Ukraine: Facing the intensification of Russian cyber attacks

Description

Cyber operations have become a central aspect of the war in Ukraine. Russian state-linked groups combine techniques of espionage, destructive malware and infiltration to pressure Ukrainian state capacity, with daily incidents rising through early 2025. In response, Ukraine has reinforced its cyber-defence tactics, expanded international cooperation, and in November 2025, introduced the draft National Cyber Hygiene Strategy to build up long-term digital resilience.

On November 5, 2025, the head of Office of Ukraine’s State Service for Special Communication and Information Protection (SSSCIP/CERT-UA), Oleksandr Potii, stated that « cyber weapons have become an integral component of the full-scale war the Russian Federation is waging against Ukraine. » In the same address, he reported that in the first half of 2025 the daily average of recorded cyber incidents in Ukraine was 16,5, and that 82% of targets were civilian infrastructure, energy, logistics, public institutions and telecommunications.

For years, Ukraine has faced continuous cyberthreats

Since 2014, Ukraine have registered repeated occasions of cyber-operations attributed to Russian-linked actors. Those operations moved from espionage toward disruptive tools leading up to the full-scale invasion in 2022.

The Ukrainian national incident response team, CERT-UA, reports a significant increase in this type of hostile activity. Ukraine faced multiple incidents of cyber attacks throughout 2024-2025. The most frequent threats include phishing campaigns (an attack that attempts to steal your money, or your identity, by getting you to reveal personal information), credential theft, data-wiping malware (destruction of data), and attempts to infiltrate energy and telecom sectors. According to Ukrainian cybersecurity authorities, the Russian Federation remains the principal source of hostile cyber activity directed at Ukraine. In addition to Russia-linked operations, activity is also recorded from Belarus, China, and North Korea.

International assessments like the Microsoft Digital Defence Report 2025, indicate that during the first half of 2025 Ukraine ranked fifth worldwide and third in Europe among countries most affected by cyber activity. In fact, 9,5% of all impacted customers in Europe were located in Ukraine.

Overall, it is clear that cyber operations have fully integrated themselves into the battlefield of the war as a part of Russian strategy of applying pressure on Ukrainian state capacity.

Russia continues to develop its cyberattack strategy

Russian cyber strategy has developed over the years into a more multi-facetted campaign that goes along its military operations against Ukraine. Espionage plays a major role in Russia’s approach. The intelligence collection directed against the Defense Forces and related institutions « has the greatest impact on the situation on the frontline », as it aims to extract military plans and various operational information. One of the most active clusters is UAC-0010 (Gamaredon/Primitive Bear), which aims to infect thousands of systems using phishing mails, malicious documents and built-in Windows tools while masking its infrastructure through Telegram, Cloudfare and related services. CERT-UA also highlights groups such as UAC-0184, which targets military personnel; UAC-0200, which distributes remote-access tools through the Signal messenger and targets defence industry entities; and UAN-0218/0219, which focuses on quick data theft.

Destructive attacks are still present in Russia’s strategy. On 26 May 2025, the pro-Russian Telegram channel « Solntsepyok » published information about coordinated series of destructive attacks against eight Ukrainian internet providers (Interlink, ActiveNet, SvitNet, smn.com.ua, GO « Gorih », Aries.od.ua, Corbina, and D-lan).

Thus, a broader shift toward destructive malware has been documented through 2024-2025. One of Russia’s most aggressive state-linked groups, Sandstorm, has intensified its operations and deployed multiple families of wipers against Ukrainian targets. In spring 2025, a Ukrainian university was attacked with two wipers called Sting (targeting Windows systems) and Zerlot (destructive model). Up until the early autumn of 2025, Sandstorm expanded its operations against government bodies, energy facilities and logistics operators. It should be noted that Sandstorm used wipers for years, with earlier attacks on the Ukrainian power grid and the global spread of NotPetya.

Russia’s cyber operations follow a targeting logic focused around Ukraine’s critical infrastructure. The energy sector finds itself at the base of this system and has been under constant attack since 2014, with intensifying pressure during the winter of 2022-2023 and 2025-2026. Disruptions there directly affect electricity supply and set off failures in communication networks and state operations. Telecommunications form the next layer: attacks against internet and mobile services aim to limit coordination, restrict information flows, and complicate both military and civilian response. The upper layer has IT systems and digital services (banking, logistics, media, registries, and law enforcement tools) whose disruption can shut down essential functions and create operational paralysis. Because each level depends on the one below it, targeting the lower layers can produce domino-effect damage across the entire system, which is why energy and telecommunications remain priority targets in Russia’s strategy.

A clear example of the impact of Russia’s cyber operations was in December 2024, when hackers overrun the digital infrastructure of the Ministry of Justice of Ukraine and disabled fourteen state registries, according to the State Service of Special Communications and Information Protection. The attack brought key public services to a standstill: border guards were unable to verify travel restrictions, causing delays at checkpoints; customs officers lost access to essential datasets on companies and vehicle owners, disrupting cargo clearance; and notaries and registrars were blocked from performing real estate transactions, inheritance cases, and other legally binding procedures. This incident showed how deeply everyday Ukrainian administrative processes depend on uninterrupted access to state registries.

Russia’s strategy also includes financially motivated intrusions. CERT-UA identifies UAC-0050 and UAC-006 as the most active financial clusters. These groups compromise accounting systems through by gaining access to modify payment orders and redirect funds to controlled accounts.

Alongside technical attacks, Russia also intensified disinformation efforts throughout the war. Television channels, news agencies, and online platforms were a repeated target to diffuse fake news, propaganda materials and even deepfakes. The objective was to create public distrust and spread pro-Russian narratives.

The latest SSSCIP analysis for the first half of 2025 shows that Russian cyber operations are not only continuing but also becoming more adaptive and technologically advanced. Russian-linked groups now rely on heavily automated processes, more complex attack chains, and advanced social engineering to bypass security measures. The use of artificial intelligence has also improved: while AI-generated phishing messages are now widespread, Ukrainian analysts have identified malware samples that show signs of being created or modified through AI tools.

Taken together, it is clear that Russia’s cyber strategy with a focus on espionage and destructive attacks, serves as an instrument for weakening state activity. Such fast evolution of cyberthreats pushes Ukraine to reevaluate and adapt their defensive posture.

Ukrainian cyber defense approach is a core national priority

Since 2021, Ukraine has restructured its cyber-defense framework, which helped to respond effectively to Russia's escalation. After February 2022, Ukraine expanded its cyber personnel by bringing private-sector IT specialists into state teams and creating a defense model that operates under wartime conditions. This model is based on coordination between government, the IT sector and volunteer groups, in order for digital systems to stay operational despite persistent hostile activity.

A core part of Ukraine's cyber strategy is rapid recovery after cyber incidents. To ensure that there would be minimal interruption, Ukraine moved key government data to secure cloud servers in the EU and the United States, in order to reduce risks of physical destruction or power outages. New backup systems and alternative access channels keep essential servers available during disruptions.

International cooperation is also a central element of Ukraine's cyber-defense strategy. Ukraine works with foreign government agencies, national CERTs/CSIRTs (Computer Emergency Response Team et Computer Security Incident Response Team), and major cybersecurity companies to detect and stop attacks on critical infrastructure (malware analysis, sharing of indicators and insight into Russian tactics). Additionally, working with the United States, the United Kingdom, the European Union and NATO have helped Ukraine respond to cyber incidents faster, with private sector experts providing technical support.

In November 2025, Ukraine also presented a draft National Cyber Hygiene Strategy, which sets goals for improving digital security habits by 2030. The plan aligns with EU NIS2 and ENISA standards (European Network and Information Security Agency) and focuses on training programs for citizens, mandatory certification for civil servants, and the implementation of security standards across government agencies. It also strengthens coordination among key institutions, including the Ministry of Digital Transformation, the State Service of Special Communications, and the National Cybersecurity Coordination Center. As Secretary of the NCSCC, Natalia Tkachuk, noted, « Compliance with digital security rules is a daily practice that increases our collective resilience […] so systematic cyber hygiene in government agencies, military structures, critical infrastructure, business, and education is an integral part of cybersecurity. » underscoring the key role of cyber question in Ukraine's defence strategy.

Thumbnail: Oleksandr Potii, Chairman of the State Service of Special Communications and Information Protection of Ukraine, during his online address to the International Scientific and Practical Conference « Digital Transformation: Strengthening Cybersecurity Capabilities in the Modern World », held in Krakow, Poland (Copyright : State Service of Special Communications and Information Protection of Ukraine).

* Valeriya Sytnik is a second-year Master's student in International relations and Ukrainian media translation at INALCO.

To cite this article: Valeriya SYTNIK (2026), "Ukraine: Facing the intensification of Russian cyber attacks" *Regard sur l'Est*, February 23.

Back to the top of the page

date créée
23/02/2026
Champs de Méta
Auteur-article : Valeriya Sytnik*