diploweb.com La revue géopolitique
ISSN : 2111-4307

Renseignement, cyberguerre et nouvelles technologies : les civils sont-ils un moyen asymétrique redoutable dans la guerre en Ukraine ?

dimanche 9 mars 2025,par Anastasia KRYVETSKA

Citer cet article / To cite this version :
Anastasia KRYVETSKA, **Renseignement, cyberguerre et nouvelles technologies : les civils sont-ils un moyen asymétrique redoutable dans la guerre en Ukraine ?**, *Diploweb.com : la revue géopolitique, 9 mars 2025.*

La guerre russe en Ukraine a été à l'origine de la "première cyber-guerre mondiale". Anastasia Kryvetska présente de manière documentée l'indispensable rôle de l'« arrière » dans ce conflit au cœur d'une reconfiguration du monde. Nul doute que de nombreux états-majors se penchent sur ces évolutions à la fois techniques et sociétales… quand les pays de l'UE se trouvent sommés de compenser les aléas américains.

L'INVASION de l'Ukraine par la Russie le 24 février 2022 a accéléré l'intégration du cyber au sein du ministère de la Défense de l'Ukraine et permis de renforcer d'autres dynamiques liées au développement du cyber. Parmi ces dynamiques, une grande mobilisation des civils [1] dans la lutte contre l'agresseur russe dans le cyberespace [2], au point qu'aujourd'hui l'effort de guerre de l'arrière du front paraît un complément indissociable des opérations réalisées par les services ukrainiens compétents. Par ailleurs, avant d'être une priorité pour le ministère de la Transformation numérique, la numérisation du ministère de la Défense de l'Ukraine et l'intégration du cyber en son sein ont été des initiatives civiles. Ces dernières démontrent aujourd'hui une grande efficacité sur le front avec un déploiement de drones sans précédent dans l'histoire militaire. Ces dynamiques du développement du cyber, au même titre que l'intégration des composantes cyber dans les Armées, mettent en exergue une véritable mise en place d'une économie de guerre cyber en Ukraine.

Ces constats poussent à **explorer l'indispensable rôle de l'« arrière » dans la guerre hybride depuis l'invasion russe de l'Ukraine**.

Premièrement, il convient de se pencher sur l'implication de l' « arrière » dans la « première cyber-guerre mondiale » à travers une description du travail des cyber-volontaires réalisé en autonomie, mais aussi en coopération accrue avec l'État. Le rôle de l'arrière sera également étudié par le biais de la transformation numérique du ministère de la Défense de l'Ukraine dans un second temps. Transformation devenue visible par le développement d'un outil de guerre en réseau info-centré, mais aussi par les changements dans le complexe militaro-industriel.

I. « L'arrière » à l'épreuve de la « première cyber-guerre mondiale »

Au lendemain de l'invasion de l'Ukraine, le ministère de la Transformation numérique lance [3] la création de *l'IT-Army of Ukraine*, une cyber-armée composée de volontaires dont la composition est similaire à celle observée après le début de la guerre dans le Donbass [4]. Ce lancement a eu pour effet de regrouper des volontaires du monde entier souhaitant défendre l'Ukraine dans le cyberespace, mais aussi réaliser des attaques informatiques sur les systèmes russes. C'est notamment la raison pour laquelle le législateur ukrainien a amendé l'article 361 et 361-1 du Code pénal, décriminalisant la recherche de vulnérabilités dans les structures de l'État [5].

A. Le travail autonome des cyber-volontaires ukrainiens

Les activités cybernétiques des volontaires ukrainiens et pro-ukrainiens n'ont cessé de

perturber les systèmes russes depuis l'invasion. Le communiqué du site officiel de *l'IT-Army* précise que l'organisation est à la recherche de **hackers** capables de réaliser des attaques informatiques, diffuser des virus, réaliser des campagnes de phishing, ainsi que d'organiser des collaborations entre les cyber-combattants. La formation de cette cyber-armée a permis à de nouveaux groupes de hackers de se former, tels que C*yber Cosaques, Hdr0, Dump Forums,* et bien d'autres.

Même si ces groupes de hackers communiquent assez peu sur leurs activités, il est possible d'en avoir une idée grâce à certaines interviews. Étant donné la participation d'étrangers et le nombre d'attaques menées, les hackers ukrainiens estiment que le monde entier participent aux cyber offensives contre la Russie et qu'il s'agit d'une véritable première « cyber-guerre mondiale » [6] . D'après ces experts informatiques, toutes les méthodes sont acceptables face à la Russie, même celles qui relèvent de la pratique du hacking non-éthique, car il s'agit d'une guerre totale. L'invasion de l'Ukraine a ainsi contribué à renverser le rapport de force avec la Russie dans le cyberespace : maintenant c'est au tour de la Russie d'être un laboratoire pour de nombreux hackers. Ce positionnement a causé plusieurs incidents avec d'autres organismes, notamment la Croix Rouge, qui a édicté une liste de règles à respecter pendant une cyberguerre. Cette publication a révolté les hacktivistes ukrainiens et le groupe *Hdr0* a même défacé [7] le site de la filiale russe de la Croix rouge, car ses représentants russes auraient humilié des prisonniers de guerre ukrainiens.

En parallèle du front numérique qui se forme, des civils ukrainiens participent à la formation militaire

En parallèle du front numérique qui se forme, des civils ukrainiens participent à la formation militaire dispensée dans les rues de Lviv au début de l'invasion de l'Ukraine. Mars 2022. Photo de Paul Dza pour Sipa

Paul Dza/Sipa

Concernant la structure des groupes de cyber-volontaires, celles-ci regroupent des amateurs et des professionnels du cyber sans aucun organe coordinateur. Cela demeure un avantage, notamment dans le cas où certains participants seraient compromis. Les cyber-volontaires sont acceptés dans ces cyber-structures selon leurs compétences, et sont répartis en groupes en fonction des spécialités (carding, scamming, hacking, OSINT, etc.). Les novices sont tout d'abord invités à consulter de nombreuses ressources méthodologiques mises à disposition gratuitement afin de monter en compétences avant de rejoindre certains groupes. Les hackers de ces cyber-structures alimentent et rendent disponibles des bases de données comportant des données des citoyens russes, y compris celles des forces de l'ordre, afin d'assister les

cyber-volontaires en activité. Ces structures de cyber-volontaires comptent parmi les recrues de nombreux cybercriminels afin d'extorquer de l'argent aux entreprises russes ou des célébrités pro-Kremlin afin de le reverser aux Forces armées de l'Ukraine (*ZSU*). D'après les spécialistes, les cybercriminels professionnels seraient particulièrement créatifs et utiles dans la construction d'opérations cybernétiques.

Outre les attaques DDoS réalisées par une grande partie des cyber-volontaires au début de l'invasion, mais que *l'Ukrainian Cyber Alliance* a critiqué pour leur faible efficacité et le gaspillage de potentielles cibles, les hackers-volontaires ukrainiens ont dévoilé plusieurs pratiques et missions réussies telles que la compromission des bases de données des clients de *YandexEats* et de la *Sberbank*. La première aurait permis de révéler [8] l'identité de plusieurs agents du renseignement militaire russe (*GRU*), grâce aux nombreuses livraisons de nourriture à l'adresse du bâtiment de l'administration. Quant à la deuxième, en parallèle du chaos semé au sein de la banque, les hackers ukrainiens ont envoyé des messages au million de clients concernés pour leur indiquer que leurs coordonnées bancaires avaient été compromises. Cette opération a créé un mouvement de foule à grande échelle en Russie vers les distributeurs automatiques de billets et une saturation du service clients.

B. Le renforcement de la coopération entre les hackers et l'État

Les activités réalisées par les civils dans le cyberespace vont au-delà des cyberattaques sur des systèmes informatiques civils russes. Le hacktivisme sert également le renseignement militaire ukrainien : outre les informations récoltées par la récupération de diverses bases de données des citoyens russes, **les hackers récoltent du renseignement à but opérationnel** en ciblant les téléphones portables des soldats et de l'encadrement militaire russe sur le front. À titre d'exemple, l'accès aux caméras et aux microphones permet d'une part aux militaires ukrainiens d'estimer le volume de personnel et de matériel, ainsi que leur emplacement géographique. D'autre part, tant les militaires que les hacktivistes emploient l'intelligence artificielle (IA) afin d'identifier les propriétaires des appareils compromis et de mener par la suite des opérations psychologiques visant leur entourage. L'utilisation de l'IA a notamment joué un rôle important dans l'identification des bourreaux des massacres des civils ukrainiens à Boutcha, Irpin et Hostomel.

Par ailleurs, le SBU ne dissimule pas sa coopération avec les groupes de hackers pour mener des activités offensives sur les systèmes informatiques russes [9], comme dans le cas de la compromission des bases de données de la banque russe Alfa Bank. Enfin, il dispose d'une unité cyber déployée directement sur le front dont une partie des missions confiées ne diffère que peu des opérations réalisées par les hacktivistes. Cependant, d'autres ont pour objectif de mettre hors service le matériel militaire russe (drones, systèmes et réseaux utilisés, caméras de surveillance) et exigent d'être au plus près de l'adversaire [10]. Cette unité cyber est d'ailleurs appuyée par les cyber-volontaires civils, qui ont mis en place le système de récolte de renseignement en sources ouvertes *Griselda*. Celui-ci est principalement spécialisé dans l'optimisation du temps de traitement des données récoltées ainsi que dans l'automatisation de la transmission et de l'entrée de ces données grâce à des modules d'analyse automatique et des réseaux neuronaux. Ce système comporte également d'autres modules automatisés pour le décodage de messages radio, la récolte de données en ligne, etc.

II. Une transformation numérique fulgurante du ministère de la Défense

La transformation numérique du ministère de la Défense ukrainien a débuté à l'époque de la guerre dans le Donbass en 2014 avec la création de l'outil *Delta* par un groupe de volontaires civils. Cet outil, intégré au sein du ministère, a permis au commandement militaire ukrainien de bénéficier d'une supériorité informationnelle face à l'agresseur dès les premiers jours de l'invasion de l'Ukraine en février 2022. L'accélération de cette transformation numérique a également été permise grâce à un emploi massif de nouvelles technologies telles que les drones.

A. Delta : un outil numérique militaire de guerre en réseau info-centré

Après plusieurs réformes, le Ministère de la Défense a fondé en 2021 le *Centre des innovations et des technologies de la défense de l'Ukraine*, constituant l'une des sous-unité *d'Aérorozvidka*. À l'origine, *Aérorozvidka* est une formation de volontaires, ayant participé à la *Révolution de Dignité* [11], et qui ont souhaité réaliser en 2014 un projet permettant d'optimiser la connaissance situationnelle [12] des militaires ukrainiens sur le terrain. À cet effet, ces volontaires d'abord civils, puis militaires [13], ont conçu le système de connaissance situationnelle *Delta*.

Ce système prend la forme d'une carte géographique composée de plusieurs couches, disponible à partir d'un navigateur web sur n'importe quel support physique (smartphone, tablette, ordinateur). Cependant, *Delta* n'est pas uniquement une carte en ligne, mais un écosystème de services sécurisés dédiés aux militaires, permettant de faciliter certaines procédures. Ce système a donc contribué à la numérisation de l'armée ukrainienne dans son ensemble, notamment grâce à la suppression de plusieurs niveaux « bureaucratiques », comme l'a permis l'application *Diia* pour les citoyens ukrainiens. Établi sur la procédure « *Intelligence, Surveillance, Target Acquisition, Reconnaissance* » [14] (*ISTAR*), ce système de connaissance situationnelle est un instrument « multi-domaines » utilisé par la défense aérienne, les forces terrestres et navales. Le concept *ISTAR* représente la capacité à collecter des renseignements nécessaires à la planification et la conduite des opérations militaires par le biais de nombreux capteurs, du soldat au satellite.

Yaroslav Gonchar, le co-fondateur de l'unité *Aérorozvidka*, estime [15] que *Delta* a joué un rôle très important dans la défense de la capitale pendant l'offensive de Kyiv [16]. En plus de l'écosystème militaire [17], de très nombreux acteurs ont rejoint *Delta*, à savoir des structures telles que le ministère de l'Intérieur, la Garde nationale, les opérateurs de téléphonie mobile, la Défense territoriale, etc. Grâce à l'interconnexion de tous ces acteurs ainsi qu'aux mises à jour rapides des informations provenant du terrain, l'armée ukrainienne a pu réagir sans attendre les ordres de la hiérarchie, et compenser ainsi sa position de faiblesse. De plus, il assure que la connaissance situationnelle ne doit pas se limiter aux militaires, raison pour laquelle *Delta* intègre des informations provenant de sources très diverses. La population elle-même a été mobilisée grâce à la mise en place de chat-bots et d'autres points de contact sur Telegram (« *eVorog* », « *pravda_of_russia_bot* », « *krymbavovna_bot* ») permettant de

transmettre des renseignements d'intérêt militaire. Ces informations sont ensuite traitées et vérifiés par des centres de veille, qui les mettent à jour au sein du système *Delta*.

Le besoin croissant des structures militaires ukrainiennes en moyens permettant d'échanger d'importantes quantités d'information par des canaux sécurisés ainsi que de gagner en efficacité dans l'exécution des ordres, a donc été comblé par cet outil de guerre en réseau info-centré [18]. En outre, *Delta* a permis de renforcer l'objectivité des analyses par son évaluation systématique du niveau de fiabilité des informations et la réduction des erreurs d'interprétations potentielles. Ces caractéristiques ont notamment permis de rationnaliser l'utilisation des ressources matérielles et humaines disponibles, un usage qui se poursuit aujourd'hui. Quand bien même existe-il déjà des systèmes de connaissance situationnelle, *Delta* a fait ses preuves dans une guerre de haute intensité en temps réel et demeure un outil sans équivalent existant à l'OTAN puisqu'il est hébergé dans le Cloud [19]. Certes, même si « *le succès « dans la bataille » ne se transforme pas naturellement en succès « dans la guerre »* [20] » grâce aux technologies, celles-ci peuvent néanmoins permettre de gagner des batailles décisives.

Ukraine. Des opérateurs militaires de drones de la 22e brigade mécanisée
Ukraine. Des opérateurs militaires de drones de la 22e brigade mécanisée assemblent un drone de reconnaissance Poséidon sur leur position dans la région de Soumy, près de la frontière avec la Russie. Août 2024. Photo de Roman Pilipey pour AFP Photo
Roman Pilipey / AFP Photo

B. Intégration du cyber au complexe militaro-industriel de l'Ukraine

L'invasion de l'Ukraine a été l'occasion pour l'armée ukrainienne de développer des moyens de lutte asymétrique sur le champ de bataille, notamment par l'emploi massif de drones civils. Ceux-ci sont devenus indispensables du fait de la grande économie de munitions et d'hommes dans les missions offensives (largage de charges explosives et attaques kamikazes principalement), mais aussi de la possibilité de les employer comme capteurs pour le renseignement militaire. Les drones sont également intégrés comme capteurs à l'écosystème *Delta,* rendant des données récoltées accessibles rapidement aux forces armées. L'IA a de plus été mise à profit dans ce type de tâche pour automatiser partiellement le processus en détectant de façon autonome les éléments cartographiques.

Le caractère essentiel de ces appareils a fait émerger un écosystème complexe autour de l'industrie des drones en Ukraine composé d'acteurs étatiques, mais aussi en très grande partie de particuliers et d'entreprises civiles volontaires. Le rapport très étroit entre cette industrie, le complexe militaro-industriel et le secteur cybernétique a conduit à l'établissement d'une coopération entre le ministère de la Transformations numérique et le ministère de la Défense au sein du *Centre des innovations et des technologies de la défense de l'Ukraine*. En effet, le déploiement des drones nécessite plusieurs spécialistes relevant de la compétence de ces deux institutions. Aux côtés des opérateurs de drones, dont la formation peut-être relativement longue, et des spécialistes du génie, on trouve ainsi des développeurs et ingénieurs en informatiques pour la conception du *software* des drones ainsi que des ingénieurs en télécommunications et réseaux pour assurer tant les aspects liés au pilotage à distance qu'à la transmission de données.

Ce développement de la filière des drones répond par ailleurs à des problématiques sécuritaires et de souveraineté technologique critiques dans le cadre de la guerre contre la Russie. En effet, les drones civils les plus populaires en Ukraine sont de marques chinoises : *DJI* et *Mavic*. Cette préférence est due au fait qu'ils considérés comme très qualitatifs pour un coût particulièrement bas. Cependant, l'accessibilité des données des drones utilisés (géolocalisation, compte lié au drone, numéro de série, etc.) aux entreprises productrices, ainsi que la coopération du gouvernement chinois avec l'État russe, confirmée par la mise à disposition d'aéroscopes [21] ainsi que l'instauration d'une limite de nombre de drones vendus à l'Ukraine [22], a rendu nécessaire une réflexion sur l'architecture des systèmes informatiques utilisés et leur sécurité.

Enfin, le commandement militaire ukrainien fait également face à des problématiques liées aux moyens de guerre électronique de l'armée russe, qui dispose d'un arsenal d'outils réduisant l'efficacité des drones. Bien que l'armée russe ait drastiquement réduit l'utilisation de véhicules transportant des moyens de brouillage, à cause de la difficulté de les dissimuler, elle emploie efficacement des brouilleurs passifs, qui parviennent à passer sous les radars du renseignement radioélectronique [23]. L'une des solutions apportées mobilise là encore l'IA, qui permet d'atteindre la cible malgré le brouillage notamment grâce à une programmation préalable de la trajectoire du drone.

Malgré plusieurs obstacles évidents, la transformation technologique et numérique de l'armée ukrainienne a conduit à un gain notable d'efficacité lors des batailles. Elle a également eu d'autres effets : l'élargissement de la liste des acteurs impliqués dans la guerre et l'intégration rapide du domaine cyber à d'autres secteurs. L'armée elle-même est concernée bien au-delà des activités de hacking des unités cyber et des cyber-volontaires ou de la collecte de renseignement : le conflit l'a en effet poussée à renforcer drastiquement son utilisation d'un système développé au niveau national pour maximiser l'efficacité de l'ensemble de ses composantes.

*

Malgré des limites dues à un manque d'attention au sujet de certaines failles dénoncées par la société civile, **le domaine cyber est ainsi devenu un élément indispensable pour la lutte de l'État ukrainien contre la Russie**. L'utilisation d'outils comme *Delta* couplée à la massification de l'emploi massif des drones civils dans une guerre de haute intensité, dont la

survenance n'avait pendant longtemps plus été envisagée par les experts militaires [24], pourraient être à l'origine de profonds changements de procédés de guerre des doctrines militaires de l'OTAN.

Par ailleurs, la spécificité de la situation ukrainienne réside en grande partie dans le poids du volontariat, qui est pleinement intégré à l'écosystème cyber. Les volontaires aident l'État ukrainien tant à se défendre qu'à attaquer, et ont également permis de considérables avancées techniques au sein du ministère de la Défense de l'Ukraine. Une multiplicité d'acteurs (citoyens, organismes privés, etc.) agit à travers le cyberespace et demeure impliquée dans la guerre à des degrés importants, ce qui justifie la qualification de « première cyberguerre mondiale » et le passage à une économie de guerre cyber.

L'implication d'une multitude d'acteurs civils soulève néanmoins de nombreuses questions juridiques, notamment concernant la sécurité internationale, auxquelles les juristes peinent à répondre à ce jour. La cyber-guerre entre l'Ukraine et la Russie démontre que chaque personne disposant d'outils nécessaires peut agir par le biais du cyberespace, ce qui en fait autant de potentielles parties prenantes sur lesquels un État peut compter que des cibles potentielles pour l'État adverse. Un enjeu essentiel pour la communauté internationale est donc plus que jamais l'établissement d'un cadre légal pour adapter le droit des conflits à ces nouvelles réalités.

P.-S.

Anastasia Kryvetska est spécialisée dans la géopolitique de l'Ukraine et de la Russie. Ses recherches portent sur les acteurs et les problématiques relatives au domaine du cyberespace ukrainien et russe, ainsi que sur le déploiement des nouvelles technologies sur le front en Ukraine

---

Notes

[1] Observée depuis 2014 : *Comment l'écosystème cyber ukrainien s'est-il adapté à la guerre ?* https://www.diploweb.com/Comment-l-ecosysteme-cyber-ukrainien-s-est-il-adapte-a-la-guerre.html.

[2] Espace informationnel compris.

[3] https://twitter.com/FedorovMykhailo/status/1497642156076511233?lang=fr

[4] Cf. *Comment l'écosystème cyber ukrainien s'est-il adapté à la guerre ?* https://www.diploweb.com/Comment-l-ecosysteme-cyber-ukrainien-s-est-il-adapte-a-la-guerre.html.

[5] https://itc.ua/ua/novini/rada-dozvolila-zaluchati-nezalezhnih-it-fahivcziv-do-testuvannya-vrazlivostej-derzhavnih-informaczijnih-sistem/

[6] Terme utilisé par Mykhaïlo Fedorov, ministre de la transformation numérique de l'Ukraine, *www.facebook.com*, https://www.facebook.com/mykhailofedorov.com.ua/posts/1007320006552185/.

[7] https://therecord.media/hacktivists-respond-to-red-cross-rules-with-ridicule

[8] https://www.youtube.com/watch?v=KSAjuZ6WDSg

[9] https://fakty.com.ua/ru/ukraine/20231020-sbu-ta-hakery-zlyly-kliyentsku-bazu-rosijskogo-alfa-banku/

[10] https://focus.ua/uk/digital/590675-hakeri-sbu-zlamuyut-tehniku-rosiyan-prosto-na-fronti-yak-ce-dopomagaye-v-nastupi-bbc

[11] « *Revolutsiya gidnosti* » (« *Революція гідності* ») : terme utilisé pour désigner le Révolution de Maïdan de 2013-2014.

[12] Terme américain « Situation awareness ». Il s'agit de l'ensemble d'éléments dont disposent des dirigeants permettant la connaissance de l'ennemi sur un champ de guerre.

[13] *Aérorozvidka* a été intégrée en 2015 au ministère de la Défense en tant qu'unité « *A2724* » (ou « *Centre de mise en œuvre et de soutien des systèmes automatisés de gestion opérationnelle* »), avant d'être dissoute au début de l'an 2020 et de nouveau réhabilitée en mars 2021.

[14] « Renseignement, surveillance, acquisition d'objectifs et reconnaissance ». Poirot, J. ISTAR. In *Dictionnaire du renseignement* ; Perrin, 2018 ; pp 487–488.

[15] https://focus.ua/digital/514225-aytishniki-protiv-okkupantov-kak-sistema-delta-pomogla-vsu-zashchitit-kiev

[16] Désigne l'offensive russe sur la capitale ukrainienne débutée le 25 février 2022 et qui s'est achevée le 2 avril 2022 par la reprise du contrôle de Kyiv par les forces armées ukrainiennes.

[17] Entendre au sens de : ministère de la Défense, SBU, Douanes, GUR.

[18] Le combat en réseau info-centré est une doctrine militaire américaine, utilisée pour la première fois par le ministère de la Défense américain sur le terrain de la guerre en Irak. Également « guerre réseau-centrée ». La *Network Centric Warfare* est l'adaptation du domaine militaire aux changements liés à l'expansion de l'ère de l'information, qui désigne une période historique marquant le passage de l'industrie traditionnelle à une économie principalement basée sur la technologie de l'information.
Castells, M. *The Rise of the Network Society* ; The information age : economy, society, and culture ; Wiley-Blackwell : Chichester, West Sussex ; Malden, MA, 2010.

[19] « […] il s'agit essentiellement d'un terme utilisé pour décrire un réseau global de

serveurs ayant chacun une fonction unique. Le cloud n'est pas une entité physique, mais un vaste réseau de serveurs distants éparpillés tout autour de la planète, reliés entre eux, et destinés à fonctionner comme un écosystème unique. Ces serveurs sont conçus pour stocker et gérer des données, exécuter des applications, ou fournir du contenu ou des services […]. Au lieu d'accéder à des fichiers et données stockés sur un ordinateur local ou personnel, vous accédez à ces ressources en ligne à partir de n'importe quel appareil compatible avec Internet : les informations sont disponibles en tout lieu et en tout temps. », Microsoft.

[20] Desportes, V. Que Sera La Guerre Aux XXIème Siècle ? *Conflits* 2018.

[21] https://zorinadii.org.ua/aerial-reconnaissance-and-civil-drone/

[22] https://suspilne.media/584155-nyt-zsu-ne-vistacae-desevih-droniv-cerez-obmezenna-kitau/

[23] https://www.radiosvoboda.org/a/drony-reb-radioelektronna-borotba-dji-mavic-fpv/32407188.html

[24] Zajec, O. Stratégies Militaires : La Fin de l'hémiplégie Doctrinale ? *Conflits* 2018.