FORUM ST-LAURENT
sur la sécurité internationale

# LA CYBERGUERRE EN UKRAINE

Note politique étudiante
Par Frédérick Côté, École supérieure d'études internationales - Université Laval

***SOMMAIRE EXÉCUTIF***

- *Le conflit armé en Ukraine n'est pas une cyberguerre, celle-ci étant définie comme l'emploi létal de codes informatiques malicieux pour atteindre un objectif politique.*
- *L'arme cyber n'est pas décisive pour briser la volonté de l'adversaire dans la phase active des opérations militaires. Cette situation est due à la complexité de mise en œuvre de la* **Cyber Kill Chain***.*
- *La situation actuelle des forces russes offre une occasion d'initier la* **Cyber Kill Chain** *de manière à renforcer la dissuasion dans la durée.*

## BUT

Présenter un compte rendu des opérations cybernétiques observées dans l'actuel conflit armé entre l'Ukraine et la Russie et proposer un plan d'action.

## CONTEXTE

La réforme des forces armées russes amorcée en 2008 semblait indiquer que la Russie s'était dotée d'une capacité de cyberguerre robuste, capable notamment de perturber les systèmes des technologies de l'information (TI) adverses et d'exercer une influence sur l'opinion publique par le biais d'Internet. La cyberattaque de 2007 contre l'Estonie et les opérations en Crimée et dans le Donbass en 2014, ont donné l'impression que la cyberguerre représentait une composante essentielle de la

« guerre hybride » russe. De même, la sophistication de l'attaque SolarWinds de 2020 laissait entrevoir un haut degré d'expertise de la part de Moscou dans le domaine. Enfin, les rapports du gouvernement ukrainien faisant état d'une série de cyberattaques dans les semaines précédant l'invasion de son territoire laissaient planer l'ombre d'une menace cybernétique proéminente dans le cadre de cette guerre. Le conflit en Ukraine présentait donc la perspective de voir se réaliser le « Pearl Harbor électronique » craint depuis plusieurs années. Toutefois, en dépit des attentes, elle ne peut pas être qualifiée, à proprement parler, de cyberguerre. Cette réalité semble donner raison aux experts qui voyaient déjà dans l'arme cyber un moyen utile dans les conflits en « zone grise », mais mal adapté à la guerre ouverte. Néanmoins, quelques tendances peuvent être observées depuis le début des opérations et méritent d'être mentionnées pour nourrir la réflexion des forces armées et des chefs politiques.

**DISCUSSION**

**Observation 1 – Portée limitée des cyberopérations.** Les actions déployées jusqu'à présent dans le cyberespace se limitent à appuyer les opérations ciblées et celles du domaine informationnel, lesquelles conservent le rôle principal. Les cyberattaques observées revêtent un caractère rudimentaire et se limitent au déni de service (*Distributed Denial of Service* – DDos), au défacement ou à l'effaçage (*Wiping*) de données. Ces observations démontrent la place que revêt le domaine cyber dans la doctrine russe, qui conçoit celui-ci comme une composante de la guerre de l'information, comprenant également les opérations psychologiques, les communications stratégiques et la déception militaire. Il semble donc que les cyberattaques perpétrées par la partie russe visent avant tout à façonner les perceptions et le comportement du gouvernement ukrainien, de la population (principalement ukrainienne, mais également russe) et de la communauté internationale. Côté ukrainien, les cyberopérations relèvent avant tout du harcèlement contre des entreprises, des médias et des citoyens en Russie et en Biélorussie. L'objectif semble être avant tout de susciter des questionnements au sein de l'opinion publique adverse, qui reçoit peu d'informations sur la guerre en Ukraine, grâce au contrôle de l'information exercé par Moscou et Minsk.

**Observation 2 – Contraintes techniques et résilience des infrastructures.** Jusqu'à présent, les systèmes d'armes et autres infrastructures de défense des deux camps ne semblent pas avoir fait l'objet de cyberattaques capables de les détruire, de les neutraliser ou de perturber les opérations à grande échelle. Bien que cette affirmation soit difficile à vérifier avec certitude, considérant les impératifs de la sécurité opérationnelle, le déroulement des opérations militaires fournit quelques indices à cet effet. Notamment, l'armée russe n'a pas réussi à établir une suprématie aérienne, l'aviation et, surtout, les défenses antiaériennes ukrainiennes étant toujours en fonction. De plus, les succès rencontrés par le gouvernement ukrainien dans la guerre de l'information n'ont été possibles que par la résilience du réseau de télécommunications du pays. Les tentatives des Russes pour museler cette architecture au moyen de la destruction physique sont d'ailleurs révélatrices de leur incapacité à agir par des moyens TI. Ces constatations sont particulièrement surprenantes à la lumière de l'avantage affiché par la Russie dans ce domaine durant les huit années de la guerre au Donbass. Le haut niveau de pénétration de l'infrastructure ukrainienne des télécommunications par la Russie et la persistance des attaques contre les réseaux de communication de l'armée ukrainienne, dont le niveau technologique apparaissait insuffisant, laissaient en effet présager des attaques massives. Tout porte donc à croire que les mesures de durcissement implantées ces dernières années

dans les centres de commandement et de contrôle, les réseaux militaires et les systèmes soutenant l'opération des infrastructures clés, fonctionnent. En dépit d'attaques constantes sur les réseaux adverses, la Russie n'est pas parvenue à mettre en place les conditions de l'activation en temps opportun (c'est-à-dire en synchronisation avec la manœuvre militaire) de la *Cyber Kill Chain* (le cycle d'engagement nécessaire à la conduite d'une cyberattaque d'ampleur, allant de l'identification des cibles à la neutralisation, en passant par l'intrusion, l'exploitation, la prise de contrôle, la dissimulation et l'extraction).

**Observation 3 – Prolifération des acteurs.** Le théâtre ukrainien des opérations est marqué par la multiplication des acteurs dans le domaine cybernétique. S'il semble que les cyberopérations russes soient principalement dirigées par les services du renseignement militaire (le GRU), l'agence de sécurité fédérale (FSB) recrute des pirates informatiques provenant de groupes criminalisés. C'est ainsi que l'acteur malicieux APT28, suspecté d'être lié au GRU, a lancé une campagne d'hameçonnage contre les utilisateurs d'un fournisseur de services Internet ukrainien. Côté ukrainien, le ministre de la Digitalisation a mis sur pied l'armée informatique de l'Ukraine (*IT Army of Ukraine*), faisant appel aux pirates du monde entier pour s'attaquer aux ressources numériques de la Russie. Cet appel joue d'ailleurs sur le caractère déterritorialisé du cyberespace, ainsi que sur son accessibilité et son anonymat, deux éléments clés de la théorie entourant la cyberguerre. À noter que ces deux caractéristiques prennent tout leur sens à la suite de la déclaration de guerre faite à la Russie par le groupe Anonymous. L'attribution d'un grand nombre de cyberattaques à des individus ou à des groupes situés en dehors des sphères officielles de l'État pourrait par ailleurs constituer un élément explicatif de la portée somme toute limitée des cyberopérations des deux camps.

## CONCLUSION

La guerre en Ukraine fournit l'occasion d'observer en temps réel la place du domaine cyber dans un conflit armé. Jusqu'à présent, le constat semble indiquer une utilité limitée de l'arme cyber durant la phase des opérations actives (sauf possiblement dans la période initiale des opérations), les cibles privilégiées durant cette phase du conflit se prêtant mal à des cyberattaques de grande ampleur et pouvant être mieux affectées par d'autres moyens. Ainsi, il apparaît que certaines caractéristiques immuables dans la conduite de la guerre limitent la portée des innovations en TI. La diversité des acteurs participant aux cyberopérations, montre toutefois le caractère habilitant des TI, dont le coût d'entrée est peu élevé. On remarque par ailleurs la centralité du domaine cyber en appui à la guerre de l'information qui fait partie intégrante des opérations.

## RECOMMANDATION

Puisque l'emploi de l'arme cyber requiert un temps de préparation important et un fort soutien en renseignement (ce qui en fait une arme de prédilection sous le seuil du conflit armé), l'OTAN pourrait profiter de la situation de l'armée russe en Ukraine pour initier la *Cyber Kill Chain* et mettre en place les conditions pour d'éventuelles attaques de grande ampleur, renforçant de fait la dissuasion. Les forces russes éprouvant des problèmes de communication, elles se rabattent, au moins partiellement, vers des communications haute fréquence sans encryptage, qui pourraient s'avérer vulnérables à la guerre électronique et ouvrir la porte à d'éventuelles cyberattaques.

## Bibliographie


Akimenko, Valeriy & Keir Giles (2020). "Russia's Cyber and Information Warfare". *Asia Policy*, Vol. 27, No. 2, pp. 67-75.

Alperovitch, Dmitri & Ian Ward (12 mars 2021). "How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks?" *Lawfare*. https://www.lawfareblog.com/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks (Consulté le 6 avril 2022).

Brantly, Aaron F., Nerea M. Cal & Devlin P. Winkelstein (2017). *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*. West Point, Army Cyber Institute.

Cranny-Evans, Sam & Thomas Withington (9 mars 2022). "Russian Comms in Ukraine: A World of Hertz". *Royal United Services Institute Commentary* [En ligne], https://rusi.org/explore-our-research/publications/commentary/russian-comms-ukraine-world-hertz (Consulté le 23 mars 2022).

Fischerkeller, Michael P. & Richard J. Harknett (2017). "Deterrence is Not a Credible Strategy for Cyberspace". *Orbis*, Vol. 61, No. 3 (Summer 2017), pp. 381-393.

Florant, Jean-Baptiste (2021). "Cyberarmes : la lutte informatique offensive dans la manœuvre future." *Focus stratégique* No. 100, Laboratoire de Recherche sur la Défense de l'Institut français des relations internationales, janvier 2021.

Giles, Keir (2014). "A new Phase in Russian Military Transformation". *Journal of Slavic Military Studies*, Vol. 27, pp. 147-162.
Martin, Lieutenant-colonel P.E.C., Les écoles de pensée de la cyberguerre : combler le fossé épistémologique et ontologique, partie 1." *La Revue de l'Aviation royale canadienne*, Vol. 5, No. 4 (été 2016), pp. 45-73.

_____"Les écoles de pensée de la cyberguerre : combler le fossé épistémologique et ontologique, partie 2." *La Revue de l'Aviation royale canadienne*, Vol. 5, No. 4 (automne 2016), pp. 64-89.

Rapin, Alexis (15 mars 2022). "En Ukraine, les limites de la « cyberguerre »? *Chroniques des nouvelles conflictualités*, Chaire Raoul-Dandurand, Université du Québec à Montréal. https://dandurand.uqam.ca/wp-content/uploads/2022/03/2022-03-15-ARapin-Cyber-Ukraine.pdf (Consulté le 23 mars 2022).

Renz, Bettina (2016). "Russia and 'hybrid warfare'". *Contemporary Politics*, Vol. 22, No. 3, pp. 283-300.

Rid, Thomas (2012). "Cyber War Will Not Take Place". *Journal of Strategic Studies*, Vol. 35, No. 1, pp. 5-32.


### Sources journalistiques


BBC World (27 février 2022). "Deadly blast at Kyiv TV tower after Russia warns capital". *BBC World* [En ligne], https://www.bbc.com/news/live/world-europe-60542877 (Consulté le 23 mars 2022).

Fendorf, Kyle & Jessie Miller (15 mars 2022). *Tracking Cyber Operations and Actors in the Russia-Ukraine War*. Council on Foreign Relations. https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war (Consulté le 21 mars 2022).

Lyngass, Sean (4 mars 2022). "Volunteer hackers and IT specialists have entered the information war in defense of Ukraine, official says." *CNN* [En ligne]. https://www.cnn.com/europe/live-news/ukraine-russia-putin-news-03-04-22/h_6c140e369cb0e5aa3b2fdc309254bb6c (Consulté le 29 mars 2022).

_____ (8 mars 2022). "Russian Hacking in Ukraine was less than anticipated, NSA director tells US lawmakers." *CNN* [En ligne]. https://www.cnn.com/europe/live-news/ukraine-russia-putin-news-03-08-22/h_74886d0a4d035d6e42578f31677c6f51 (Consulté le 29 mars 2022).

Perry, Dave (animateur) (11 mars 2022). Air Operations Above Ukraine. Dans *Defence Deconstructed*. Podcast du Canadian Global Affairs Institute. https://www.cgai.ca/air_operations_above_ukraine (Consulté le 12 mars 2022).

Radio-Canada (23 février 2022). "L'Ukraine rapporte une nouvelle cyberattaque d'envergure". *Radio-Canada International* [En ligne]. https://ici.radio-canada.ca/nouvelle/1864265/cyberattaque-ukraine-russie-republique-donetsk-armee (Consulté le 23 mars 2022).

Tidy, Joe (7 mars 2022). "Twitter is part of our war effort – Ukraine minister". *BBC World* [En ligne]. https://www.bbc.com/news/technology-60608222 (Consulté le 23 mars 2022).

_____ (20 mars 2022). "Anonymous: How hackers are trying to undermine Putin". *BBC World* [En ligne]. https://www.bbc.com/news/technology-60784526 (Consulté le 22 mars 2021).