Chapter 11: The Cyber Dimension in Russia's War of Aggression against Ukraine

Arthur de Liedekerke and Kira Frankenthal

Abstract

The Russian war of aggression against Ukraine in 2022 is one of the world's first conventional conflicts between two states with advanced cyber capabilities. Although at first glance the cyber dimension of the war appears to be of small scale, Ukraine has been consistently affected by cyberattacks and the spread of disinformation. Nevertheless, the cyber situation has not developed as many experts expected. This chapter looks at the most significant developments to date, explains reasons for the steadfastness of Ukrainian cybersecurity, and identifies what to expect in cyberspace as the war continues.

Keywords

Russia-Ukraine war, cyberattacks, disinformation, deepfakes, cyberdefense, BSI, ENISA

1 Introduction

Cyberattacks have been part of modern warfare for some time. In fact, the Russians view cyber-enabled operations as both "an arm of the Russian propaganda machine and a means of creating and disseminating disinformation, as well as a tool for disrupting an adversary's critical infrastructure or military capabilities".[1]

With an invasion looming in early 2022, experts warned of Russia's distinctive cyber capabilities. These would have the potential to unleash a new wave of cyberattacks on Ukraine, with possible spillover outcomes affecting

1 Willet, Marcus: The Cyber Dimension of the Russia-Ukraine War, International Institute for Strategic Studies, 6 October 2022.

the rest of the world. Since the beginning of the war, however, opposing assessments of the character and significance of the cyber dimension in Russia's war against Ukraine can be observed, ranging from "full-scale cyberwar" to "conspicuously absent".

2 The Role of Cyber-Based Operations in Russia's War against Ukraine in 2022

Ukraine has not only been affected by Russian cyber operations since February 24, 2022. Already since the occupation of Crimea in 2014, the Kremlin has interfered in local elections, attacked Ukraine's critical infrastructure, successfully compromised government websites, and spread disinformation, among other things.

For years, Ukraine has been something of a test bed for Russian cyberattacks. Cyberweapons, some of them very advanced, have sometimes been particularly effective and in many ways unprecedented. For example, in 2015, the *BlackEnergy Malware* crippled Kyiv's power grid, triggering a major blackout in the middle of winter.[2] These and other devastating incidents in subsequent years, such as the *NotPetya* worm[3] are part of Moscow's longstanding efforts to destabilize its neighbor, hindering Ukraine's ability to operate in cyberspace, and maintain a decisive edge in cyberspace.

Even before the large-scale military offensive, Russia intensified its digital attacks on Ukrainian targets. A Microsoft report published at the end of April 2022 confirms that Russia-linked actors were probably already preparing for this since March 2021.[4] For example, websites of government institutions have been regularly defaced since late 2021. Hackers directly sponsored by the Kremlin, or very much aligned with its interests, released destructive *malware* – particularly data wipers – on government networks, including the Ministry of Foreign Affairs of Ukraine. On January 14, 2022, an ominous warning was disseminated on official Ukrainian websites, "Be

2 Zetter, Kim: "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", WIRED, 3 March 2016.

3 *NotPetya*, derived from the *Petya malware* that first appeared in 2016, was a highly destructive extortion software (*ransomware*) that was first used against Ukraine and affected thousands of businesses worldwide in mid-2017. Many countries have since accused the Russian government of being behind these attacks.

4 Digital Security Unit: Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine, Microsoft, 27 April 2022.

afraid and expect the worst".[5] Just a few hours before the invasion of Ukraine, Russia again attacked a number of key facilities in the country resulting in the computer systems of several government, military, and critical infrastructure sectors becoming severely dysfunctional. In many ways, this was similar to the attacks Russia carried out against Georgia in 2008 and during the invasion of Crimea in 2014.[6]

Since the beginning of the war in February 2022, the number of cyberattacks increased. The use of a full range of Russian cyberweapons could be observed: *Wiper Malware*, *Distributed Denial of Service* (DDoS; flooding a server with Internet traffic to prevent users from accessing the website in question), *phishing campaigns*, and, most notably, the disruption of satellite-based Internet services. The latter refers to a now infamous sabotage operation attributed to Russia[7] that partially took down the ground segment of *Viasat's* KA-SAT network, on which the Ukrainian military, intelligence, and police rely.[8]

As the war has progressed, the Kremlin has continued to ramp up its cyber operations, particularly those targeting attack critical infrastructure. A Russian cyberoperation against *Ukrtelecom* – a major national telecommunications operator – crippled communications services in Ukraine for several hours in late March.[9] In early April, *Industroyer2*, an enhanced variant of a malware that caused power outages in Kyiv in 2016, was identified and neutralized on the systems of one of the country's largest utilities.

In addition to cyberattacks, numerous sustained and large-scale disinformation campaigns and information operations have been observed. This has been supplemented by traditional propaganda with staged scenes in the Russian media and tight control of reporting in the press and on other media platforms. Using relatively new technologies, *deep-fakes* – manipulated videos and audio files – were also disseminated on the Internet, including fake clips of Ukrainian President Volodymyr Zelenskyy as well as Russian

5 Harding, Luke: "Ukraine hit by 'massive' cyber-attack on government websites", The Guardian, 14 January 2022.

6 Willet, The Cyber Dimension of the Russia-Ukraine War, 6 October 2022.

7 Council of the European Union: Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union, 10 May 2022.

8 Pearson, James/Satter, Raphael/Bing, Christopher/Schectman, Joel: "Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say", Reuters, 12 March 2022.

9 Vallance, Chris: "Ukraine war: Major internet provider suffers cyber-attack", BBC, 28 March 2022.

strongman Vladimir Putin.[10] The goal was to create chaos, destabilize Ukraine, and exhaust its moral forces in support of Russia's conventional operations.

Nevertheless, most experts expected far greater disruptions, even an unprecedented level of "shock and awe".[11] The fact that this did not occur at the time this chapter[12] was completed should not lead us to downplay the damage that has already been done. After all, the speed and cumulative effect of these attacks has had a very disruptive effect. Moreover, it can be assumed that many incidents either went undetected or unreported as part of covert operational activities. Nevertheless, we are not dealing with an incident of catastrophic proportions, a "cyber Pearl Harbor" that would bring entire portions of Ukraine's critical infrastructure or vital command and control systems to their knees. The scale of Russian cyberattacks since the war began is a far cry from what was predicted and has provided Moscow with little, if any, strategic benefit to its war aims.

3 The Cyber Resistance of Ukraine

Various theories have been put forward as to the causes of the rather limited impact of Russian cyber operations in the war against Ukraine.

Firstly, Ukraine's ability to effectively defend against or contain the tide of various cyberattacks is, among other things, the result of the country's direct experience gained during eight years of war against the Kremlin and its proxies. The constant threat from Kremlin-sponsored cyber actors has led Ukraine to prepare intensively for potential cyberattacks since 2014. Efforts in this respect include a new cybersecurity strategy, a cybersecurity law, an overhaul of its intelligence services, and strengthened incident response capabilities at the Computer Emergency Response Team of Ukraine (*CERT-UA*).

10 Simonite, Tom: "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be", WIRED, 17 March 2022.

11 *Shock and Awe* is a military strategy that aims to instill "fear and terror" in an adversary at the outset of a conflict through the use of overwhelming force (in this case, in the form of cyberattacks), thereby breaking that adversary's will to resist. HarperCollins: Shock and Awe, 2022.

12 This contribution was submitted in November 2022 to the original German version of this anthology.

Secondly, the support Ukraine has received from NATO allies and industry partners has played an important role. As the Director of the National Security Agency and U.S. Cyber Command, General Paul Nakasone, himself admitted, a *Mission Force* "*hunt-forward*" team travelled to Ukraine in December 2021 to help build resilience against cyberattacks.[13] Large private sector technology companies were very proactive from the beginning of combat operations, offering their capabilities to defend Ukraine. This included migrating Ukrainian government data and services to distributed *cloud servers* and providing continuous threat intelligence. This close collaboration between the private and public sectors, and even the participation of nonprofit organizations as part of a "whole-of-society response", has greatly assisted the Ukrainian government in strengthening its cyber resilience.

Thirdly, the mass mobilization of Ukrainian (and even international) volunteer hackers and patriotic programmers – many under the banner of the "IT Army" – is believed to have played a part in mounting a digital counteroffensive. With a talent pool of up to 300,000 professionals in the run-up to the war, Zelenskyy could indeed rely on many tech-savvy men and women to act as a second line of defense.[14]

Fourthly, Russia has failed to meaningfully integrate cyber operations with its conventional operations. Moscow has not yet deployed cyber operations in a manner that is clearly coordinated with military units and designed to facilitate the advance of ground or air forces. For example, Russian cyber units have not yet crippled power supplies or Internet connections in Ukraine on a large scale – such as immediately before an offensive. In an article in *Foreign Affairs*, NATO Assistant Secretary General for Intelligence and Security, David Cattler points to Russia's "missteps and struggles" that have almost certainly resulted in Russia's inability to date to meaningfully deploy its cyber program in support of its conventional forces.[15]

Finally, some experts suspect that Russia has tactically restrained its attacks to avoid exposing certain strategic capabilities. However, the limited

13 Smalley, Suzanne: "Nakasone says Cyber Command did nine 'hunt forward' ops last year, including in Ukraine", CyberScoop, 4 May 2022.

14 Mäder, Lukas: "Im Ukraine-Krieg kämpft eine 'IT-Armee' online gegen Russland. Die Freiwilligen attackieren sogar Apotheken und Universitäten", Neue Zürcher Zeitung, 23 July 2022.

15 Cattler, David/Black, Daniel: "The Myth of the Missing Cyberwar", Foreign Affairs, 6 April 2022.

attacks could also be related to Russia's caution about causing massive effects – even beyond Ukraine – that could trigger a Western response.[16] Spillover damage caused by Moscow, spreading far beyond the war zone, something reminiscent of *NotPetya,* could draw NATO into the fight. The Alliance has indeed stated that not only could a highly damaging cyberattack on an Alliance member trigger Article 5, but so could an accumulation of smaller attacks (assessed on a case-by-case basis).

4 The Impact of Russian Cyberattacks on Europe and Germany

In addition to the direct impact on Ukraine, some expansion of Russian cyber activities to other countries could also be observed.[17]

An October 2022 report by *Moody's Investors Service* noted that the Russian invasion of Ukraine has contributed to a significant increase in cyberattacks in the EMEA[18] region.[19] However, Juhan Lepassaar, Director of the European Union Cyber Security Agency (ENISA), emphasized that there has been no "radical change in cyber threats" despite a "challenging" threat landscape.[20]

Germany has not been spared from the effects of the conflict in the cyber domain. On March 15, 2022, the German Federal Office for Information Security (BSI) warned users against operating any security software developed by Moscow-based software developer *Kaspersky Lab.* It said this posed an increased risk of being ordered by Russian authorities to hack into customers' networks.[21] A few days later, a cyberattack on the ground infrastructure of the *KA-SAT network* shut down thousands of wind turbines in

16 De Liedekerke, Arthur/Laudrain, Arthur: "Russia's Cyber War: What's Next and What the European Union Should Do", Council on Foreign Relations, 30 March 2022.

17 Sabbagh, Dan: "Russian hackers targeting opponents of Ukraine invasion, warns GCHQ chief", The Guardian, 10 May 2022.

18 EMEA refers to the economic region "Europe", "Middle East" and "Africa".

19 Xiao, Menghan: "Cyberattacks accelerating in Europe, Moody's says", SC Media, 17 October 2022.

20 Kabelka, Laura: "EU's cybersecurity agency chief warns to keep guard up", Euractiv, 27 September 2022.

21 Nasr, Joseph: "Germany issues hacking warning for users of Russian anti-virus software Kaspersky", Reuters, 15 March 2022.

the country.[22] Later, in early 2023, pro-Russia hacker group *Killnet* claimed responsibility for taking down websites of key German administrations, including large companies and airports, in retaliation for Berlin's decision to deliver tanks to Ukraine.[23]

Even though Germany has been relatively spared from Russian attacks compared to other European partners, according to the German government,[24] these events prompted the Federal Ministry of the Interior and Home Affairs (BMI) to present a new cybersecurity agenda in July 2022.[25]

5 First Lessons

It would be premature to draw definitive conclusions based on the war that is still ongoing at the time this chapter was completed. Nonetheless, initial important lessons can be drawn from the activities in cyberspace to date.

The war in Ukraine should cause experts to reevaluate the concept of cyberwar or the role of cyberspace in a conventional war. It is likely that expectations of "shock and awe" were unrealistic. Nevertheless, the situation currently unfolding in Ukraine can provide a sound example of the Internet's contribution to a conventional conflict. Above all, Ukraine's impressive cyber defenses could serve as a model for Germany and other European countries for their own cyber defenses. Technology companies in particular play a crucial role here, with high-end capabilities that can extract valuable insights from a vast amount of processed data. But the need for closer cooperation between public and private actors, as well as support from allies, should not be underestimated either. To this end, governments could, for example, consider setting up so-called "data embassies"[26] abroad.

22 Burgess, Matt: "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine", WIRED, 23 March 2022.

23 Reuters: "Russian 'hacktivists' briefly knock German websites offline", 25 January 2023.

24 Kabelka, Laura: "Germany still not affected by Russia-linked cyberattacks", Euractiv, 6 May 2022.

25 Deutsche Welle: "Germany bolsters defenses against Russia cyber threat", 12 July 2022; Bundesministerium des Innern und für Heimat: Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode, June 2022.

26 The establishment of data embassies is an innovative approach first explored by Estonians. The concept aims to ensure the digital continuity of nation states through state server resources outside their national borders.

Western observers should not assume, however, that the strategy Kyiv has used to so successfully fend off Russia's attacks in cyberspace can be easily applied to its own countries. Many aspects are specific to the Ukrainian context:

- Ukraine's capacity to respond to and mitigate a high number of complex cyberattacks from various state and state-sponsored actors is partly the result of the country's direct experience gained in eight years of war against the Kremlin and its proxies;
- the mass mobilization of Ukrainian volunteer hackers and patriotic programmers is a unique feature. Zelenskyy was able to draw on a whole-of-society response, with the private sector and nonprofit organizations joining the defense effort alongside the government. This is due in large part to Ukraine's status as a global "IT powerhouse", a vibrant digital civil society, and a tradition of activism. In many Western countries, however, the deployment of such an "IT army" might face significant hurdles – including legal and ethical reservations due to privacy and security risks for potential collateral victims of attacks by hacker collectives;
- "information operations" around the theater of war also play a crucial role. Ukraine's success can be attributed in part to its familiarity with Russian disinformation campaigns and its ability to respond to them accordingly. In this regard, the effective use of social media, in particular, is of great importance in disseminating counter-narratives. In addition, Ukrainians have the ability to communicate in the Russian language. On the eve of the invasion, for example, Zelenskyy himself addressed his message directly to the Russian people – in Russian.[27]

6 Conclusion

Although the impacts of the cyberwarfare we are seeing unfold have been limited to date, it would be a grave mistake to be overly optimistic. A cornered Russia, facing a series of defeats on the battlefield and with few other options on the table – the nuclear dimension excluded – is likely to increasingly resort to cyberspace. This will prove an ideal basis for

27 For more details, see: De Liedekerke, Arthur/De Rivoire, Hector: "Ukraine's cyber resistance is impressive – but hard to replicate", EUobserver, 26 September 2022.

circumventing isolation, spying on, and disrupting Western defense plans, stealing technology and intellectual property, and amplifying global unrest.

After Western countries increased their support for Ukraine in recent months, a number of "punitive" actions by Russian cyber actors against specific countries have been observed – most notably in Finland,[28] Estonia,[29] and Montenegro.[30] This assessment is shared by *ENISA Threat Landscape 2022,* published in November, which assumes that Western or NATO allies (especially critical infrastructure facilities) are highly likely to be increasingly targeted as part of retaliatory actions.[31]

The more Western companies withdraw from Russia – a kind of strategic disengagement – the more incentive Russia has to use cyberweapons against companies and other states. Even if Moscow agrees to some kind of ceasefire, the increased use of cyberattacks and disinformation campaigns would be one of the few available options to inflict damage on Ukraine and the West in a kind of gray zone – then again below the threshold of direct confrontation.

In the long run, however, lost investments, limited access to key technologies, and fundamental constraints on the Russian economy will severely impact Russia's ability to wage war in cyberspace. The West's resolve and the support of other like-minded partners in maintaining the necessary sanctions will be critical to throttling the capabilities of Putin's cyber army.

Bibliography

Bundesministerium des Innern und für Heimat: Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode, June 2022, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.html, 28.11.2022.

Burgess, Matt: "A mysterious satellite hack has victims far beyond Ukraine", Wired, 23 March 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia/, 19.11.2022.

28 Teivainen, Aleksi: "Finnish Parliament's website brought down by Russian hacker group", Helsinki Times, 10 August 2022.

29 Sytas, Andrius: "Estonia says it repelled major cyber attack after removing Soviet monuments", Reuters, 18 August 2022.

30 Euractiv: "Cyberattack hits Montenegro government, defense minister points at Russia," 28 August 2022.

31 ENISA: ENISA Threat Landscape 2022, 3 November 2022.

Cattler, David/Black, Daniel: "The myth of the missing cyberwar", Foreign Affairs, 1 August 2022, https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar, 19.11.2022.

Council of the European Union: Russian cyber operations against Ukraine: Declaration by the high representative on behalf of the European Union, 10 May 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/, 19.11.2022.

De Liedekerke, Arthur/De Rivoire, Hector: "Ukraine's cyber resistance is impressive – but hard to replicate", EUobserver, 26 September 2022, https://euobserver.com/opinion/156126, 28.11.2022.

De Liedekerke, Arthur/Laudrain, Arthur: "Cyber War: What's Next and What the European Union Should Do", Council on Foreign Relations, 30 March 2022, https://www.cfr.org/blog/russias-cyber-war-whats-next-and-what-european-union-should-do, 19.11.2022.

Deutsche Welle: "Germany bolsters defenses against Russia cyber threat", 12 July 2022, https://www.dw.com/en/germany-bolsters-defenses-against-russian-cyber-threats/a-62442479, 19.11.2022.

Digital Security Unit: Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine, Microsoft, 27 April 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd, 19.11.2022.

ENISA: ENISA Threat Landscape 2022, 3 November 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, 28.11.2022.

Euractiv: "Cyberattack hits Montenegro Government, defense minister points at Russia", 28 August 2022, https://www.euractiv.com/section/global-europe/news/cyberattack-hits-montenegro-government-defence-minister-points-at-russia/, 19.11.2022.

Harding, Luke: "Ukraine hit by 'massive' cyber-attack on government websites", The Guardian, 14 January 2022, https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers, 19.11.2022.

HarperCollins: Shock and Awe, https://www.collinsdictionary.com/de/worterbuch/englisch/shock-and-awe, 29 November 2022.

Hoyer, Katja: "Germans are under attack. Can they adapt?", The Washington Post, 25 October 2022, https://www.washingtonpost.com/opinions/2022/10/25/russia-sabotage-germany-railroads-hacking-drones/, 19.11.2022.

Kabelka, Laura: "EU's cybersecurity agency chief warns to keep guard up", Euractiv, 28 September 2022, https://www.euractiv.com/section/cybersecurity/news/eus-cybersecurity-agency-chief-warns-to-keep-guard-up/, 19.11.2022.

Kabelka, Laura: "Germany still not affected by Russia-linked cyberattacks", Euractiv, 6 May 2022, https://www.euractiv.com/section/cybersecurity/news/germany-still-not-affected-by-russia-linked-cyberattacks/, 19.11.2022.

Mäder, Lukas: "Im Ukraine-Krieg kämpft eine 'IT-Armee' online gegen Russland. Die Freiwilligen attackieren sogar Apotheken und Universitäten", Neue Züricher Zeitung, 23 July 2022, https://www.nzz.ch/technologie/ukraine-krieg-freiwillige-it-armee-greift-russische-ziele-an-ld.1689428, 29.11.2022.

Nasr, Joseph: "Germany issues hacking warning for users of Russian anti-virus software Kaspersky", Reuters, 15 March 2022, https://www.reuters.com/technology/germany-issues-hacking-warning-users-russian-anti-virus-software-kaspersky-2022-03-15/, 19.11.2022.

Pearson, James/Satter, Raphael/Bing, Christopher/Schectman, Joel: "Exclusive: U.S. Spy Agency probes sabotage of satellite internet during Russian invasion, sources say", Reuters, 11 March 2022, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/, 19.11.2022.

Reuters: "Russian 'hacktivists' briefly knock German websites offline", 25 January 2023, https://www.reuters.com/world/europe/russian-hacktivists-briefly-knock-german-websites-offline-2023-01-25/, 03.07.2023.

Sabbagh, Dan: "Russian hackers targeting opponents of Ukraine invasion, warns GCHQ chief", The Guardian, 10 May 2022, ://www.theguardian.com/technology/2022/may/10/russian-hackers-targeting-opponents-of-ukraine-invasion-warns-gchq-chief, 19.11.2022.

Simonite, Tom: "A Zelensky Deepfake was quickly defeated. The next one might not be", Wired, 17 March 2022, https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/, 19.11.2022.

Smalley, Suzanne: "Nakasone says Cyber Command did nine 'hunt forward' ops last year, including in Ukraine", CyberScoop, 4 May 2022, https://www.cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/, 19.11.2022.

Sytas, Andrius: "Estonia says it repelled major cyber attack after removing Soviet monuments", Reuters, 18 August 2022, https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/, 19.11.2022.

Teivainen, Aleksi: "Finnish Parliament's website brought down by Russian Hacker Group", Helsinki Times, 10 August 2022, https://www.helsinkitimes.fi/finland/finland-news/domestic/22011-finnish-parliament-s-website-brought-down-by-russian-hacker-group.html, 19.11.2022.

Vallance, Chris: "Ukraine war: Major internet provider suffers cyber-attack", BBC News, 28 March 2022, https://www.bbc.com/news/60854881, 10.11.2022.

Willett, Marcus: The Cyber Dimension of the Russia-Ukraine War, International Institute for Strategic Studies, 6 October 2022, https://www.iiss.org/blogs/survival-blog/2022/10/the-cyber-dimension-of-the-russia-ukraine-war, 19.11.2022.

Xiao, Mengha: "Cyberattacks accelerating in Europe, Moody's says", SC Media, 18 October 2022, https://www.scmagazine.com/analysis/vulnerability-management/cyberattacks-accelerating-in-europe-moodys-says, 19.11.2022.

Zetter, Kim: "Inside the cunning, unprecedented hack of Ukraine's power grid", Wired, 3 March 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 19.11.2022.