Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2023)
Heft: [1]: Numéro Thématique 1

Artikel: Opérations offensives dans le cyberespace ciblant l'Ukraine : un cyber Pearl Harbour?

Autor: Huskaj, Gazmend

DOI: https://doi.org/10.5169/seals-1055345

Cyber

Opérations offensives dans le cyberespace ciblant l'Ukraine : Un cyber Pearl Harbor ?

Gazmend Huskaj
Directeur de la cyber sécurité, Geneva Centre for Security Policy (GCSP)

Ces produits de recherche examinent la guerre cybernétique en Ukraine. La cyberguerre, définie comme « les actions d'un Etat-nation ou d'une organisation internationale pour attaquer et tenter d'endommager les ordinateurs ou les réseaux d'information d'un autre pays par, par exemple, des virus informatiques ou des attaques par déni de service » (RAND, 2022) est en cours dans la guerre russo-ukrainienne. Certains affirment que même si la Russie et les opérations cyberspatiales offensives parrainées par la Russie visent l'Ukraine, le soi-disant « cyber-Pearl Harbour » n'a pas eu lieu (voir par exemple Glosserman, 2012). Cependant, nous avons peut-être vu et voyons presque tous, mais pas tous, les éléments de ce qui constitue un « cyber-Pearl Harbor ».

En 2012, l'ancien secrétaire américain à la Défense Leon Panetta a décrit les cyber-capacités les plus destructrices comme impliquant « des cyber-acteurs lançant plusieurs attaques sur notre infrastructure critique en même temps, en combinaison avec une attaque physique » (Bumiller & Shanker, 2012). Le résultat de ce type de cyber-attaque destructrice a été défini comme une « cyber-Pearl Harbor qui causerait la destruction physique et la mort, une attaque qui paralyserait et choquerait la nation et créerait un nouveau sentiment profond de vulnérabilité » (Bumiller & Shanker, 2012).

Les menaces qui pèsent sur les infrastructures critiques sont réelles. La Russie et les acteurs de la menace parrainés par la Russie ont mené des opérations offensives dans le cyberespace visant l'Ukraine depuis l'annexion illégale de la Crimée. Les exemples incluent les attaques distribuées et par déni de service (DDoS) ciblant divers réseaux (Clayton, 2014) ; les e-mails de phishing aux entreprises de services publics du secteur de l'énergie (Park & Walstrom, 2017) ; et le sabotage par accès à distance en prenant le contrôle des systèmes de contrôle industriel et en ouvrant « des disjoncteurs dans quelque 30 sous-stations de distribution dans la capitale Kiev et dans la région ouest d'Ivano-Frankivsk, entraînant une perte de courant pour plus de 200'000 consommateurs » (Park & Walstrom, 2017). Et maintenant, depuis le 24 février 2022, les cibles ukrainiennes comprennent les réseaux gouvernementaux, les réseaux logistiques, les systèmes ferroviaires et une compagnie d'énergie nucléaire (Microsoft, 2022).

Ce produit de recherche examinera les opérations offensives du cyberespace russes et parrainées par la Russie ciblant des entités en Ukraine, et en relation avec la définition de Panetta d'un « cyber-Pearl Harbor », évaluera si un « cyber-Pearl Harbor » a lieu en Ukraine ou non. La contribution de ce produit de recherche est de présenter les implications des cyber-événements en Ukraine pour les décideurs politiques, ainsi que pour la cyberdéfense et l'infraction.

Méthodes et matériels

Ce produit de recherche est basé sur la philosophie de recherche de l'interprétivisme. L'interprétativisme concerne les humains et leur interprétation du monde (Saunders, Lewis & Thornhill, 2016). Ainsi, « le but de la recherche interprétative est de créer de nouvelles compréhensions et interprétations plus riches des mondes et des contextes sociaux » (Saunders, Lewis & Thornhill, 2016, p. 140).

La base théorique de ce produit de recherche est la théorie de l'intelligence, et bien qu'il n'y ait pas une seule théorie de l'intelligence (cf. Knorr, 1964), Marrin (2018) note que de nombreuses théories de l'intelligence peuvent être créées, et Johnson (2003), Eriksson, Fox, Gill et Rogg (2018) notent que toute théorie sur l'intelligence doit être basée sur le cycle de l'intelligence : planification et direction ; Le recueil; Traitement et Exploitation ; Analyse et Production ; Diffusion et intégration. La collecte de données est basée sur des sources ouvertes et l'analyse des données est basée sur l'analyse linguistique (Goldkuhl, 2002).

Tout d'abord, une analyse linguistique de la définition de l'ancien secrétaire américain à la Défense Leon Panetta d'un « cyber-Pearl Harbor » est effectuée. Ensuite, un cadre pour évaluer les opérations offensives dans le cyberespace est développé. Enfin, un ensemble de cas sera analysé à l'aide du cadre développé.

Résultats

L'analyse linguistique de la définition de l'ancien secrétaire à la Défense des Etats-Unis, Leon Panetta, d'un « cyber-Pearl Harbor » a révélé trois éléments: 1) *« plusieurs cyberattaques combinées à une attaque physique »*; 2) l'impact devrait être *« la destruction physique et la perte de vies »*; et 3) l'attaque *« paralyserait et choquerait la nation et créerait un nouveau sentiment profond de vulnérabilité »*. Enfin, il est sous-entendu que les cibles sont les infrastructures essentielles et les personnes.

Deux des composantes, 1 et 2, sont liées à la dimension cyber et une dimension physique ciblant directement les infrastructures critiques. L'analyse linguistique de la troisième composante révèle que l'attaque « rendrait impuissant, inutile ou inefficace; amortir l'action ou le pouvoir de » (= paralysie) et « une impression soudaine et inquiétante sur l'esprit » (= choc) la « race de personnes, un grand groupe de personnes ayant une ascendance et une langue communes » (= nation) et « apporter en être » (= créer) un « profond » (= profond) « fait ou établi pour la première fois, frais, récemment fait ou développé » (= nouveau) « percevoir ou comprendre (un fait ou une situation) non par perception directe » (= sens) de "blessure; blesser, blesser, blesser, mutiler » (= vulnérabilité).

Le cadre conçu sur la base de la définition de l'ancien secrétaire américain à la Défense Leon Panetta (DSLP) est ici connu sous le nom de cadre DSLP. Le cadre DSLP est présenté dans le tableau 1.

Tableau 1: Le cadre DSLP

Component 1 Attack Type	**Component 2 Impact of Attack**
Cyber attacks AND physical attacks	Physical destruction AND loss of life
Component 3 – Cognitive Effects	
Bring into being a deep, fresh, perceived wounding	
[PICTURE TO VISUALLY PRESENT THE PERCEIVED WOUNDING]	

Le cadre DSLP est conçu autour des trois composantes de la composante 1) *« plusieurs cyberattaques combinées à une attaque physique »*; Composante 2) l'impact devrait être « la destruction physique et la perte de vies »; et Composante 3) l'attaque *« paralyserait et choquerait la nation et créerait un nouveau sentiment profond de vulnérabilité »*.

Le composant 1 concerne les types d'attaques: cyber et cinétiques. Il existe de nombreuses définitions des types de cyberattaques. Pour cette recherche, cependant, la

Chaque action ou mouvement doit être couvert par un élément de défense contre-avions ou de guerre électronique. Au minimum, un élément est en mesure de donner l'alerte afin de protéger les effecteurs.

classification de la destruction, de la perturbation, de la désinformation et de la propagande et de la militarisation des données du CyberPeace Institute (2022) est utilisée. Les attaques de destruction sont définies comme des *« attaques visant à supprimer définitivement des données ou à endommager des systèmes les rendant irrécupérables »* et l'impact peut être *« des effets durables sur les organisations si elles ne sont pas en mesure de récupérer des sauvegardes ou de réinitialiser des systèmes »* (CyberPeace Institute, 2022).

Les attaques par perturbation consistent à "refuser complètement mais temporairement l'accès ou le fonctionnement de, une cible pour une période de temps. Une heure de démarrage et d'arrêt souhaitée est normalement spécifiée. La perturbation peut être considérée comme un cas particulier de dégradation où le niveau de dégradation est de 100% » (JCS, 2018, p. II-7). La désinformation et la propagande sont définies comme des « attaques axées sur la diffusion de fausses informations et de propagande » (CyberPeace Institute, 2022)

La militarisation des données est définie comme « les attaques menant au vol ou à l'exfiltration de données ou à l'acquisition de données à des fins d'espionnage, de surveillance ou de renseignement » (CyberPeace Institute, 2022).

Le tableau 2 présente les types d'attaques et le total sur la base des informations au 13 décembre 2022.

Disruption	**Disinformation & Propaganda**	**Data Weaponization**	**Destruction**
608	29	140	27

De ce qui précède, trois cas seront discutés plus en détail. Les trois cas sont liés à Odessa, Zaporizhzhia et Lviv. Le cadre DSLP sera appliqué dans chaque cas.

Cas 1 - Odessa

Component 1 Attack Type	**Component 2 Impact of Attack**
Cyber attacks AND physical attacks	Physical destruction AND loss of life
C - 14 Feb - Odessa-based critical infrastructure compromised by likely Russian actors.	
K - 4 April - Russian airstrikes hit fuel depots and processing plants around Odessa.	
Component 3 – Cognitive Effects	
Bring into being a deep, fresh, perceived wounding	
[PICTURE TO VISUALLY PRESENT THE PERCEIVED WOUNDING]	

Cas 2 - Zaporizhzhia

Component 1 Attack Type	**Component 2 Impact of Attack**
Cyber attacks AND physical attacks	Physical destruction AND loss of life
C - 2 Mar - Russian group moves laterally on network of Ukrainian nuclear power company.	
K - 3 Mar - Russia's military occupies Ukraine's largest nuclear power station.	
Component 3 – Cognitive Effects	
Bring into being a deep, fresh, perceived wounding	
[PICTURE TO VISUALLY PRESENT THE PERCEIVED WOUNDING]	

Cas 3 - Lviv

Component 1 Attack Type	**Component 2 Impact of Attack**
Cyber attacks AND physical attacks	Physical destruction AND loss of life
C - 19 Apr - IRIDIUM launches destructive attack on Lviv-based logistics provider.	
C - 29 Apr - IRIDIUM conducts reconnaissance against transportation sector network in Lviv.	
K - 3 May - Russian missiles strike railway substations, disrupting transport service.	
Component 3 – Cognitive Effects	
Bring into being a deep, fresh, perceived wounding	
[PICTURE TO VISUALLY PRESENT THE PERCEIVED WOUNDING]	

Discussion

Un « cyber-Pearl Harbor » se met en place en Ukraine. Depuis la race et les personnes ayant une ascendance et une langue communes, dans ce contexte, les Ukrainiens, ont été et sont ciblés et frappés par des cyberattaques et des attaques physiques contre des infrastructures critiques et causent des destructions physiques et des pertes de vie. Ces attaques ont et dans une certaine mesure rendent les Ukrainiens (en particulier les civils) impuissants, sont frappés par des meurtres insensés (de civils) et des infrastructures critiques qui créent une impression inquiétante dans l'esprit. Les attaques cybernétiques et cinétiques russes contre l'Ukraine ont créé une profonde nouvelle blessure perçue en Ukraine.

G. H.

Pour en savoir plus :

Bumiller, E. & Shanker, T. (2012). Panetta Warns of Dire Threat of Cyberattack on U.S. Retrieved from: https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

Clayton, M. (2014). Russia Hammers Ukraine With Massive Cyber-Attack. Retrieved from: https://www.businessinsider.com/russia-cyberattack-ukraine-2014-3?international=true&r=US&IR=T.

CyberPeace Institute. (2022). Cyber Threats. Retrieved from: https://cyberconflicts.cyberpeaceinstitute.org/threats.

Etymonline. (2022a). Paralyze. Retrived from: https://www.etymonline.com/word/paralyze

Etymonline. (2022b). Shock. Retrived from: https://www.etymonline.com/word/shock

Etymonline. (2022c). Nation. Retrived from: https://www.etymonline.com/word/nation

Etymonline. (2022d). Create. Retrived from: https://www.etymonline.com/word/create

Etymonline. (2022e). New. Retrived from: https://www.etymonline.com/word/new

Etymonline. (2022f). Sense. Retrived from: https://www.etymonline.com/word/sense

Etymonline. (2022g). Vulnerability. Retrived from: https://www.etymonline.com/word/vulnerability

Goldkuhl, G. (2002). Anchoring scientific abstractions – ontological and linguistic determination following socio- instrumental pragmatism. European Conference on Research Methods in Business and Management (ECRM 2002), Reading, 29-30 April 2002.

Glosserman, B. (2022). The conflict in Ukraine makes us rethink cyberwar. Retrieved from: https://www.japantimes.co.jp/opinion/2022/10/12/commentary/world-commentary/conflict-ukraine-makes-us-rethink-cyberwar/.

Joint Chiefs of Staff. (2018). Joint Publication 3-12 Cyberspace Operations. Retrieved from: https://fas.org/irp/doddir/dod/jp3_12.pdf.

Johnson, L. K. (2003). Bricks and Mortar for a Theory of Intelligence. Comparative Strategy, 22(1), 1–28. https://doi.org/10.1080/01495930390130481.

Knorr, K. (1964). Foreign intelligence and the social sciences. [Princeton, N.J.] Center of International Studies, Woodrow Wilson School of Public; International Affairs, Princeton University, 1964.

Marrin, S. (2018). Evaluating intelligence theories: current state of play. Intelligence and National Security, 33(4), 479–490. https://doi.org/10.1080/02684527.2018.1452567.

Microsoft. (2022). Defending Ukraine: Early Lessons from the Cyber War. Retrieved from: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

Park, D. & Walstrom, M. (2017). Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks. Retrieved from https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2016). Research Methods for Business Students (7th ed.). Financial Times/Prentice Hall.