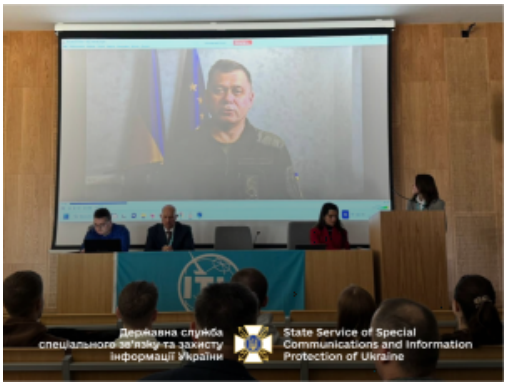
Ukraine : face à l'intensification des attaques cyber russes

Description

Les opérations cybernétiques sont devenues un élément central de la guerre en Ukraine. Des groupes liés à l'État russe combinent des techniques d'espionnage, l'usage de logiciels malveillants et des actions d'infiltration afin d'exercer une pression sur les capacités de l'État ukrainien. En réponse, l'Ukraine a renforcé ses dispositifs de cyberdéfense, élargi sa coopération internationale et, en novembre 2025, a présenté un projet de Stratégie nationale de cyber-hygiène visant à consolider la résilience numérique sur le long terme.



Le 5 novembre 2025, le chef du bureau du Service d'État ukrainien pour les communications spéciales et la protection de l'information (SSSCIP/CERT-UA) Oleksandr Potii a déclaré que *« les cyberarmes sont devenues une composante intégrante de la guerre de grande ampleur que la Fédération de Russie mène contre l'Ukraine »*. Il a indiqué qu'au cours du premier semestre 2025, la moyenne quotidienne des incidents cybernétiques enregistrés en Ukraine s'était élevée à 16,5 et que 82 % des cibles concernaient des infrastructures civiles, notamment les secteurs de l'énergie, de la logistique, des institutions publiques et des télécommunications.

Depuis des années, l'Ukraine est confrontée à des cybermenaces continues

Depuis 2014, l'Ukraine a recensé de multiples cyberopérations attribuées à des acteurs liés à la Russie. Ces actions ont évolué de l'espionnage à l'emploi d'outils perturbateurs, jusqu'à accompagner l'invasion à grande échelle lancée en 2022.

L'équipe nationale ukrainienne de réponse aux incidents, CERT-UA, fait état d'une augmentation significative de ce type d'activités hostiles, notamment en 2024 et 2025. Les menaces les plus fréquentes incluent des campagnes de phishing visant à dérober des informations personnelles ou financières, le vol d'identifiants, l'utilisation de logiciels malveillants destinés à l'effacement de données, ainsi que des tentatives d'infiltration dans les secteurs de l'énergie et des télécommunications. Selon les autorités ukrainiennes, la Russie demeure la principale source d'activités cyber-hostiles dirigées contre l'Ukraine. Des activités provenant du Bélarus, de Chine et de Corée du Nord ont également été observées.

Des évaluations internationales, telles que le *Microsoft Digital Defense Report 2025*, indiquent qu'au cours du premier semestre 2025 l'Ukraine se classait au cinquième rang mondial et au troisième rang européen parmi les pays les plus affectés par les activités cybernétiques. À l'échelle européenne, 9,5 % de l'ensemble des clients touchés se trouvaient en Ukraine.

Il apparaît clairement que ces opérations cybernétiques se sont pleinement intégrées au champ de bataille de la guerre, en tant qu'élément à part entière de la stratégie russe visant à exercer une pression durable sur les capacités de l'État ukrainien.

La Russie poursuit le développement de sa stratégie de cyberattaques

La stratégie cybernétique russe s'est progressivement transformée, au fil des années, en une campagne multifacette, étroitement articulée avec les opérations militaires menées contre l'Ukraine. L'espionnage y occupe une place centrale.

La collecte de renseignements visant les forces de défense ukrainiennes et les institutions qui leur sont associées *« a l'impact le plus important sur la situation sur le front »*, dans la mesure où elle cherche à extraire des plans militaires et diverses informations opérationnelles. Parmi les groupes les plus actifs figure le cluster UAC-0010, également connu sous les noms de Gamaredon ou Primitive Bear, dont l'objectif est d'infecter des milliers de systèmes à l'aide de courriels de phishing, de documents malveillants et d'outils intégrés à Windows, tout en dissimulant son infrastructure *via Telegram*, *Cloudflare* et des services connexes. CERT-UA met également en avant d'autres groupes, tels que UAC-0184 qui cible le personnel militaire, UAC-0200 qui diffuse des outils d'accès à distance *via* la messagerie *Signal* et vise des entités de l'industrie de la défense, ainsi que UAN-0218 et UAN-0219, spécialisés dans le vol rapide de données.

Les attaques destructrices restent un pilier de la stratégie russe. Le 26 mai 2025, la chaîne Telegram prorusse *Solntsepyok* a revendiqué une série coordonnée d'attaques visant huit fournisseurs ukrainiens d'accès à Internet : Interlink, ActiveNet, SvitNet, smn.com.ua, l'ONG Gorih, Aries.od.ua, Corbina et D-lan.

Plus largement, les années 2024 et 2025 marquent une intensification du recours aux logiciels malveillants destructeurs. Le groupe étatique russe *Sandstorm* a accru ses opérations et déployé plusieurs familles de wipers contre des cibles ukrainiennes. Au printemps 2025, une université a été touchée par deux wipers distincts : *Sting*, ciblant Windows, et *Zerlot*, à finalité explicitement destructrice. Jusqu'au début de l'automne 2025, *Sandstorm* a étendu ses attaques aux administrations, aux infrastructures énergétiques et aux opérations logistiques. Ce recours aux wipers s'inscrit dans une continuité opérationnelle, illustrée par les attaques antérieures contre le réseau électrique ukrainien et la diffusion mondiale du malware NotPetya.

La logique de ciblage des opérations cybernétiques russes s'organise autour des infrastructures critiques ukrainiennes. Le secteur de l'énergie a été attaqué de manière continue depuis 2014, avec une intensification notable durant les hivers 2022-2023 et 2025-2026. Les télécommunications constituent l'échelon suivant : les attaques contre les services d'Internet et mobiles visent à limiter la coordination, restreindre les flux d'informations et compliquer les réponses militaires et civiles. Le niveau supérieur concerne les systèmes informatiques et services numériques (services bancaires, logistique, médias, registres administratifs et outils des forces de l'ordre), dont la paralysie peut interrompre des fonctions essentielles et entraîner une désorganisation généralisée. Chaque niveau dépendant du précèdent, le ciblage des couches inférieures produit des effets en cascade à l'échelle du système.

Un exemple révélateur de l'impact de ces opérations s'est produit en décembre 2024, lorsque des hackers ont pris le contrôle de l'infrastructure numérique du ministère ukrainien de la Justice et désactivé quatorze registres d'État. Cette attaque a entraîné l'arrêt des services publics essentiels : impossibilité pour les gardes-frontières de vérifier les restrictions de déplacement, retards aux points de contrôle, perte d'accès pour les douanes à des bases de données clés sur les entreprises et propriétaires de véhicules, perturbant le dédouanement. Les notaires et agents d'enregistrement ont également été empêchés de réaliser des transactions immobilières, des procédures successorales et d'autres actes juridiques.

La stratégie russe inclut également des intrusions visant des objectifs financiers. CERT-UA identifie les groupes UAC-0050 et UAC-006 comme les clusters financiers les plus actifs. Ces groupes compromettent des systèmes comptables en obtenant un accès leur permettant de modifier des ordres de paiement et de rediriger des fonds vers des comptes sous leur contrôle.

Parallèlement aux attaques techniques, la Russie a intensifié ses efforts de désinformation. Les chaînes de télévision, les agences de presse et les plateformes en ligne ont été régulièrement ciblées pour diffuser de fausses informations et du contenu de propagande. L'objectif poursuivi consiste à susciter la défiance au sein de la population et à promouvoir des récits favorables à la Russie.

La dernière analyse du SSSCIP sur le premier semestre 2025 montre une sophistication accrue des opérations russes. Les groupes affiliés à la Russie utilisent désormais des processus hautement automatisés, des chaînes d'attaque plus complexes et des techniques avancées d'ingénierie sociale pour contourner les dispositifs de sécurité. Le recours à l'intelligence artificielle s'intensifie également : au-delà des messages de phishing générés par l'IA, des analystes

ukrainiens ont également identifié des logiciels malveillants présentant des traces de création ou de modification par des outils de l'IA.

La cyberdéfense, priorité nationale ukrainienne

Depuis 2021, l'Ukraine a profondément restructuré son dispositif de cyberdéfense, ce qui lui a permis de répondre plus efficacement à l'escalade des attaques russes. Après février 2022, le pays a renforcé ses effectifs spécialisés en intégrant des experts informatiques issus du secteur privé au sein des équipes étatiques et en mettant en place un modèle de défense adapté au contexte de guerre. Ce modèle repose sur une coordination étroite entre les autorités publiques, le secteur des technologies de l'information et des groupes de volontaires.

Un élément central de la stratégie cybernétique ukrainienne réside dans la capacité de rétablissement rapide après un incident. Dans cette optique, l'Ukraine a transféré des données gouvernementales essentielles vers des serveurs cloud sécurisés situés dans l'Union européenne et aux États-Unis, afin de limiter les risques liés à la destruction physique ou aux coupures d'électricité. De nouveaux systèmes de sauvegarde et des canaux d'accès alternatifs permettent ainsi de maintenir la disponibilité des serveurs critiques en cas de perturbation.

La coopération internationale constitue également un pilier majeur de la cyberdéfense ukrainienne. L'Ukraine collabore avec des agences gouvernementales étrangères, des CERT et des CSIRT nationaux (*Computer Emergency Response Team* et *Computer Security Incident Response Team*), ainsi qu'avec de grandes entreprises de cybersécurité, afin de détecter et de neutraliser les attaques visant les infrastructures critiques, notamment par l'analyse de logiciels malveillants, le partage d'indicateurs de compromission et la diffusion d'informations sur les tactiques russes. Les partenariats avec les États-Unis, le Royaume-Uni, l'Union européenne et l'OTAN ont par ailleurs permis d'accélérer la réponse aux incidents cybernétiques, grâce à l'appui technique d'experts du secteur privé.

En novembre 2025, l'Ukraine a également présenté un projet de Stratégie nationale de cyber-hygiène, qui fixe des objectifs d'amélioration des pratiques de sécurité numérique à l'horizon 2030. Ce document s'inscrit dans le cadre des normes européennes NIS2 et des recommandations de l'ENISA (Agence de l'Union européenne pour la cybersécurité), et met l'accent sur des programmes de formation à destination des citoyens, la certification obligatoire des agents publics et la mise en œuvre de normes de sécurité au sein des administrations. Il vise en outre à renforcer la coordination entre les principales institutions concernées, notamment le ministère de la Transformation numérique, le Service d'État pour les communications spéciales et le Centre national de coordination de la cybersécurité. Comme l'a souligné Natalia Tkachuk, secrétaire du NCSCC (Centre national de coordination de la cybersécurité d'Ukraine), *« le respect des règles de sécurité numérique relève d'une pratique quotidienne qui renforce la résilience collective, ce qui fait de la cyber-hygiène systématique dans les administrations, les structures militaires, les infrastructures critiques, le monde économique et le système éducatif un élément indissociable de la cybersécurité »*.

Vignette : Oleksandr Potii, président du Service national des communications spéciales et de la protection de l'information de l'Ukraine, lors la conférence *Transformation numérique : renforcer les capacités en matière de cybersécurité dans le monde moderne*, Cracovie (Pologne), 5 novembre 2025 (Copyright : Site du Service national des communications spéciales et de la protection de l'information de l'Ukraine).

* Valeriya Sytnik est étudiante en Master 2 en Relations internationales et en traduction des médias ukrainiens à l'INALCO.

Pour citer cet article : Valeriya SYTNIK (2026), « Ukraine : face à l'intensification des attaques cyber russes », *Regard sur l'Est*, 23 février.

Retour en haut de page

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