SSOAR

Open Access Repository
www.ssoar.info

Cyber operations in Russia's war against Ukraine: uses, limitations, and lessons learned so far

Schulze, Matthias; Kerttunen, Mika

Veröffentlichungsversion / Published Version
Stellungnahme / comment

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

Empfohlene Zitierung / Suggested Citation:
Schulze, M., & Kerttunen, M. (2023). *Cyber operations in Russia's war against Ukraine: uses, limitations, and lessons learned so far.* (SWP Comment, 23/2023). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2023C23

Nutzungsbedingungen:
Dieser Text wird unter einer Deposit-Lizenz (Keine Weiterverbreitung - keine Bearbeitung) zur Verfügung gestellt. Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.
Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

Terms of use:
This document is made available under Deposit Licence (No Redistribution - no modifications). We grant a non-exclusive, non-transferable, individual and limited right to using this document. This document is solely intended for your personal, non-commercial use. All of the copies of this documents must retain all copyright information and other information regarding legal protection. You are not allowed to alter this document in any way, to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public.
By using this particular document, you accept the above-stated conditions of use.

gesis Leibniz-Institut für Sozialwissenschaften

Mitglied der Leibniz-Gemeinschaft

Diese Version ist zitierbar unter / This version is citable under:
https://nbn-resolving.org/urn:nbn:de:0168-ssoar-88112-1

SWP Comment
NO. 23 APRIL 2023

Cyber Operations in Russia's War against Ukraine

Uses, limitations, and lessons learned so far

Matthias Schulze and Mika Kerttunen

One year after Russia's invasion of Ukraine, certain assumptions about the utility of cyber operations during wartime can now be put to the test. Russian cyber salvos opened this war, but they failed to achieve their objectives in the face of a resilient cyber defender. Joint cyber/conventional warfighting is still hard to implement due to its uncertain effects, the potential for spill-over, malware development cycles, and differing operational tempos. Cyber operations against Ukraine have not (yet) achieved major strategic effects in reducing Ukraine's capacity to resist. Additionally, Russian information operations targeting Ukrainian and Western audiences fell on deaf ears. The greatest value of cyber operations therefore still appears to lie in their intelligence and reconnaissance functions.

Since the early 1990s, cyber warfare has been heralded by its proponents as a revolution in military affairs or a perfect weapon of war. Most of these discussions have been theoretical, often focusing on questions of how the application of cyber capabilities might meet or exceed the threshold of an armed attack and thus lead to conventional war. Yet few empirical studies examine the military operational utility of cyber capabilities *during* war. Over the past year of war in Ukraine cyber capabilities have been employed in the midst of a conventional war, allowing us to draw preliminary conclusions about the potential game-changing nature of cyber capabilities when used as an instrument of war.

Three Western schools of thought

Cyber capabilities and wartime strategy

Literature on 'cyber warfare' is usually concerned with the application of cyber capabilities for politico-strategic or even criminal purposes rather than military operational ones. The *strategic cyber war narrative* of the 1990s saw cyber warfare as a next-generation front that would threaten modern society. One of the guiding frames of reference was the "Cyber Pearl Harbor" metaphor: With digital decapitation strikes, the power grid could be shut down, critical infrastructure destroyed, and entire economies brought to a halt all without the need

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

for physical military force. Within this narrative, cyber operations were seen as a strategic counter-value capability that would target societies with the aim of affecting state behaviour during peacetime. In a nutshell, cyber operations were expected to alter the balance of power in the international system because they were perceived to be superior to conventional force.

As the field matured, however, expectations scaled down. Scholars like Martin C. Libicki pointed out that when it comes to the objectives of war, cyber war cannot disarm, "much less destroy", the enemy. Moreover, in the absence of physical combat and violence, cyber warfare cannot result in territorial gains, which can still be considered one of the primary objectives of most modern wars. Furthermore, it is hard to bend an adversary to one's will — the famous Clausewitzian purpose of war — by relying on digital means alone. Research has also shown that strategic attacks against civilians rarely contribute to war-winning objectives, and secondly, are difficult to orchestrate against thousands of different systems that control critical functions of modern societies. Unlike conventional weaponry, many cyber operations are target-dependent, meaning they cannot be used indiscriminately against any system, which complicates operational planning. Furthermore, with such complex attack chains, there is always the risk of failure and unintended cascade effects that could actually backfire on the attacker.

Cyber capabilities on the battlefield

Since the mid-2000s, cyber warfare has not been seen as a standalone capability that elicits effects independent of kinetic conflict, but rather as a compliment to conventional capabilities. In other words, cyber operations can serve as a *force enabler/multiplier* for conventional capabilities when used in a joint and combined fashion. Here, cyber operations in war are not necessarily measured by their strategic effects but are rather seen as a *counter-force capability* that can be directed against enemy armies. One example is the X-Agent malware that infiltrates targeting equipment that guides artillery fire and then leaks the geolocation of artillery positions to enemy forces, which then directs counter-battery fire. Within this conceptualisation of cyber capabilities, the application of cyber means matches well with the ideals of manoeuvre warfare and paralysing the enemy with surgical or acupunctural strikes.

While studies show that military hardware has plenty of vulnerabilities that can be exploited by cyber operations in theory, in practice, this is hard to operationalise. A study by Nadiya Kostyuk and Yuri M. Zhukov on the use of Distributed Denial-of-Service attacks and kinetic military operations in Syria (2013) and eastern Ukraine (2014) shows that timing is often off in joint operations. Conventional attacks and disruptive cyber operations have different planning times and different operational tempos, which makes it hard to achieve joint effects. Malware, for example, has lifecycles: It must first be developed, tested, and then deployed toward adversary IT to produce effects until it is discovered and mitigated. This takes time, often weeks or months. In principle, a single software update or change in configurations on the part of the defender has the potential to nullify the effect of malware. Malware is much more target-specific than bullets. Lastly, to synchronise its effects with ground operations, malware might need live command and control connections to the outside world, which might be infeasible in a combat environment that employs active electronic warfare interference. Therefore, a cyber operation might be useful in the early stages of war as a type of first strike, but the longer that hostilities last, the harder it is to keep operational stockpiles of functional malware and to maintain backdoor access to adversary systems.

Additionally, it is difficult to coordinate manoeuvres between conventional and cyber forces. First, conflicting goals are an issue: intelligence-oriented actors tend to favour hidden long term access to a system (cyber espionage or presence-based opera-

tions) over short-term disruptions of systems (so-called cyber-effect operations), which will likely lead to the discovery of the used backdoor and thus burn the capability. Second, the geographies of the digital and conventional battlefields rarely align. The US learned this with Operation Glowing Symphony as it targeted ISIS's digital infrastructure. ISIS relied on digital services in dozens of countries and the take-down/takeover of these assets by way of cyber operations needed to be coordinated with allies and third-party countries. Furthermore, ISIS proved to be cyber resilient; it quickly rebuilt its disabled infrastructure. Operation Glowing Symphony showed that not ad hoc, but continuous cyber engagement is more effective, and that the utility of cyber operations in war lies less in their disruptive or destructive effects, but more in their intelligence collection and psychological capabilities. If an adversary fears that their network is compromised and someone is listening to them, they will switch to other means of communication, thus slowing and complicating their operational planning. Erica D. Borghard and Shawn W. Lonergan conclude that another utility of cyber operations in war might be their ability to target logistic systems, as these are often civil and less secure than military systems. Still, many conclude that cyber capabilities work best for intelligence and reconnaissance functions and do not replace conventional weapons. In many instances, it is quicker, simpler, and less costly — and more effective — to neutralise a target with airstrikes or artillery fire, rather than by way of a cyber-effect operation.

Cyber capabilities between peace and war

Since around 2014, much emphasis has been placed on the *hybrid* or *grey zone* nature of cyber capabilities. Within this understanding, cyber activity is perceived not as a destructive force of war, but as an intelligence contest or strategic competition in which the primary goal is not to disable armies but to subvert, exploit, and shape the cyber and information environment. More so, the main utility of cyber operations is the theft or manipulation of information for political, economic, or even criminal purposes. The effect of these operations on the balance of power within this narrative is twofold: First, they can be used to influence political discourse and processes, for example, weakening Western democracies in peacetime; and second, they can allow attackers to reap strategic gains in the form of long-term cyber espionage, as seen in the Chinese or North-Korean model of cyber-statecraft.

This reading of cyber operations is heavily inspired by two trends: Firstly, under international law, most cyber operations are not seen to meet the legal criteria of use of force or an armed-attack, and thus cannot be used to justify the self-defence clause under Article 51 of the UN Charter. In many cases, cyber operations are intentionally designed to fall below the threshold of war, not risking escalation of armed or violent retaliation, much less war proper. Similarly, the defender might also have an interest in not escalating its response to such activity. Secondly, the normative narrative surrounding cyber activity has been shaped by Russia's application of such capabilities since its 2014 annexation of Crimea, and through to its attempts to meddle in the 2016 US presidential elections.

Expectations before the Russia-Ukraine war

Before Russia's physical invasion of Ukraine, many intelligence agencies expected some sort of digital first strike. In its invasion of Georgia in 2008, Russia used large-scale Distributed Denial-of-Service attacks to temporarily overload and disrupt the Georgian government and media websites as Russian troops crossed the border. One goal of this approach was to thwart Georgian communication with the wider world, and thereby to shroud the situation in the proverbial fog of war. Over the years, Russia has

cultivated its image as a "larger than life" cyber power that has dramatically beefed up its game. Russian Advanced Persistent Threat (APT) actors seemed to infiltrate networks everywhere, from government agencies and electoral processes through to critical infrastructure, the latter of which caused two power outages in Ukraine (via the Blackenergy and Industroyer malwares). In this context, many in the intelligence community expected cyber operations to lay the groundwork for Russia's conventional invasion by, for example, disabling the power grid, communications systems, or government ministries. Indeed, "all of those systems have been Russian targets in the past six years", as David Sanger wrote in the *New York Times* in February 2022, basing his evaluation on a secret intelligence assessment. Suddenly, the *Cyber Pearl Harbor* metaphor was back on the table. Disabling these essential systems en masse would make military sense as it would hamper Ukraine's ability to coordinate its defences. Some also feared unintentional spill-over effects from indiscriminate malware — as seen with Not-Petya a few years earlier — which could accidentally draw other parties into the conflict. Still, CrowdStrike's Dimitri Alperovitch scaled-down expectations, arguing, "Russia is likely to conduct three types of campaigns in cyberspace to support its military objectives: intelligence gathering operations, operations aimed at disrupting or deceiving the Ukrainian military, and psychological operations against the Ukrainian public."

Russia's application of cyber and information warfare capabilities against Ukraine in 2022

The total number of operations within the Russia-Ukraine war may not be known, but in August 2022, the Computer Emergency Response Team of Ukraine (CERT-UA) reported over 1,123 cyberattacks in the first half of the war. This represents a three-fold increase in cyber activity to the pre-war period. In January 2023 CERT-UA reported that it responded to more than 2,194 attacks. Still, the estimated number of unreported or unpublished cases remains unclear. Within the framework of the European Repository of Cyber Incidents project, we tracked numerous incidents as well. There are lessons to be learned from the way Russia has employed cyber and information means — and the way Ukraine has managed to avert or rein in the attacks.

Cyber operations require preparation

As was expected by researchers, intelligence gathering seems to be the primary utility of cyber operations (also) in war. Russian intelligence's preparation of the battlefield started well before the February 2022 offensive commenced. Intelligence informing either conventional or digital strikes was collected in advance, likely assisting the Russian federal military intelligence agencies and armed forces in identifying targets. Russian network reconnaissance increased in quality and quantity in late 2021. Linked to the Russian Foreign Intelligence Service (SVR), the APT group Nobelium was identified as one rather active actor in this regard since May 2021. Also, during this time, Russian state actors and affiliated threat actors made continual attempts to compromise Ukrainian communication, transportation, energy, defence, administrative, and diplomatic systems and services. Also, Russia's Federal Security Service (FSB) groups have been involved in cyberattacks and intelligence activities targeting Ukraine.

Prebunking and open-source intelligence

Before hostilities broke out, Russia made numerous attempts to fabricate a *casus belli*. This includes multiple Russian information operations on Telegram and Twitter that tried to paint Ukraine as an attacker while Russia merely tried to defend itself. Across traditional and social media, Ukraine and the US have been accused of manufacturing biological weapons in secret laboratories, a recycled story from the 1980s that was also

regurgitated when Russia invaded Georgia in 2008. Moreover, videos displaying alleged Ukrainian sabotage of Russian targets and Ukraine's supposed shelling of a Kindergarten surfaced online just days before Russia's invasion. Nonetheless, these attempts to shape public perception were quickly debunked by the Open Source Intelligence community as it conducted forensic analyses of the material. The US intelligence community also engaged in efforts to "prebunk" Russian narratives, countering them in advance.

A cyber-opening salvo

On 23 February 2022, one day before the invasion, the Russian military intelligence agency (GRU) launched several destructive data-wiping cyberattacks against the Ukrainian government and other IT, energy, and financial organisations. These attacks were meant to support the coming land and air strikes. By deleting data on government systems, Russia was likely attempting to slow the coordination of Ukrainian defence forces and government services. It was expected that cyber capabilities could be used in this way in the run-up to the war, but this use of highly-destructive wiper malware in multiple iterations had a new quality to it. The wiper malware capabilities also showed how far cyber warcraft had evolved since the war in Georgia 2008.

Even for successful hacks, results are uncertain

Moreover, Russia's 24 February 2022 attack on Viasat satellite communications provides some interesting lessons. This cyber operation shut down satellite communication over Ukraine and Europe, creating unintended spill-over effects by deactivating the satellite modems of German wind turbines. Although the cyber operation was technically successful, it did not manage to hamper Ukrainian command and control and intelligence operations. Ukrainian officials later claimed that it actually had a negligible operational impact, as satellite communications were never the primary means of communication for the Ukrainian military but rather a redundancy option. Although Ukraine has a vested interest in belittling the effects of this attack, the Viasat example still leads us to conclude that:

a) it is hard to contain cyber operations against widely used systems without creating the risk of unintended spill-over when third parties are involved;
b) even a technically successful cyber operation might not achieve its goal, creating significant uncertainty for military planners who are relying on these effects in joint operations; and
c) in cyber warfare, defenders would do well to practice redundancy and have an analogue fall-back option that cannot be accessed by cyber operations.

Joint manoeuvre/cyber operations are difficult

Another finding of this analysis relates to the joint use of cyber and conventional operations towards common goals. For some, the Russian approach during the early stages of the war seemed chaotic. Russia's conventional military attacks have indiscriminately targeted civilian and societal targets that had no direct significance to ongoing tactical or operational manoeuvres. Moreover, an April 2022 Microsoft report observed that Russian state APT actors conducted cyber intrusions together with kinetic military action but the different types of attacks did not appear to function well in concert. Indeed, Russian cyberattacks targeted the same organisations and services that the conventional military fire, missiles, rockets, and bombs did, so as government data was hit by missiles, government on-premises computer networks were targeted by destructive data-wiping cyberattacks. While Microsoft noticed that Russian cyberattacks managed to disrupt technical services and to create a "chaotic information environment", it claims to be unable to evaluate the broader strategic impact of Russian cyber and information operations,

for example, those pushing for the erosion of public confidence and deterioration of the capacity of Ukrainian military defence.

Still, this reading of events is contested by many observers, such as security expert James A. Lewis, who bluntly commented that "all these hacking efforts [...] seem to have been poorly coordinated with Russian military actions in Ukraine." Gavin Wilde notes that the most advanced military cyber forces are still wrestling with how to effectively integrate cyber capabilities into conventional military operations, pointing out that "Russia doesn't appear to have done so thus far." Jon Bateman also concludes that "Russia seems unwilling or unable to plan and wage war in the precise, intelligence-driven manner that is optimal for cyber operations."

There are multiple reasons for this, such as poor strategy, insufficient intelligence preparation as well as over-burdening secrecy and mistrust that made inter-agency planning difficult. Like ground troops that did not know they were going to attack, Russian cyber and conventional forces seemed to lack the same joint preparation. The lesson to be learned is that cyber and conventional operations are hard — but not impossible — to coordinate.

Achieving physical effects with cyber means is difficult

In April 2022 researchers discovered Industroyer2, a malware designed to affect industrial control systems within Ukraine's energy grid. It represented an evolution of the same malware that knocked out Kyiv's power grid in 2016 for a few hours. So far, this is the only publicly known reference to malware that could potentially be designed to cause a physical impact in Ukraine (observers should keep in mind that many potentially impactful cyber incidents remain unknown due to secrecy). Incident responders were able to deactivate the Industroyer2 malware before its programmed timer was initiated. This malware shows cyber operations' potential to cause physical damage, but also their limitations. The effect was mitigated before it could do anything, undoing probably years of malware development. Conversely, conventional bombings were able to shut down more than 40 per cent of Ukraine's power grid. The finding is clear: In war, conventional means are often quicker, cheaper, and more precise, their outcomes more certain and — usually — more destructive than cyber operations.

Cyber operations did not produce strategic effects

Regardless of the type of attack, the main purpose of Russian cyberattacks seems to have been to cripple the Ukrainian state and society on a strategic level. Rather than destroying or inhibiting the Ukrainian military forces or weapon systems, Russian cyber operations targeted the overall will of the Ukrainian people and their capacity to defend themselves. Still, there is little evidence that these operations produced strategic effects such as Ukrainians' diminished will to resist. On the contrary, research shows that strategic attacks on civil infrastructure don't reduce an enemy's will to resist, but rather spark a rally around the flag effect that generates strong support for the defending country's leadership. This holds true for Ukraine: The early volleys of Russian cyber and conventional attacks on broadband internet access in the first days of the war were likely intended to isolate the Ukrainian government in the very moment of a major military offensive. While successful in Georgia in 2008, Russia failed this time.

The lack of strategic and military operational significance of Russia's cyber operations surprised many observers. According to James A. Lewis, Russia has been unable to disrupt "finance, energy, transportation, and government services to overwhelm defenders' decisionmaking and create social turmoil." After observing four months of the war, he went so far as to declare that "[c]yberattacks are overrated. While invaluable for espionage and crime, they are far from decisive in armed conflict." One of the likely reasons for this is that Ukraine learned

from and adapted to previous Russian cyber operations. It built capacities and a cyber workforce, streamlined interagency coordination, including the urgent reduction of bureaucratic barriers, and conducted cyber-range exercises to glean from Russian activity. As in all domains of warfare, constant learning, adaptation, and innovation are key.

Information operations win hearts and minds

Shot amid Russia's first cyber and conventional strikes that tried to neutralise Ukrainian leadership, President Volodymyr Zelensky's February 25 "we are all here" video message became one of the most impactful information operations in history. In these 37 seconds, the world realised that the Russians had not succeeded, and that the fight had just begun. Since then, the Ukrainian government has skillfully navigated the information environment, pursuing multiple goals whether by (successfully) rallying for international military and humanitarian aid or by mocking Russian incompetence online. It can be stated that, at least in the Western infosphere, Ukraine has won the battle for the hearts and minds — one of the primary psychological goals in any major war. This also led to an outpouring of support by international hacktivists communities that quickly joined the ranks of the IT Army of Ukraine, hacking into all sorts of Russian government and business infrastructure. As a result, there is now an unprecedented amount of leaked material on the notoriously secretive Russian state.

Nonetheless, the Russian state's oppressive information security practices have managed to insulate the domestic information sphere from Western influence. Moreover, despite being condemned by certain UN General Assembly resolutions, Russian diplomacy, anti-Western messaging, and military presence have all prevented many developing countries from expressing their resistance to the Russian invasion let alone offering their active support to Ukraine.

Cyber resilience is key

Ukraine's cyber defenders have shown skill and flexibility in fighting off Russian cyber operations. It is reported that some governmental networks were back in operation a mere hours after they had been deleted by wiper malware. This essentially nullified some of the strategic effects of the wiper operations. A few key takeaways observed in Ukraine's wartime cyber efforts include:

1) moving government data to faraway cloud storage creates resilience and enhances threat detection speeds;
2) Western threat intelligence sharing and threat-hunting activities were likely influential in uncovering many operations before they could trigger effects — Ukraine has been operating at a high tempo to pre-emptively use this knowledge to defend against coming attacks;
3) cyber operations seem to work best when they are unexpected, but when defenders are agile and proactively anticipate the coming moves, it becomes harder for the attacker.

Lessons learned

Russian cyber activities have primarily focused on intelligence gathering, data destruction, and Denial-of-Service attacks on critical infrastructure. Surprisingly, thanks to Ukraine's proactive cyber defence and societal resilience, this kind of cyber warfare has not produced significant strategic, operational, or tactical benefits for Russia, at least as far as we know publicly.

Still, just because Russia wasn't able to align its digital and analogue manoeuvres this time doesn't mean that others cannot learn from this failure and do so in the next major war. Nonetheless, better algorithms alone will not balance the inherent weaknesses of offensive cyber operations: they require excessive time, are target-dependent, and might simply fail against an agile, proactive defender. Although imperfect, cyber-defence is not futile, even against prolific attackers. To be successful, it requires flexi-

bility, speed, forward-thinking, useful threat intelligence, and streamlined interministerial processes to reduce information silos, as well as exercises and training. Defence planning in the cyber domain requires a whole-of-government-and-industry approach. When it comes to offensive wartime cyber operations, the uncertainty of war makes significant cyber-effects hard to achieve. One possible line of action may be to better align network operations with electronic warfare, information operations, intelligence operations, and physical destruction of key adversary nodes of communication, command and control, and logistics. This course would require extensive joint exercises. Policy and joint operations planners should also be modest in their planning: Cyber operations are useful for intelligence gathering, subversion and shaping information spheres, but they are not a substitution for decisive military force. Since the effects of cyber operations are target-dependent, military planners would do well to establish contingency plans in case they fail. Planners should also avoid overly complex attack chains wherein downstream conventional operations depend heavily on upstream cyber operations. For NATO, this means more joint training, and potentially the integration of cyber-ranges into operational planning.

Lastly, the full picture won't be known until after the war, when we can evaluate the significance of Russian information warfare in light of Russia and Ukraine's dependencies, intentions, and priorities, as well as their conventional and covert manoeuvres and counter-manoeuvres.

© Stiftung Wissenschaft und Politik, 2023
All rights reserved

This Comment reflects the authors' views.

The online version of this publication contains functioning links to other SWP texts and other relevant sources.

SWP Comments are subject to internal peer review, fact-checking and copy-editing. For further information on our quality control procedures, please visit the SWP website: https://www.swp-berlin.org/en/about-swp/quality-management-for-swp-publications/

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1861-1761
ISSN (Online) 2747-5107
DOI: 10.18449/2023C23

Dr Matthias Schulze is Deputy Head of the Security Research Division at SWP. Dr Mika Kerttunen is a Visiting Fellow at SWP. This paper is based on research conducted by the European Repository of Cyber Incidents (EuRepoC) Project, of which both authors are members.
The authors are grateful for valuable comments by James Lewis, Martin Libicki, Martin Müller, Tuomo Rusila, and Max Smeets, and the researchers at SWP's Security & Eurasia Research Divisions.