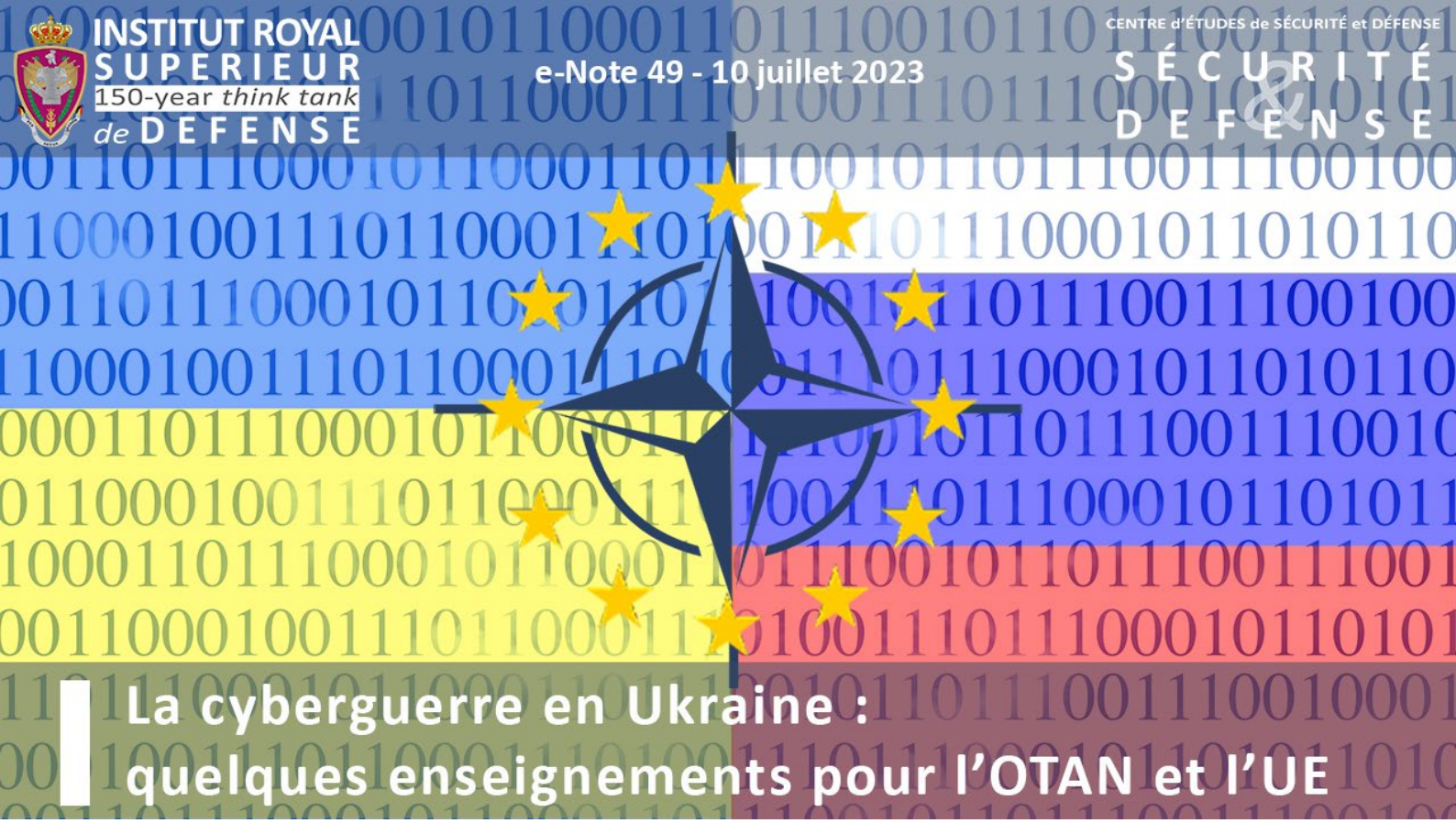
INSTITUT ROYAL SUPERIEUR de DEFENSE
150-year think tank
e-Note 49 - 10 juillet 2023
CENTRE d'ÉTUDES de SÉCURITÉ et DÉFENSE
SÉCURITÉ & DEFENSE



La cyberguerre en Ukraine : quelques enseignements pour l'OTAN et l'UE

Commandante d'aviation Estelle Hoorickx, PhD[1]

« Cyber-Pearl Harbour » : une menace improbable dans un conflit de haute intensité ?

Depuis le début de l'invasion de l'Ukraine par la Russie le 24 février 2022, les experts n'en finissent pas d'épiloguer sur les effets des cyberattaques menées par Moscou pour appuyer son « opération spéciale ». Alors que certains parlent de « cyberguerre qui n'a pas lieu », d'autres considèrent au contraire que les cyberattaques jouent un rôle facilitateur dans la campagne militaire. D'aucuns craignent enfin que la Russie ne lance des cyberopérations plus destructrices aux stades ultérieurs du conflit[2].

Pour Christian-Marc Liflander, les répercussions des cyberattaques menées par la Russie vont bien au-delà du sol ukrainien. Elles ont pour conséquence, « par un effet de vases communicants, d'augmenter le niveau général de la menace dans tous les domaines, cyber ou non, et remettent en question la stabilité internationale »[3]. Ainsi, d'après un rapport du géant américain de l'informatique

[1] Chercheuse à l'Institut royal supérieur de défense (IRSD)

[2] Andreas Loverdos, *Trouver le juste équilibre entre cyberopérations offensives et défensives : un défi croissant pour l'OTAN* (s.l. : Assemblée parlementaire de l'OTAN, 2023), 19, https://www.nato-pa.int/fr/document/2022-cyberoperations-offensives-ou-defensives-un-defi-pour-lotan-rapport-pinotti-015-dscfc.

[3] Sophie Caulier, « La guerre en Ukraine fait basculer le monde dans l'ère des cyberattaques », *Le Monde*, 12 février 2023, https://www.lemonde.fr/economie/article/2023/02/12/la-guerre-en-ukraine-fait-basculer-le-monde-dans-l-ere-des-cyberattaques_6161549_3234.html.

Google, les cyberattaques russes ont augmenté de 300 % dans les pays de l'OTAN en 2022 par rapport à 2020, et de 250 % en Ukraine[4]. Depuis l'annexion de la Crimée par la Russie en 2014, la part des attaques contre des États membres de l'UE serait passée de 9,8 % à 46,5 %[5]. En plus de poursuivre la recherche de vulnérabilités sur les réseaux ukrainiens, la Russie a augmenté ses opérations de cyberespionnage, de campagne de désinformation et ses cyberattaques chez les Alliés et les nations qui apportent leur assistance à l'Ukraine[6]. Julien Nocetti relativise néanmoins le lien entre les cyberopérations russes et la recrudescence des attaques visant les entreprises, les administrations et les hôpitaux observée ces derniers mois dans la plupart des pays occidentaux. Selon lui, « [l]es attaques d'hôpitaux ne sont pas totalement déconnectées du conflit, puisque la plupart des logiciels de rançonnage émanent historiquement de Russie. Mais la plupart sont probablement opportunistes et profitent du brouillard ambiant »[7].

Si des débats subsistent à propos de la manière de quantifier et de décrire le volet cybernétique de la guerre en Ukraine, celui-ci est particulièrement bien documenté[8]. Pour Kevin Limonier, « c'est la première fois dans un conflit de haute intensité que l'occupation sur le territoire physique s'accompagne en temps réel d'une occupation en parallèle sur le terrain numérique »[9]. Jusqu'à présent, le recours à l'arme cyber s'inscrivait essentiellement dans le cadre de « guerres hybrides », consistant à mettre en œuvre, de manière souvent coordonnée, une panoplie de moyens conventionnels et non conventionnels afin d'exploiter les vulnérabilités de l'adversaire sans avoir à subir les conséquences d'une opération militaire en bonne et due forme. On a pu observer un bon exemple de l'usage du cyber en contexte hybride lors de l'invasion de la Crimée par la Russie en 2014[10].

Selon James Andrew Lewis, les cyberopérations liées à la guerre en Ukraine constituent un « cas d'école qui préfigure ce qui se passera dans les futurs conflits »[11]. Pour cet expert en cybersécurité, le principal enseignement de cette guerre est qu'« une bonne défense peut résister à une campagne cyber. Et c'est une des raisons pour lesquelles les Russes doivent finalement déployer des missiles

[4] Shane Huntley, « Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape », *Threat Analysis Group* (blog), 16 février 2023, https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

[5] Ingrid Vergara, « Le " bouclier cyber " de l'UE prendra forme en 2024 », *Le Figaro*, 5 avril 2023, https://www.lefigaro.fr/secteur/high-tech/le-bouclier-cyber-de-l-ue-prendra-forme-en-2024-20230405.

[6] Loverdos, *Trouver le juste équilibre*, 21. Ainsi par exemple, une opération de propagande, vaste et sophistiquée, a produit pendant plus d'un an de faux sites officiels français et de faux articles de médias (Florian Reynaud et Damien Leloup, « Révélations sur " Doppelgänger ", la campagne de désinformation russe dénoncée par la France », *Le Monde*, 13 juin 2023, https://www.lemonde.fr/pixels/article/2023/06/13/revelations-sur-doppelganger-la-campagne-de-desinformation-russe-denoncee-par-la-france_6177446_4408996.html.

[7] Pierre-Yves Bocquet, « Cyberguerre. Les premières leçons », *Epsiloon*, n° 20 (février 2023) : 24, https://www.epsiloon.com/common/product-article/135.

[8] Sur les opérations numériques en Ukraine, lire notamment les rapports du *Cyber Peace Institute* : https ://cyberpeaceinstitute.org/news/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q1-2023/ ; les analyses de Microsoft : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK et https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf ; ou encore les mises à jour régulières du programme « Cyber Vault » des *National Security Archives* de la *George Washington University* : https://nsarchive.gwu.edu/document/29562-cyber-vault-ukraine-timeline.

[9] Bocquet, « Cyberguerre. Les premières leçons », 28.

[10] Sur l'émergence de la problématique hybride (et sa terminologie) dans les milieux européens et otaniens, lire notamment : Estelle Hoorickx, « La défense contre les " menaces hybrides " : la Belgique et la stratégie euro-atlantique », *Sécurité & Stratégie* (Institut royal supérieur de défense), n° 131 (octobre 2017), https://www.defence-institute.be/publications/securite-strategie/ss-131/.

[11] Bocquet, « Cyberguerre. Les premières leçons », 23.

pour infliger des dommages à des infrastructures critiques. »[12] D'après les informations disponibles, les cyberopérations menées de manière constante par la Russie (activités de sabotage, d'espionnage et de subversion essentiellement)[13] n'ont, jusqu'à présent, pas eu d'impact décisif sur la conduite des opérations, notamment si on les compare aux actions cinétiques[14]. Pour Stéphane Taillat, ces cyberattaques ont essentiellement « des effets indirects » qui contribuent à appuyer les opérations militaires par des actions de déstabilisation ou par l'atteinte d'avantages relatifs (en matière de renseignement ou d'influence)[15].

Certaines de ces attaques sont pourtant de haut niveau. Ainsi par exemple, le jour-même de l'invasion, une importante attaque informatique, visant le satellite KA-SAT de l'entreprise américaine VIASAT, a entraîné des défaillances de communication sur le sol ukrainien mais également dans quelques autres pays européens[16]. Les infrastructures critiques ukrainiennes (réseaux électriques et de télécommunications en particulier) font également l'objet de cybersabotages réguliers[17]. Les câbles sous-marins – pièces incontournables des structures de commandement et de contrôle (C2) et des systèmes d'armes intégrés –, sont aussi des cibles potentielles, notamment par la voie cyber[18]. En juin 2023, l'UE et l'OTAN ont dès lors annoncé la mise en place d'une *task force* pour la résilience et la protection des infrastructures critiques, « au vu des actions du président Poutine, qui se sert des approvisionnements énergétiques comme d'une arme, et du sabotage des gazoducs Nord Stream » (dixit Jens Stoltenberg)[19]. De son côté, l'UE développe une véritable politique européenne sur la cyberdéfense (*EU Policy on Cyber Defence*). Celle-ci vise à augmenter la posture de dissuasion européenne, à mieux détecter les cyberattaques, à développer des capacités de « réponse active » et, enfin, à créer une solidarité opérationnelle[20]. Cette politique vise notamment la mise en place

[12] Bocquet, « Cyberguerre. Les premières leçons », 25.
[13] Nicolas Mazzucchi, « Cyberattaques et cyberconflits », dans *Atlas militaire et stratégique*, dir. Bruno Tertrais, (Paris : Autrement, 2023), 24, https://www.autrement.com/atlas-militaire-et-strategique/9782080416285.
[14] Bocquet, « Cyberguerre. Les premières leçons », 24. ; Stéphane Taillat, « Les cyberopérations dans la guerre en Ukraine », *Défense & Sécurité Internationale*, n° 159 (mai-juin 2022) : 90, https://www.areion24.news/2022/08/08/les-cyberoperations-dans-la-guerre-en-ukraine/.
[15] Taillat, « Les cyberopérations dans la guerre en Ukraine », 90.
[16] Taillat, « Les cyberopérations dans la guerre en Ukraine », 90. L'attaque du réseau satellitaire KA-SAT n'était pas le fait d'une action de guerre électronique, même si la maîtrise de la guerre électronique va rester d'autant plus stratégique qu'elle est perçue comme l'une des armes les plus viables dans l'espace (Lauraline Maniglier, « Guerre électronique en Ukraine, quels enseignements ? » CERBAIR, 6 octobre 2022, https://www.cerbair.com/fr/guerre-electronique-en-ukraine-quels-enseignements/. ; Romain Mielcarek, « [Décryptage] De la haute intensité à l'espace, les défis de la guerre électronique », *B2 Pro Le quotidien de l'Europe géopolitique*, 15 juin 2023, https://club.bruxelles2.eu/2023/06/decryptage-de-la-haute-intensite-a-lespace-les-defis-de-la-guerre-electronique/).
[17] Alexis Rapin, « Invisible, impotent ou immature ? Premières leçons de l'usage du cyber en Ukraine », *Le Rubicon*, n°20 (février 2023) : 24, https://lerubicon.org/publication/premieres-lecons-de-lusage-du-cyber-en-ukraine/.
[18] Sur le sujet, lire notamment : Aurélie Pugnet et Hugo de Waha, « [Analyse] Assurer la sécurité des câbles sous-marins : deuxième défi européen après les gazoducs ? », *B2 Pro Le quotidien de l'Europe géopolitique*, 21 octobre 2022, https://club.bruxelles2.eu/2022/10/analyse-assurer-la-securite-des-cables-sous-marins-deuxieme-defi-europeen-apres-les-gazoducs/.
[19] « L'OTAN et l'UE mettent en place une équipe spéciale pour la résilience et la protection des infrastructures critiques », OTAN, 12 janvier 2023, https://www.nato.int/cps/fr/natohq/news_210611.htm ; *EU-NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report* (s.l. : European Commission, 2023), https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en.
[20] Aurélie Pugnet, « [Actualité] La stratégie cyber défense révisée à l'aune de la guerre en Ukraine », *B2 Pro Le quotidien de l'Europe géopolitique*, 11 novembre 2022, https://club.bruxelles2.eu/2022/11/actualite-la-strategie-cyber-defense-revisee-a-laune-de-la-guerre-en-ukraine/.

d'un « bouclier cyber » qui devrait prendre forme en 2024[21]. Le Centre des cyberopérations (CyOC) de l'OTAN devrait être quant à lui pleinement opérationnel dans le courant de l'année 2023[22].

D'après Susan Landau, la cybercapacité russe – régulièrement classée dans le top 5 des cyberpuissances mondiales – n'est pas, comme certains le pensent, moins bonne que prévu. C'est juste que le cyber « n'est (…) peut-être pas l'arme la plus adaptée dans une guerre que l'on veut mener en deux semaines en envahissant un territoire »[23]. Pour James Andrew Lewis, « le cyber est bien meilleur que toute autre technique quand il s'agit d'espionner et d'influencer ». Les experts sont d'ailleurs surpris de voir comment l'armée russe reroute vers la Russie les connexions Internet des territoires qu'elle envahit au fur et à mesure de son avancée sur le territoire ukrainien. Ce *modus operandi* lui permet de mettre la main sur les réseaux d'information et de soumettre les populations conquises au même régime de restrictions et de censure que sa propre population[24]. La force du narratif russe sur la responsabilité de l'OTAN dans le déclenchement du conflit illustre également l'importance de la « stratégie d'influence informationnelle » menée par le Kremlin vis-à-vis des sociétés occidentales mais également vis-à-vis de sa propre population[25].

Comme le souligne Julien Nocetti, l'omniprésence des téléphones portables et des autres appareils photo sapent néanmoins, d'une manière tout à fait inédite, le monopole des gouvernements sur le contrôle des informations provenant des zones de guerre. Utilisée massivement par les soldats des deux camps, l'application de messagerie instantanée chiffrée Telegram est également devenue une source d'information stratégique sur ce qui se passe sur le champ de bataille[26]. La guerre électronique, bien moins visible car totalement passive, est également essentielle pour le renseignement. Elle permet notamment de situer les systèmes sol/air, les troupes ou les postes de commandement adverses, et même pour écouter le contenu des communications radio[27]. D'aucuns estiment pourtant que « le cyber est en train de phagocyter la guerre électronique (…) [alors que] la guerre en Ukraine montre l'importance des moyens classiques : protéger, brouiller, localiser »[28].

Une des principales difficultés que rencontrent les acteurs gouvernementaux russes et leurs « proxys » porte sur le maintien d'un rythme opérationnel soutenu pour mener leurs cyberopérations, dans un domaine où le cycle de planification est long et où la conduite est sensible aux facteurs d'opportunité[29]. Les capacités organisationnelles, opérationnelles, techniques et humaines représentent en effet un volume important dans la conduite de cyberopérations offensives[30]. En outre, pour influencer de manière significative une guerre de haute intensité, les opérations cybernétiques doivent être menées à un rythme que la Russie n'a apparemment pu

[21] Concrètement, cinq à six centres opérationnels de sécurité (SOC) seront installés à plusieurs endroits stratégiques du territoire européen afin de mieux détecter les attaques informatiques en amont (Ingrid Vergara, « Le " bouclier cyber " de l'UE prendra forme en 2024 », *Le Figaro*, 5 avril 2023, https://www.lefigaro.fr/secteur/high-tech/le-bouclier-cyber-de-l-ue-prendra-forme-en-2024-20230405).
[22] Loverdos, *Trouver le juste équilibre*, 16.
[23] Bocquet, « Cyberguerre. Les premières leçons », 25.
[24] Bocquet, « Cyberguerre. Les premières leçons », 27.
[25] Kévin Limonier, « La stratégie d'influence informationnelle russe », La Grande Conversation, 4 avril 2023, https://www.lagrandeconversation.com/monde/la-strategie-dinfluence-informationnelle-russe/.
[26] Bocquet, « Cyberguerre. Les premières leçons », 27-28.
[27] Maniglier, « Guerre électronique en Ukraine, quels enseignements ? ».
[28] Mielcarek, « [Décryptage] De la haute intensité à l'espace ».
[29] Stéphane Taillat, « Guerre en Ukraine : un an après », *Défense & Sécurité Internationale*, n° 164 (mars-avril 2023) : 88, https://www.areion24.news/2023/06/02/guerre-en-ukraine-un-an-apres/.
[30] Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (Oxford: Oxford University Press, 2022), 163-166.

maintenir que pendant quelques semaines[31]. Pour Lennart Maschmeyer, « plus les effets que vous souhaitez produire sont intenses, plus les cyberopérations seront lentes et peu fiables, et inversement. C'est ce qui rend la menace d'un cyber-Pearl Harbour peu probable »[32].

L'efficacité de la cyberdéfense des armées : un frein à la cyberconflictualité ?

Depuis le début du conflit, l'efficacité de la cyberdéfense ukrainienne contribue largement à l'« apparente absence de cyberconflictualité »[33]. Le soutien de l'OTAN et de l'UE, dont bénéficie l'Ukraine depuis 2014 pour développer ses capacités numériques et résister aux cyberattaques régulières de la Russie, contribue à cette cyberrésilience[34]. En mai 2023, l'Ukraine a également rejoint le Centre d'excellence coopératif de cyberdéfense de l'Otan (CCDCOE), situé à Tallinn[35]. Le gouvernement ukrainien bénéficie en outre d'un soutien extérieur décisif apporté par toute une série d'acteurs non étatiques (ou semi-étatiques)[36]. C'est d'ailleurs la première fois que des entreprises privées qui se revendiquent comme apolitiques – telles que Starlink, Microsoft ou Google –, s'engagent de façon aussi forte et aussi ouverte aux côtés d'un belligérant[37]. Microsoft et Google jouent ainsi un rôle déterminant dans la remédiation et la prévention de certaines attaques subies par l'Ukraine tandis que Starlink lui fournit l'accès à internet par satellite. Si certains se réjouissent de l'implication de ces entreprises privées en faveur de l'Ukraine, d'autres craignent qu'une telle dépendance technologique vis-à-vis d'acteurs extra-européens ne limite la souveraineté opérationnelle des armées[38]. En février 2023, la décision d'Elon Musk de ne plus permettre à Kiev d'utiliser Starlink à des fins militaires a d'ailleurs relancé le débat sur la souveraineté technologique des États. L'OTAN dispose quant à elle de quelques outils destinés à renforcer son autonomie. Ainsi par exemple, depuis 2021, l'outil informationnel MERLIN lui permet d'avoir une perception des informations échangées sur internet et les réseaux sociaux afin de garder une certaine supériorité cognitive[39].

Enfin, les groupes de pirates informatiques, qui soutiennent le camp ukrainien depuis le début de la guerre – Anonymous et l'« Armée informatique d'Ukraine » (IT Army of Ukraine)[40] en particulier –,

[31] Jon Bateman, Nick Beecroft et Gavin Wilde, « What the Russian Invasion Reveals About the Future of Cyber Warfare », *Carnegie Endowment for International Peace*, 19 décembre 2022, https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667.

[32] Bocquet, « Cyberguerre. Les premières leçons », 29.

[33] Bocquet, « Cyberguerre. Les premières leçons », 22.

[34] Nidal Taibi, « Guerre en Ukraine: " L'Ukraine est aujourd'hui mieux préparée en cyberdéfense " », *Le Vif,* 6 mars 2022, https://www.levif.be/international/guerre-en-ukraine-lukraine-est-aujourdhui-mieux-preparee-en-cyberdefense/ ; Élise Viniacourt, « Guerre en Ukraine : les États-Unis indiquent mener des cyberattaques, la Russie menace », *Libération*, 7 juin 2022, https://www.liberation.fr/international/europe/guerre-en-ukraine-les-etats-unis-revelent-mener-des-cyberattaques-la-russie-menace-20220607_3RIL2RF52VHW5GYBVXJ2KGK2DM/.

[35] « Guerre en Ukraine : Kiev rejoint le centre de cyberdéfense de l'Otan », *RTBF*, 17 mai 2023, https://www.rtbf.be/article/guerre-en-ukraine-kiev-rejoint-le-centre-de-cyberdefense-de-lotan-11199260.

[36] Les acteurs non étatiques (principaux acteurs du secteur numérique) et semi-étatiques (groupes d'hacktivistes ou cybercriminels) se distinguent par la relation de proximité ou de distance construite avec les acteurs gouvernementaux [Florian Egloff, *Semi-State Actors in Cybersecurity* (Oxford : Oxford University Press, 2021)].

[37] Bocquet, « Cyberguerre. Les premières leçons », 26.

[38] Bocquet, « Cyberguerre. Les premières leçons », 26-27.

[39] Nicolas Gros-Verheyde, « Merlin, le nouvel outil informationnel de l'OTAN », *B2 Le Quotidien de l'Europe géopolitique*, 21 octobre 2021, https://www.bruxelles2.eu/2021/10/merlin-le-nouvel-outil-informationnel-de-lotan/.

[40] L'IT Army of Ukraine a été mobilisée par le gouvernement ukrainien dès février 2022. Le statut juridique des hackers qui la composent de manière volontaire soulève néanmoins d'épineuses questions juridiques (Amaelle Guiton, « L'IT Army of

jouent également un rôle non négligeable, notamment par les attaques en déni de service[41] qu'ils mènent contre l'ennemi de manière continue. De son côté, le Kremlin est également soutenu par des groupes de hackers (Conti et KillNet, notamment) qui, – et c'est une première, précise Julien Nocetti – se sont livrés à des attaques spontanées, augmentant un peu la confusion qui règne sur le front cyber[42].

La nécessité de renforcer la cyberdéfense fait en tout cas son chemin, dans les armées en particulier. Depuis plusieurs années, les Américains insistent même sur la nécessité de renforcer leurs cybercapacités offensives pour dissuader toute cyberattaque à leur encontre[43].

Conclusions et réflexions pour l'OTAN et l'UE

S'il est évidemment impossible de tirer des conclusions définitives sur le rôle joué par les cyberopérations dans la guerre russo-ukrainienne, quelques réflexions peuvent déjà être formulées. Tout d'abord, la défense des systèmes d'information et de communication est essentielle pour contrer les offensives cyber. Ensuite, les acteurs non étatiques (ou semi-étatiques) – tels que les GAFAM et autres géants de la technologie, mais également les groupes d'hacktivistes – sont appelés à jouer un rôle de plus en plus important dans les conflits, renforçant ainsi leur position dominante dans le paysage cyber de la guerre. Enfin, les « ingérences dans l'espace de l'information »[44] se matérialisent désormais par la reconfiguration, en temps réel, des réseaux numériques situés sur les territoires conquis.

La guerre en Ukraine rappelle avec force aux dirigeants de l'UE et de l'OTAN que le maintien et l'intensification du soutien politique et militaire à l'Ukraine passe aussi par l'amélioration de la résilience et des défenses cyber de Kiev. Il convient dès lors de redoubler d'efforts pour soutenir les cyberdéfenses de l'Ukraine dans la durée. Les répercussions numériques de la guerre sur les pays occidentaux mettent également en exergue l'importance de renforcer la cyberdéfense de l'OTAN – notamment au travers des « plans de résilience nationaux » et des nouveaux « plans régionaux de défense du territoire allié », qui feront appel à plus de 300 000 militaires placés dans un état de préparation élevé[45]. Comme évoqué dans sa nouvelle « politique de cyberdéfense », dont les lignes

---

Ukraine, l'armée numérique qui brouille l'Internet russe », *Libération*, 14 février 2023, https://www.liberation.fr/international/europe/lit-army-of-ukraine-larmee-numerique-qui-brouille-linternet-russe-20230214_VZAOH6DNYZEUJMB34HJSI65IHY/).

[41] Les « attaques en déni de service » (*DOS-Deny of Service*) sont destinées à empêcher les utilisateurs légitimes d'un service internet d'utiliser celui-ci.

[42] Bocquet, « Cyberguerre. Les premières leçons », 27-28.

[43] Bocquet, « Cyberguerre. Les premières leçons », 25.

[44] L'UE définit les « ingérences étrangères dans l'espace de l'information » (qui ont souvent lieu dans le cadre d'une opération hybride plus large), comme « des efforts coercitifs et trompeurs déployés par un acteur d'un État étranger ou des agents de celui-ci dans le but d'entraver la formation et l'expression libres de la volonté politique des individus » [*Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions relative au plan d'action pour la démocratie européenne (COM(2020) 790 final)* (Bruxelles : Commission européenne, 2020), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020DC0790].

[45] Amélie Zima, « La présence avancée renforcée de l'OTAN (eFP) dans les pays baltes et en Pologne : apports et limites de la dissuasion conventionnelle multilatérale », *Note de recherche IRSEM*, n° 131, 12 octobre 2022, 18, https://www.irsem.fr/institut/actualites/note-de-recherche-n-131-2022.html. ; Nicolas Gros-Verheyde, « [Décryptage] Sommet de Madrid (OTAN) : les points clés de la déclaration finale », *B2 Pro Le quotidien de l'Europe géopolitique*,

essentielles ont été dévoilées lors du sommet de Bruxelles de 2021, la cyberrésilience de l'Alliance doit avoir lieu aux niveaux militaire (le cyberespace est reconnu comme un domaine d'opérations depuis 2016), politique (la cyberdéfense contribue aux efforts de dissuasion)[46] et technique (protection des « Systèmes d'information et de communication » (SIC) de l'OTAN)[47].

La troisième déclaration UE-OTAN laisse entrevoir la volonté de renforcer la coopération entre les deux organisations dans la lutte contre les menaces hybrides et cybernétiques[48]. Cette déclaration appelle néanmoins des mesures concrètes et rapides, qui devraient être annoncées dans une prochaine feuille de route, dont la date de publication n'a pas encore été fixée[49]. L'interopérabilité des capacités cyber, la riposte commune face aux attaques cybernétiques et aux ingérences informationnelles mais également la souveraineté opérationnelle vis-à-vis des acteurs numériques non étatiques ou semi-étatiques font partie des sujets cruciaux à aborder.

30 juin 2022, https://club.bruxelles2.eu/2022/06/decryptage-sommet-de-madrid-otan-les-points-cles-de-la-declaration-finale/. ; Olivier Jehin, « [Actualité] Avant Vilnius, ce qu'il faut retenir de l'actualité ministérielle en matière de défense OTAN : Ukraine, Adhésion, 2 % », *B2 Pro Le quotidien de l'Europe géopolitique*, 16 juin 2023, https://club.bruxelles2.eu/2023/06/actualite-ministerielle-defense-lukraine-au-coeur-de-toutes-les-discussions-avant-vilnius/.

[46] Depuis 2014, l'OTAN considère que l'impact des cyberattaques « sur les sociétés modernes pourrait être tout aussi néfaste que celui d'une attaque conventionnelle » et affirme qu'« il reviendrait au Conseil de l'Atlantique Nord de décider, au cas par cas, des circonstances d'une invocation de l'article 5 à la suite d'une cyberattaque », comme il le ferait en cas d'agression armée (Chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue au pays de Galles les 4 et 5 septembre 2014, « Déclaration du sommet du Pays de Galles ». OTAN, 5 septembre 2014, § 72, https://www.nato.int/cps/fr/natohq/official_texts_112964.htm).

[47] Nicolas Gros-Verheyde, « En cas de cyberattaque, peut-on déclencher l'article 5 et une réponse militaire ? » *B2 Pro Le quotidien de l'Europe géopolitique*, 31 mars 2022, https://club.bruxelles2.eu/2022/03/en-cas-de-cyberattaque-peut-on-declencher-larticle-5-et-une-reponse-militaire/. ; « L'article 5 pourra être invoqué pour une attaque dans l'espace et le cyberespace [Sommet de Bruxelles] », *B2 Pro Le quotidien de l'Europe géopolitique*, 16 juin 2021, https ://club.bruxelles2.eu/2021/06/larticle-5-pourra-etre-invoque-pour-une-attaque-dans-lespace-et-le-cyberespace-sommet-de-bruxelles/.

[48] « Joint Declaration on EU-NATO Cooperation, 10 January 2023 », Conseil de l'Europe, 10 janvier 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/.

[49] Aurélie Pugnet, « [Confidentiel] La troisième déclaration UE-OTAN enfin prête pour donner les pleins pouvoirs à l'OTAN (v2) », *B2 Pro Le quotidien de l'Europe géopolitique*, 10 janvier 2023, https://club.bruxelles2.eu/2023/01/confidentiel-la-troisieme-declaration-ue-otan-enfin-prete-pour-donner-tous-les-pouvoirs-a-lotan/.