia's military intelligence," *Cyberscoop*, 14 Jun. 2023, [Online]. Available: https://cyberscoop.com/microsoft-gru-russia-ukraine-hacking/. [Accessed: Dec. 15, 2023].

[67] K. Giles, "Russian cyber and information warfare in practice," *Chatham House*, 14 Dec. 2023. [Online]. Available: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice. [Accessed: Jan. 9, 2024].

[68] RBC. (Nov. 1, 2023). *Glava minzyfry podderzhal sozdaniye kibervoisk*. [Online]. Available: https://www.rbc.ru/rbcfreenews/654224319a79471580f33da6. [Accessed: Jan. 16, 2024].

[69] V. Kiselev, A. Kostenko, "Kibervoyna kak Osnova Gibridnoi Operatsii," *Armeiskii Sbornik*, vol. 11, no. 257, pp. 3–6, 2015. [Online]. Available: https://sc.mil.ru/files/morf/military/archive/AS_11_2015.pdf. [Accessed: Dec. 11, 2023].

[70] P.I. Antonovich, "O sushhnosti I soderzhanii kibervoyny," *Voennaya Mysl*, no. 7, pp. 39–46, 2011.

[71] R. Hastings, "Why Russia's cyber warfare has failed in Ukraine – But remains a threat to the UK," *I News*, 16 Jun. 2023. [Online]. Available: https://inews.co.uk/news/technology/russia-cyber-warfare-failed-ukraine-threat-uk-2404924. [Accessed: Dec. 15, 2023].

[72] D. Vergun, "Partnering with Ukraine on cybersecurity paid off, leaders say," *DOD News*, 03 Dec. 2022. [Online]. Available: https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/. [Accessed: Dec. 11, 2023].

[73] M. Kofman, R. Connolly, J. Edmonds, A. Kendall-Taylor, S. Bendett, "Assessing Russian state capacity to develop and deploy advanced military technology," *Center for a New American Security*, 21 Oct. 2022. [Online]. Available: https://www.cnas.org/publications/reports/assessing-russian-state-capacity-to-develop-and-deploy-advanced-military-technology. [Accessed: Nov. 27, 2023].

[74] N. Eftimiades, "Small satellites: The implications for national security," *Atlantic Council*, 05 May 2022. [Online]. Available: https://www.atlanticcouncil.org/in-depth-research-reports/report/small-satellites-the-implications-for-national-security/. [Accessed: Jan. 9, 2024].

[75] J. Pavur, I. Martinovich, "The cyber-ASAT: On the impact of cyber weapons in outer space," *IEEE Xplore*, May 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8756904. [Accessed: Jan. 16, 2024].

[76] D.T. Burbach, "Early lessons from the Russia-Ukraine war as a space conflict," *Atlantic Council*, 30 Aug. 2022. [Online]. Available: https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/early-lessons-from-the-russia-ukraine-war-as-a-space-conflict/. [Accessed: Dec. 11, 2023].

[77] J. Menn, "Cyberattack knocks out satellite communications for Russian military," *Washington Post*, 30 Jun. 2023. [Online]. Available: https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/. [Accessed: Jan. 9, 2024].

[78] E. Howell, "Elon Musk says Russia is ramping up cyberattacks on SpaceX's Starlink systems in Ukraine," *Space*, 14 Oct. 2022. [Online]. Available: https://www.space.com/starlink-russian-cyberattacks-ramp-up-efforts-elon-musk. [Accessed: Nov. 27, 2023].

[79] European Space Policy Institute. (Oct. 10, 2022). *The war in Ukraine from a space cybersecurity perspective*. [Online]. Available: https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf. [Accessed: Dec. 11, 2023].

[80] D. Goward, "Why isn't Russia doing more to jam GPS in Ukraine?", *C4ISRNET*, 22 Jul. 2022. [Online]. Available: https://www.c4isrnet.com/opinion/2022/07/22/why-isnt-russia-jamming-gps-harder-in-ukraine/. [Accessed: Dec. 15, 2023].

[81] R. Thomas, "Russian aggression shows the west's GNSS weakness," *Army Technology*, 19 Aug. 2022. [Online]. Available: https://www.army-technology.com/interviews/russian-aggression-shows-the-wests-gnss-weakness/. [Accessed: Jan. 9, 2024].

[82] A.R. Sarkar, "China building cyber weapons to 'seize control' of enemy satellites, says leaked CIA report," *The Independent*, 21 Apr. 2023. [Online]. Available: https://www.independent.co.uk/asia/china/cyber-weapon-satellite-cia-report-b2324222.html. [Accessed: Nov. 27, 2023].

[83] R. Thornton, M. Miron, "Towards the 'third revolution in military affairs': The Russian military's use of AI-enhanced cyber warfare," *RUSI Journal*, vol. 165, no. 3, pp. 12-21, 2020, doi: 10.1080/03071847.2020.1765514 [Online]. Available: https://rusi.org/publication/rusi-journal/towards-%E2%80%98third-revolution-military-affairs%E2%80%99-russian-military%E2%80%99s-use-ai. [Accessed: Jan. 16, 2024].

[84] L. Hay Newman, "AI-generated voice deepfakes aren't scary good – Yet," *Wired*, 15 Mar. 2023. [Online]. Available: https://www.wired.com/story/ai-voice-deepfakes/. [Accessed: Jan. 9, 2024].