# RUSSIA CONTINUES TO LOOK FOR A WEAK LINK IN UKRAINIAN CYBERSPACE

**Russia uses cyberattacks to support its general goals in Ukraine: to break Ukrainian resistance, undermine the government's image and disrupt the functioning of the state. Cyber espionage is likely the biggest threat stemming from cyberspace.**

**Russia underestimated the resilience of Ukraine's cyberspace and the help it receives from Western countries and cybersecurity companies.**

**Threats posted on social media and cyberattacks continue as part of the influence operations against countries that actively support Ukraine, including Estonia.**

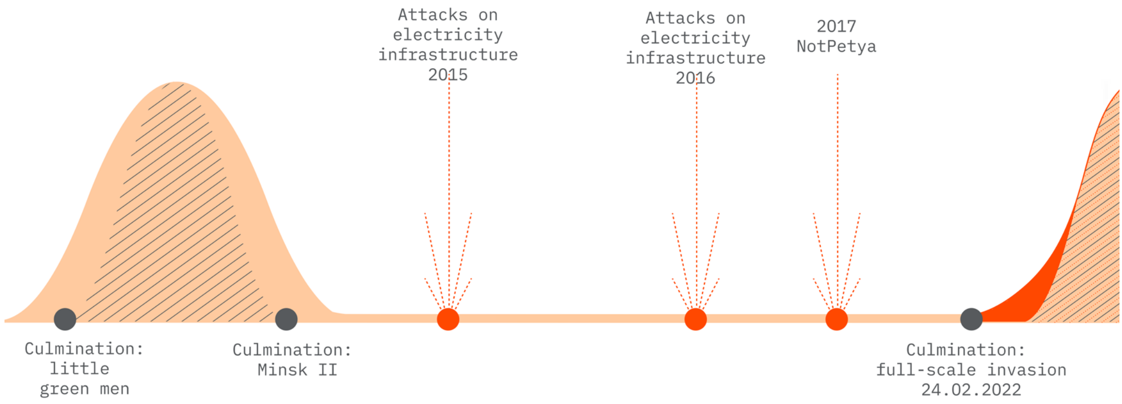
At least since the start of the Russo-Ukrainian war in 2014, Ukraine has been a constant target of cyberattacks by Russian special services.[1] Attacks intensified immediately before kinetic warfare began and continued throughout the active phase of the war. Russia mainly organised cyberattacks as part of influence operations, such as denial-of-service and defacement attacks and data leaks. One of the goals of these activities is to prevent the Ukrainian government from sharing information with its citizens, to cause fear and distrust in the state's leadership, to weaken society's resistance and to create information noise that makes it difficult to distinguish reality from disinformation. After the most active phase of kinetic warfare, Russia tried to keep the Ukrainian state weak and organised cyberattacks to disrupt critical services.[2] Low-intensity cyberattacks, mainly for intelligence purposes, were conducted until Russia again stepped up its aggressive rhetoric towards Ukraine. In January and February 2022, Russia's cyberattacks against Ukraine seemed to be aimed at supporting its general goals: to break the resistance of the Ukrainian population and create an impression of Russia's vast superiority, the hopelessness of the situation for Ukraine and the weakness of the Ukrainian state.

From 13 to 14 January 2022, cyberattackers broke into the websites of Ukrainian state institutions and made these inaccessible to the public. During the same period, cyberattackers spread the WhisperKill/WhisperGate malware in Ukrainian computer networks.[3]

[1] At least since 2014, the FSB's 18th Centre has been directing cyberattacks against Ukraine, including stealing information, https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys -kiberatak-na-derzhavni-orhany-ukrainy.

[2] In December 2015 and 2016, the GRU carried out cyberattacks on Ukraine's energy sector, which led to several-hour power outages in Western Ukraine. In 2017, the GRU organised the NotPetya cyber operation to make Ukrainian government agencies' data unusable. https://www.wired.com/story/sandworm-kremlin-most-dangerous-hackers

[3] https://cert.gov.ua/article/18101; https://ssu.gov.ua/en/novyny/sbu-rozsliduie-prychetnist-rosiiskykh-spetssluzhb-do-sohodnishnoi-kiberataky-na-orhany-derzhavnoi-vlady-ukrainy; https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion; 27 April 2022, Microsoft, Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine.



From 15 to 16 February 2022, denial-of-service attacks took place against the websites of Ukrainian state institutions and banks.[4]

A few hours before the reactivation of kinetic warfare, cyberattacks against Ukraine suddenly increased even more.

On 23 February 2022, denial-of-service attacks took place against the websites of Ukrainian state institutions and banks.

From 23 to 25 February 2022, cyberattackers installed several types of malware in Ukrainian information systems, which can disrupt computer use or make data on the computer inaccessible. For example, on 23 February, the GRU installed the destructive HermeticWiper malware in the information systems of Ukrainian government agencies, the IT sector, and the energy and financial sectors. On 24 February, it conducted a cyberattack on Viasat's subsidiary KA-SAT by installing the AcidRain malware in the latter's information system.[5]

While the West distinguishes between cyberattacks and influence operations, Russia interprets them as a single concept – information confrontation (*информационное противоборство*). This Russian Armed Forces' doctrine consists of three main components: exerting informational, technological and psychological influence on another country, and protecting Russia itself from such influences.

It is possible that specific cyberattacks against energy, water supply or other similar critical infrastructure,[6] which would lead to long-term service interruptions, were not organised early on because Russia expected to achieve its military objectives quicker and wanted to maintain the support of the local population.

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

[5] https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-oneurope/

[6] An attack on the specific industrial control information systems, which are used for vital services such as energy and water supply, is somewhat different from attacking ordinary information systems. Simply put, these information systems are built differently. The Industroyer2 malware was specially developed to attack industrial control information systems, and the GRU probably used it on 8 April 2022 against the Ukrainian energy sector. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Despite failing to occupy Ukraine in a few days as originally intended, Russia continued its cyberattacks against Ukraine. These were more frequent during certain periods. For example, Ukrainian cyber defenders working with cybersecurity companies repeatedly detected destructive malware over a period of about 30 days from the second half of March. Cyberattacks started to gain momentum again in the autumn.[7] Cyberattacks to obtain information have continued.[8] Cyber espionage is likely the biggest threat stemming from cyberspace. Stolen information can effectively be used as input to Russian special services' operations and influence activities.

> During the war, Russia has used several destructive malware repeatedly. On 11 October 2022, Microsoft detected the CaddyWiper malware in the critical infrastructure of the Mykolaiv and Kyiv regions. The cybersecurity company ESET detected this malware for the first time on 14 March 2022 in the information system of a Ukrainian bank.[9]
>
> On 14 October 2022, Microsoft identified the Prestige ransomware in the information system of Ukrainian and Polish logistics and transport companies.

In 2022, cybersecurity researchers identified at least nine types of destructive malware in Ukrainian cyberspace that have attempted to disrupt services (ENISA Threat Landscape 2022, p. 25; Recorded Future, 2022). Destructive malware makes a computer unusable by corrupting programs or data. Ransomware that encrypts data without the possibility of decrypting, such as Prestige, can be used to the same end. Such an amount of destructive malware has never been observed anywhere in such a short period of time. This shows that Russia is capable of quickly developing new malware.

Russian cyberattacks, like the actions of its armed forces, are likely aimed at wearing down Ukraine's cyber defenders and then finding the weakest link that would help achieve Russia's overall military goal – to wear down Ukraine, damage the international image and credibility of the Ukrainian leadership, reduce aid from allies, and undermine the society's morale. Therefore, a cyberattack need not actually disrupt an information system, as with each attack, investigators have to spend human and time resources to check whether and how extensively the information system has been attacked, how to improve defence, etc.

Russia underestimated the resilience of Ukraine's cyberspace and the help it receives from Western countries and cybersecurity companies. Despite denial-of-service attacks on the websites of state institutions to disrupt the flow of information, among other things, the Ukrainian government has found alternative ways of communication, for example, using social media. Using Starlink devices also plays an important role in maintaining civilian and military communications. Cybersecurity companies have been helping Ukraine defend its cyberspace since 2014. Aid intensified during the full-scale Russian invasion and, with allied support, was likely instrumental in ensuring the resilience of Ukraine's cyberspace. Russia's influence operations in cyberspace have not had the expected effect. Ukrainian society remains united and trusts its government despite threats posted on social media and data leaks.

[7] On detected cyberattacks, see e.g. https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/

[8] https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/

[9] https://twitter.com/ESETresearch/status/1503436420886712321

Russian cyberattacks go beyond the territory of Ukraine. Pro-Kremlin cyberattackers threaten the cyberspace of countries that support Ukraine, including Estonia, Latvia, Lithuania and Poland. In the active phase of kinetic warfare, they have attempted to intimidate societies with threats on social media, denial-of-service attacks and data leaks. Their activities support Russian special services' influence operations.

> From 16 to 17 August 2022, denial-of-service attacks took place on the information systems of Estonian companies and state institutions.[10] Pro-Russian hacktivists took responsibility for these cyberattacks and claimed to have attacked 207 targets in Estonia.[11] In fact, they just copied a list of services where the Smart-ID app can be used, and actual attacks were not carried out against all these targets.

Russia uses cyberattacks to support its strategic objectives (e.g., causing fear and weakening society's resistance to the aggressor, disrupting the functioning of the state, and creating information noise to make it difficult to distinguish reality from disinformation). The Russo-Ukrainian war confirms that cybersecurity measures[12] make it possible to withstand cyber espionage, cyber sabotage and influence operations.

| Instrument of Attack | Purpose | Protective Measure |
|---|---|---|
| defacement attacks | • intimidation/threatening<br>• creating confusion<br>• disrupting information flow | Website software update. When outsourcing a website, make sure the provider diligently implements cybersecurity measures. If defaced, use alternative information channels if possible, such as social media.<br>Main targets: media, state institutions (mediators of crisis information), website providers |
| denial-of-service attacks | • disrupting information flow<br>• intimidation | Protection against denial-of-service attacks (see RIA suggestions)[13] |
| social media posts | • intimidation/threatening | Check the information against reliable sources and be critical of sources. See advice on the conduct of information warfare from the website kriis.ee |
| data leaks | • damage to reputation (reduce help from allies and intelligence sharing) | Think carefully about what information you share and with whom. Make sure your shared information is kept secure, and the recipient keeps the shared information in an environment where cybersecurity best practices are implemented. |
| data encrypting malware | • disrupting the functioning of the state<br>• intimidation | Back up data properly |
| destructive malware | • disrupting the functioning of the state<br>• intimidation | Keep your software updated. Implement cybersecurity best practices.<br>Back up data properly |
| cyber intelligence (phishing, brute force attacks, exploitation of security vulnerabilities) | • information gathering<br>• leaking stolen information out of context, combined with fabricated information | Keep your software updated.<br>Implement cybersecurity best practices.<br>Get cyber hygiene training |

[10] https://www.ria.ee/en/news/ddos-attacks-16th-and-17th-august-targeted-around-20-websites

[11] https://www.runews24.ru/society/17/08/2022/a66e4f36646d32e3bb459604947b3390?

[12] See recommendations for cybersecurity measures on the Estonian Information System Authority (RIA) website at https://www.ria.ee

[13] https://www.ria.ee/kuberturbe-nouanded/nouanded-asutusele-ja-ettevottele/teenusetokestusrunde-ennetus