L'EMPLOI DE LA CYBER-ELECTRONIQUE EN UKRAINE

La qualité des commentaires et des questions suscités lors de l'audition du général de division Aymeric Bonnemaison, COMCYBER, par la Commission de la défense nationale et des forces armées le 7 décembre 2022 puis lors de sa conférence de presse le 12 janvier dernier, illustrent l'intérêt mêlé d'inquiétude qu'une société toujours plus digitalisée et cyberdépendante porte à un domaine à la fois riche de promesses et de menaces.

L'article « *Jusqu'à quand pourra-t-on éviter une cyber-catastrophe* ? » paru dans le Figaro du 7 février n'est pas sans rappeler l'avertissement du secrétaire d'État américain à la Défense Léon Panetta en 2012 lorsqu'il parlait de « Cyber Pearl Harbor »[i] en égrenant des scénarios semblables. Suite aux « faits d'armes » cybernétiques de la Russie, notamment contre l'Estonie et la Géorgie, nombreux étaient ceux qui pensaient que l'Ukraine allait succomber sous les attaques des hackers russes, qu'ils soient corsaires ou pirates. Il s'avère que la « cyber blitzkrieg » n'a pas eu lieu du fait d'une défense en profondeur ukrainienne particulièrement efficiente. Toutefois, il n'est pas interdit de penser que la Russie n'a pas mis en œuvre tout son arsenal cybernétique et qu'elle pourrait réserver des surprises stratégiques à l'Ukraine, mais aussi à ses alliés.

En 1992, le général Monchal, alors chef d'état-major de l'armée de Terre, déclarait « *à l'avenir, le maître de l'électron, l'emportera sur le maître du feu* ». Force est de constater qu'en Ukraine, le maître du feu ne le cède pas au maître de l'électron et que, si dans la guerre 2.0 l'information – sous toutes ses formes, est une arme, c'est le plus souvent le feu qui est décisif.

Drones kamikazes ukrainiens FPV armés d'ogives PG-7V de 85 mm — Photo Résistance ukrainienne

Il n'en reste pas moins que les actions cinétiques sont appuyées par des actions cyber-électroniques pour atteindre des objectifs stratégiques, opératifs ou tactiques ; qu'il y a une réelle complémentarité entre cyber et guerre électronique ; que l'emploi massif de téléphones portables équipés d'applications innovantes, de drones et de munitions « intelligentes » pourrait sinon transfigurer le champ de bataille numérique au moins modifier les doctrines en matière de commandement, de contrôle et d'acquisition du renseignement.

Les informations diffusées par le COMCYBER, notamment celles figurant dans le compte-rendu de son audition, décrivent avec suffisamment de précision et de concision le contexte et les opérations menées par les belligérants. L'objet du présent document n'est donc pas de faire l'exégèse de ses propos mais, à partir de l'exploitation d'informations ouvertes – notamment anglo-saxonnes, de proposer quelques pistes supplémentaires de réflexion sur l'emploi de la cyber-électronique en Ukraine.

****

1. De la cyber-électronique

« *Depuis une décennie, le retour d'une guerre majeure structure la pensée des puissances militaires de premier ordre. Pour vaincre, il faudra dans une logique stratégique classique produire des effets décisifs par la manœuvre. Toutefois, celle-ci devra s'accommoder de deux variables : la maîtrise opérationnelle du second âge des technologies numériques (IA, robotique, etc.) et la capacité à outrepasser les nouvelles formes d'attrition résultant de la multiplication des capacités adverses de déni d'accès et d'actions indirectes dans la profondeur. Une refonte doctrinale au sein des grandes puissances est donc en cours, avec en tête les États-Unis et la Russie, pour déterminer les voies et moyens nécessaires à la restauration de la liberté d'action. (…)*

Big Data — Photo BS © Gary Killian

Les doctrines russes et américaines des opérations futures convergent sur la nature de la manœuvre envisagée, qui devra être une ***synergie des domaines****. Afin d'outrepasser les capacités de déni d'accès (Anti-Access/Area Denial) sans cesse renforcées par les progrès technologiques, il faut parvenir à fonder des dilemmes opérationnels à l'adversaire, saturant ses capacités de réaction par l'intégration des domaines de lutte dans la profondeur. Toutefois, dans un contexte stratégique d'affrontement majeur, la variable nucléaire demeure structurante, ce qui fait qu'en réalité ces opérations en synergie font prendre en considération un retour de la « guerre limitée », puisqu'il s'agit d'obtenir des effets tout en contenant les risques d'escalade pour ne pas atteindre le seuil nucléaire. (…)*
À cette vision doctrinale, répond un plan capacitaire semblable pour ces deux États dans l'usage des technologies de la deuxième génération du numérique. Dans ce cadre, une ***cybernétisation générale*** *de l'action est envisagée (IA, systèmes autonomes, communications globales) ainsi qu'un développement des moyens d'action en profondeur (allongement des portées des tirs indirects, durcissement des moyens de projection).* »[ii]

La Russie avait mis en pratique tout ou partie de ces principes, avec succès, en Géorgie en 2008 puis dans le Donbass en 2014. De l'application de ceux-ci nous retiendrons en particulier la convergence entre les actions dans le cyberespace et celles conduites dans le spectre électromagnétique, ce que l'armée de terre américaine exprime dans son concept d' « activités cyber-électroniques ».
" Les activités cyber-électromagnétiques (Cyber Electro Magnetic Activities) sont des activités mises en œuvre pour saisir, conserver et exploiter un avantage sur les adversaires et les ennemis dans le cyberespace et le spectre électromagnétique, tout en dégradant et en leur interdisant l'accès à ceux-ci et en protégeant notre propre système de commandement. La CEMA comprend les opérations dans le cyberespace, la guerre électronique et les opérations de gestion du spectre "[iii]

Cette définition peut s'appliquer aux deux belligérants actuels car, si les armées soviétiques disposaient, jusqu'au plus bas niveau tactique, d'une large palette de moyens de guerre électronique, il apparaît que les forces en présence aujourd'hui en possèdent tout autant.
« *À partir de 2014, alors que les pays de l'OTAN avaient délaissé leurs capacités de guerre électronique (GE), ils ont pris conscience, que d'autres pays comme la Russie avaient développé les leurs. Moscou en a fait un atout majeur d'une nouvelle forme de guerre à laquelle nos pays ne semblent plus préparés. (…) L'emploi de la guerre électronique russe en appui des forces séparatistes a surpris non seulement l'armée ukrainienne mais aussi les observateurs occidentaux. La GE russe a apporté les contributions suivantes :*

- *protection des forces amies en leurrant les missiles, en brouillant les systèmes de guidage ou en causant l'explosion prématurée des munitions ;*
- *acquisition d'objectifs en localisant les postes de commandement adverses ;*
- *brouillage des communications de l'ennemi pour le fixer avant les frappes d'artillerie ;*
- *perturbation des moyens de navigation comme le GPS ;*
- *brouillage des liaisons des drones pour empêcher leur emploi ;*
- *appui aux opérations d'information, notamment par la diffusion de SMS personnalisés afin de déstabiliser leurs adversaires ou de les inciter à émettre pour révéler leur position.* » [iv]

« *De la mi-2014 au début de l'année 2015, troupes russes et ukrainiennes s'affrontèrent dans le Donbass, et les secondes subirent plusieurs sévères défaites. L'une des clés des succès russes reposait sur la supériorité initiale de leur complexe "reconnaissance-frappe", soit l'association entre drones de reconnaissances, moyens de guerre électronique et de communication et batteries d'artillerie. Ce complexe leur permit de noyer sous des déluges de feu les positions ou les unités ennemies dans les quinze minutes suivant leur détection, avec pour conséquence que 80 % des pertes ukrainiennes durant la période furent le fait de l'artillerie russe. »*[v]

Ces constats valent pour aujourd'hui.

Enfin, et ainsi que le souligne le général Bonnemaison, « *les Russes ont, de longue date intégré la manœuvre cyber et la manœuvre informationnelle, en liant fortement les deux dans leur action. Ils couvrent aussi bien le contenu que le contenant dans leur approche* »[vi]

Le chercheur britannique Keir Giles donne ici une définition beaucoup plus exhaustive du concept de « guerre de l'information » :
« *Pour la Russie, la " confrontation informationnelle " ou " guerre de l'information " est un concept large et inclusif qui couvre un vaste éventail d'activités différentes. Il couvre les activités hostiles utilisant l'information comme un outil, ou une cible, ou un domaine d'opérations. Par conséquent, ce concept englobe les opérations sur les réseaux informatiques ainsi que des disciplines telles que les opérations psychologiques, les communications stratégiques, l'influence, le renseignement, le contre-espionnage, la "maskirovka", la désinformation, la guerre électronique, l'affaiblissement des communications, la dégradation des aides à la navigation, la pression psychologique et la destruction des capacités informatiques de l'ennemi. Pris dans sa globalité cela forme un ensemble de systèmes, de méthodes et de tâches visant à influencer la perception et le comportement de l'ennemi, de la population et de la communauté internationale à tous les niveaux.* » [vii]

2. De l'emploi de la cyberguerre

Toutefois, si l'emploi des armes cyber-électroniques a densifié le brouillard de la guerre hybride que mènent les armées russes en Ukraine depuis un an, il n'a pas été aussi épais qu'elles l'auraient souhaité. En effet, s'il est possible d'analyser les conséquences des diverses cyber-actions menées avant le déclenchement des hostilités, il est difficile d'en mesurer leur efficacité réelle depuis le début de l'offensive – tant pour la destruction d'objectifs que pour la qualité de leur appui d'ensemble.

« *Bien que la cyberguerre ait été une partie importante et âprement disputée d'un conflit qui a servi de terrain d'essai pour cette forme de bataille encore inédite, elle ne semble pas avoir été l'application tueuse, pour ainsi dire, que certains attendaient*. »[viii]

« *Nous militaires, tendons à attribuer à la cyberguerre un rôle majeur dans les conflits du futur. Or, dans ce conflit-là, le cyber n'a pas tout fait, malgré la domination russe initiale. Quand la poudre parle, la lutte informatique offensive trouve ses limites. Dans la phase préparatoire de la guerre comme dans sa phase intensive, les actions de sabotage cyber ont été atténuées au profit d'une guerre classique bien plus létale, cinétique et brutale. On peut être tenté de développer une vision un peu romantique selon laquelle tout se fera à l'avenir dans un monde virtuel, mais la réalité est qu'il est nécessaire de prendre en compte tous les aspects d'un conflit*. »[ix]

Plusieurs explications sont données à ce qui apparaît comme une contre-performance des forces armées russes.[x]

a. La surestimation des capacités des armées russes et la sous-évaluation de la difficulté à conduire la guerre dans l'éther

En 2017, Nicolas Mazzuchi s'interrogeait déjà sur le potentiel réel de la Russie dans le domaine cyber :

« *Comment ce pays qui semblait, il y a peu, loin du niveau des Etats-Unis et de la Chine serait-il devenu en quelques années le principal cyber agresseur mondial ? Cette vision d'un éveil du cyber-ours russe, utilisant le Net pour mener des actions à visée géopolitique, doit être mise en balance avec la réalité des potentiels techniques et économiques nationaux autant qu'avec les visées stratégiques d'un pays dont les priorités demeurent orientées vers son « étranger proche (…)* »

et plus loin

« *Les hackers russes apparaissaient, avant 2013-2014, comme étant d'un bon niveau, mais incapables d'atteindre la masse critique nécessaire à la formation d'un bloc unifié et organisé, brique de base d'une force cyber respectable. Que s'est-il donc passé en l'espace de quelques années pour arriver à un tel renversement, suscitant des craintes parfois exagérées pendant les élections présidentielles américaines et françaises ou au moment du référendum britannique sur le Brexit ?* »[xi]

« *La plupart des attaques (2022) ont été attribuées par des sources ukrainiennes et occidentales à des entités gouvernementales russes - principalement le GRU, le service de renseignement militaire russe, qui a l'habitude de recourir à des cyberattaques perturbatrices. Dans quelques cas, des groupes mandataires (tels que le principal groupe de ransomware Conti) ont également été impliqués, et il a été signalé qu'un groupe de pirates brésiliens soutenant la Russie a attaqué des universités ukrainiennes. Tous ces initiatives de piratage, qu'elles soient le fait du GRU ou non, semblent avoir été mal coordonnées avec les actions militaires russes en Ukraine.* »[xii]

« *Certains espions occidentaux disent donc que la guerre révèle le gouffre qu'il existe entre la compétence américaine et russe dans les cyber-opérations de haut niveau contre le matériel militaire. Mais d'autres avertissent qu'il est trop tôt pour tirer des conclusions catégoriques. La cyber-campagne de la Russie a peut-être été limitée moins par son incapacité que par l'orgueil démesuré qui a également affecté ses forces armées conventionnelles.* »[xiii]

Ainsi la Russie aurait pêché à la fois par orgueil et par excès d'optimisme en ses compétences, ce qui l'aurait amené à sous-évaluer les capacités de résistance de son adversaire et, partant, à négliger la planification d'un plan élaboré de cyber-attaques d'envergure, vorace en temps de préparation et en mobilisation de ressources.

La conduite et la coordination d'actions tactiques combinées sur terre et dans le cyberespace se révèle être particulièrement complexe, notamment lorsqu'il y a friction.

« *Faire coïncider la vitesse des lignes d'opérations dans le cyberespace avec celle du terrain est une gageure. Or, dans le plan russe, la foudroyance de l'action conventionnelle – quelques jours pour faire tomber Kiev – devait permettre aux forces terrestres de capitaliser sur les effets générés dans le cyberespace. Ainsi, au 24 février, les principaux objectifs géographiques russes voient leur degré de connectivité baisser. C'est également à ce moment que le malware/wiper AcidRain paralyse les modems du réseau de communication satellitaire Viasat, utilisé notamment par les armées ukrainiennes. Cependant, la lenteur de la progression terrestre ne permettra pas de capitaliser convenablement sur cet avantage et permettra aux forces ukrainiennes de trouver des solutions palliatives, de rétablir une connectivité suffisante et d'empêcher le black-out.* »[xiv]

« *Les responsables américains, européens et ukrainiens affirment tous qu'il existe de nombreux exemples de cyber-attaques russes synchronisées avec des attaques physiques, ce qui suggère un certain degré de coordination entre les deux secteurs. Mais il y a aussi eu des maladresses. Dans certains cas, les frappes cinétiques ont mis hors service les mêmes réseaux que les cyber-forces russes tentaient d'infecter - obligeant paradoxalement les Ukrainiens à revenir à des moyens de communication plus sûrs.* »[xv]

« *L'incapacité (jusqu'à présent) à perturber les opérations, la logistique et les communications ukrainiennes reflète probablement la nature désordonnée de la planification russe, des prévisions erronées sur l'accueil que recevraient leurs troupes et la force des cyberdéfenses ukrainiennes.* »[xvi]

La même remarque s'applique aux actions de guerre électronique offensive, certes efficaces contre les drones ukrainiens et les *smartphones*, mais pour lesquelles on a pu observer de nombreux cas de brouillages fratricides (dans les deux camps d'ailleurs) du fait de l'imbrication d'unités fortement numérisées, que ce soit avec du matériel militaire ou civil, et dépendantes du même spectre électromagnétique.

« *Alors que les troupes russes auraient également utilisé des téléphones portables et même volé des cartes SIM, ce qui signifie qu'ils sont probablement dépendants de l'infrastructure de communication ukrainienne, donc qu'ils ne disposent pas de leurs propres moyens de communication, résilients ou redondants.*
Par conséquent, une autre explication possible est que les Russes n'utilisent pas de brouilleurs pour ne pas perturber leurs communications sur le champ de bataille, car même si le brouillage peut être efficace contre les communications ennemies, il peut également interférer avec les communications amies s'il n'est pas effectué correctement, ce qui indique que les forces russes n'ont pas de tactiques appropriées pour mener la guerre dans le domaine du spectre électromagnétique, qui nécessite une gestion rigoureuse.
Cela a été observé non seulement pour les réseaux de communication, mais aussi pour les signaux de navigation par satellite où les forces armées russes ont été confrontés à un "fratricide électronique" à cause de leurs actions de brouillage.»[xvii]

Cette observation vaut pour les équipements de GE dont sont dotés certains aéronefs.

« (…) *le fratricide est un problème systémique russe. Par exemple, le pod GE Khibiny, monté sur un certain nombre d'avions, détecte automatiquement les radars et les perturbe. Malheureusement pour eux, il a tendance à faire de même avec les autres avions. Les tandems d'avions d'attaque russes équipés de ce système ont donc dû choisir entre un radar fonctionnel et une protection contre la GE. Ils ont souvent reçu l'ordre de donner la priorité à leur radar. (...)* »[xviii]
Par ailleurs les écoutes et la localisation font peser une menace permanente.

« *Les écoutes électroniques étaient omniprésentes sur la ligne de front au Donbass, et les unités ukrainiennes et séparatistes/russes utilisaient les équipements appropriés. Les talkies-walkies, les téléphones portables et même les stations de radio étaient surveillés, et les chefs avaient tendance à discuter des questions importantes en personne lorsque cela était possible*.» [xix]

« *Les communications russes étaient insuffisamment sécurisées (...) Alors que les forces spéciales russes avaient accès à des équipements de communication tactiques sophistiqués utilisant un système de chiffrement performant (à en juger par les opérations précédentes en Ukraine), ces équipements étaient en nombre insuffisant pour les autres unités lors de cette invasion. Certaines unités russes ont employé des équipements chinois de grande diffusion insuffisamment sécurisés. D'autres se sont appuyées sur l'infrastructure civile. Cette dépendance crée deux difficultés majeures. Premièrement, lorsque les Russes ont détruit l'infrastructure de télécommunications ukrainienne, par inadvertance ou intentionnellement, cela a entravé leurs propres communications. Deuxièmement, le fait de s'appuyer sur le système de communication d'un adversaire a pour conséquence de faciliter les écoutes. Nombreux sont ceux qui supposent que l'une des raisons du taux élevé de pertes parmi les officiers supérieurs russes était que les moyens de communication qu'ils utilisaient permettaient de les localiser*.»[xx]

Enfin, des cyber-attaques majeures auraient pu avoir pour effet de neutraliser des infrastructures ou de détruire des bases de données que les Russes pensaient pouvoir utiliser à brève échéance.

« *Les responsables occidentaux affirment que la Russie n'a pas réussi à planifier et à lancer des cyberattaques hautement destructrices sur les réseaux électriques, l'énergie et les transports, non pas parce qu'elle en était incapable, mais parce qu'elle supposait qu'elle occuperait bientôt l'Ukraine et prendrait possession de ces infrastructures. Pourquoi détruire ce dont vous aurez bientôt besoin ? Lorsque la guerre s'est prolongée, la Russie a dû s'adapter. Mais les cyber-armes ne sont pas comme les armes physiques qu'il suffit de réorienter vers une autre cible et les réapprovisionner en munitions. Elles doivent au contraire être adaptées à chaque cible.* »[xxi]

En décembre 2022, Jon Bateman tirait les leçons suivantes des opérations de cyberguerre russes :

a. « *Les "feux" cybernétiques russes (attaques perturbatrices ou destructrices) ont sans doute appuyé modestement les opérations au début de l'invasion, mais depuis, ils n'ont infligé que des dommages négligeables aux cibles ukrainiennes.*
b. *Les cyber-feux n'ont rien ajouté de significatif à la puissance de feu cinétique de la Russie ni rempli des missions distinctes de celles des armes cinétiques. Plutôt que de jouer un rôle spécifique, de nombreux cyber-feux russes ont visé les mêmes catégories de systèmes ukrainiens que les armes cinétiques, à savoir les infrastructures de communication, d'énergie et de transport. Pour presque toutes ces catégories de cibles, les feux cinétiques semblent avoir causé des dommages bien supérieurs*.
c. *La collecte de renseignements - et non les feux - a probablement été le principal objectif des cyber-opérations russes, mais cela n'a pas non plus donné beaucoup d'avantages militaires.*
d. *Si de nombreux facteurs ont limité l'efficacité cybernétique de Moscou, les plus importants sont peut-être l'insuffisance de la capacité cybernétique russe, les faiblesses des institutions non cybernétiques de la Russie et les efforts défensifs exceptionnels de l'Ukraine et de ses partenaires*.» [xxii]

b L'efficacité de la défense cybernétique ukrainienne

« *Réputée pour ses formations d'ingénieurs, l'Ukraine était devenue ces dernières décennies l'une des places fortes de l'informatique offshore mondiale. Certains y voyaient la capitale européenne du métier, rebaptisée « near-shore » compte tenu de la proximité culturelle et horaire avec les clients finaux.*
(…) Le pays emploie des dizaines de milliers d'informaticiens pour le compte d'entreprises de services elles-mêmes mandatées par des groupes comme Deutsche Bank, IBM ou l'opérateur télécoms international Lebara. »[xxiii]

L’invasion de 2014 et la qualité des cyber-attaques russes avaient conduit l’Ukraine à renforcer la protection de ses systèmes informatiques, à développer des plans de sauvegarde des données en développant le *cloud computing* et en généralisant la dispersion des données sensibles, en particulier hors des frontières.
Entre 2014 et 2022, l’Ukraine a mis en place une solide politique en matière de cyberdéfense.

« *L'Ukraine a publié une stratégie nationale de cybersécurité en 2016 et a défini un niveau de redondance et de résilience pour les données, et a généralisé l'utilisation du chiffrement avant l'invasion. Elle a mis en œuvre certaines mesures élémentaires de cyber « hygiène » après 2015. La cyber-hygiène avant une attaque est importante, mais l'élément primordial de la défense est la capacité d'identifier et de réagir rapidement.*
L'Ukraine (avec une assistance extérieure) a entrepris de surveiller en temps réel les réseaux et systèmes critiques afin de détecter rapidement les intrusions, puis d'agir sans tarder pour les contrer (...) L'Ukraine aurait fait appel à des tierces parties pour héberger certaines données et services en dehors des limites géographiques du conflit. Cela n'a fait que compliquer et contraindre la planification russe. »[xxiv]

Balle clef-USB — Photo BS Sasha85ru

Les services ukrainiens ont joué le rôle principal dans la défense, mais les seuls moyens nationaux ne seraient pas parvenus à contenir les 4.500 cyber-attaques[xxv] dont ils ont été victimes. L'Ukraine disposait d'un réseau de partenaires (gouvernements et entreprises) qui ont pu fournir une formation et une assistance, y compris la surveillance à distance et les moyens pour réduire les conséquences des attaques, avant et après l'invasion.

« *L’arrivée des Américains chargés de détecter d’éventuels logiciels prépositionnés a été capitale au cours des semaines précédant le conflit. En deux semaines, leur mission est devenue l’un des plus grands déploiements du Cyber Command américain, mobilisant plus de quarante personnes des services armés américains. Ils étaient aux premières loges lorsque la Russie a intensifié ses opérations dans le cyberespace, en janvier, éprouvant les systèmes ukrainiens de façon inédite. Ces équipes se sont engagées dans une mission de hunting forward, qui consiste à arpenter les réseaux informatiques des partenaires à la recherche de signes de prépositionnement.* » [xxvi]

Général Aymeric Bonnemaison, COMCYBER — Photo Ministère des Armées

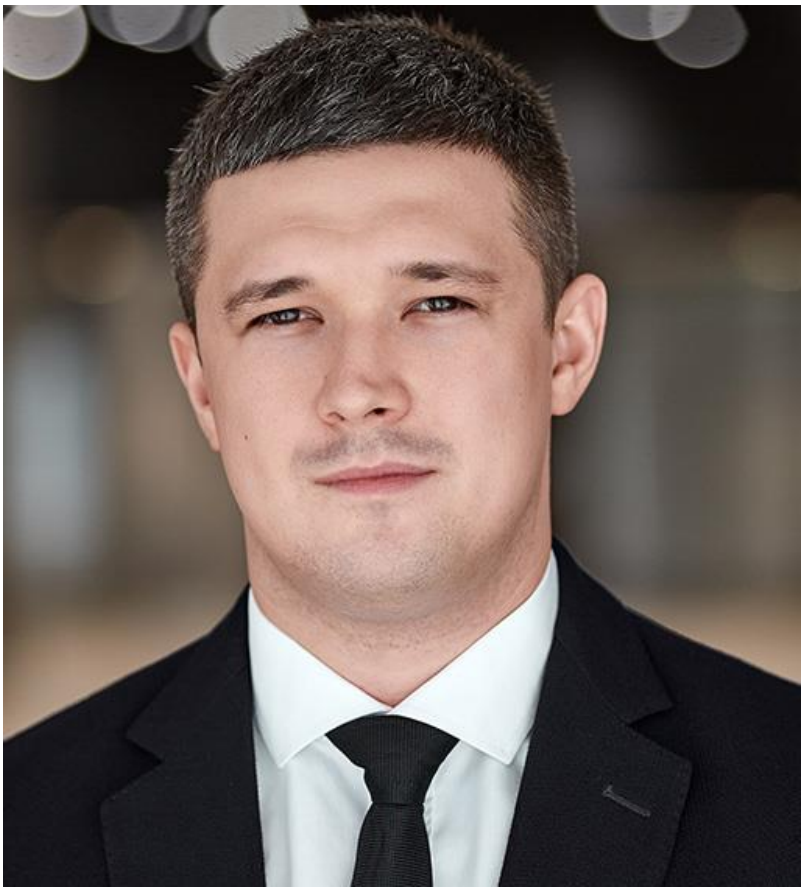
Les entreprises de la tech ont fourni une aide précieuse. Une action collective mêlant national et étranger, gouvernemental et privé, a donné à l'Ukraine un avantage en matière de surveillance et de réaction rapide pour bloquer les attaques et réparer ou éliminer les vulnérabilités.

« *L'aide occidentale a également été cruciale. En prélude à la guerre, l'OTAN a notamment renforcé sa coopération avec l'Ukraine en lui donnant accès à sa bibliothèque de cybermenaces, un répertoire de logiciels malveillants connus. La Grande-Bretagne a fourni un soutien de 6 millions de livres (7,3 millions de dollars), y compris des pare-feu pour bloquer les attaques et des moyens d'analyse technique des intrusions. La coopération était réciproque. "Il est probable que les Ukrainiens ont enseigné aux États-Unis et au Royaume-Uni plus de choses sur les cyber-tactiques russes qu'ils n'en ont appris d'eux", note Marcus Willett, ancien responsable des questions de cybercriminalité au sein du Government Communications Headquarters (GCHQ). La capacité de résilience de l'Ukraine a paradoxalement été confortée par la nature primitive de nombre de ses systèmes de contrôle industriel, hérités de l'époque soviétique et non encore modernisés.*

Les entreprises privées de cybersécurité ont également joué un rôle de premier plan. M. Zhora (chef de l'agence ukrainienne de cyber-sécurité défensive) considère que Microsoft et ESET, une entreprise slovaque, occupent une place de premier plan du fait de leur forte présence sur les réseaux ukrainiens et de la "télémétrie", ou données réseau, qu'elles y collectent.
Microsoft affirme que l'intelligence artificielle, qui analyse les codes plus rapidement qu'un être humain, a facilité la détection des attaques. Le 3 novembre, Brad Smith, le président de Microsoft, a annoncé que sa firme étendrait gratuitement son assistance technique à l'Ukraine jusqu'à la fin de 2023.
Cette promesse a porté à plus de 400 millions de dollars le soutien apporté par Microsoft à l'Ukraine depuis février. »[xxvii]

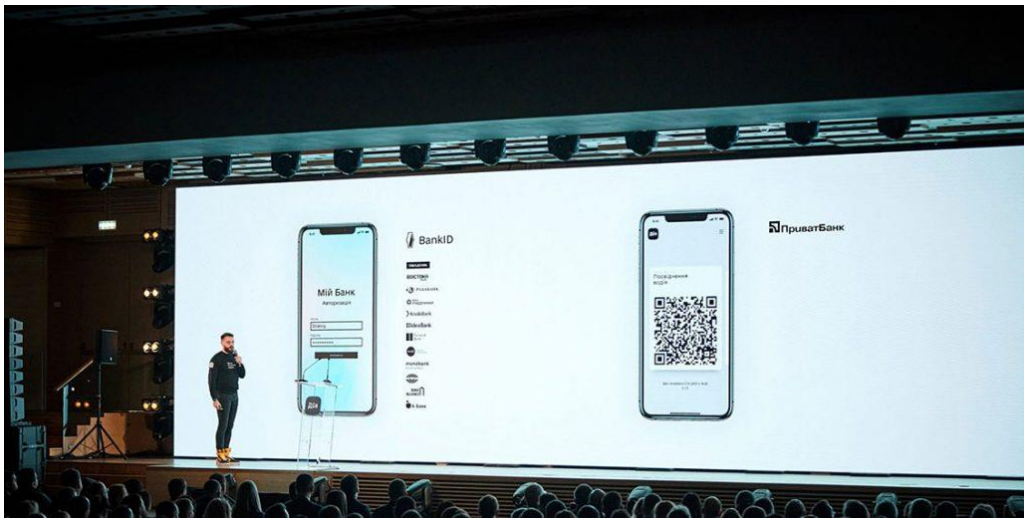
3. L'information est une arme, le smartphone en est le vecteur

Depuis sa nomination comme ministre de la transformation numérique en 2019, Mykhailo Fedorov a eu pour ambition de faire de l'Ukraine un champion mondial du numérique (« a *digital country* »)[xxviii] en lançant un ambitieux plan de digitalisation nationale grâce à une offre numérique de services publics appelés Diia. L'application mobile, qui permet d'accéder, entre autres, à 14 documents numériques (carte d'identité, passeport, permis, …) avait été téléchargée par plus de 18 millions d'Ukrainiens en décembre 2022.



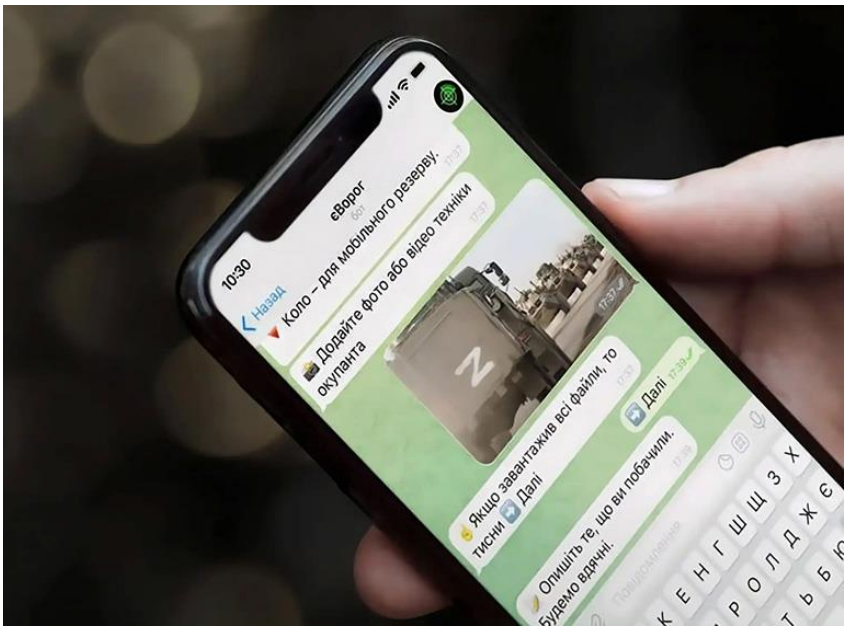
Mykhailo Fedorov — Photo Dubetskyi-Ph

Il semblerait que cette plateforme et ses applications aient bien résisté aux cyber-attaques russes et qu'elles aient permis d'assurer la continuité des service publics[xxix] car la connectivité avait pu être maintenue grâce à la mise à disposition par Elon Musk (à titre gracieux) du service satellitaire Starlink beaucoup plus résistant au brouillage que Viasat.



Présentation du portail et de l'application mobile Diia — Photo Anton Filonenko

Depuis le 24 février 2022, Diia a trouvé un usage hybride en hébergeant l'application Delta rapidement mise au point grâce à l'inventivité et à la détermination des développeurs civils et militaires ukrainiens. En conformité avec les standards techniques de l'OTAN[xxx], Delta fournit une image détaillée de l'espace de bataille et permet aux utilisateurs d'identifier les amis et les ennemis, de connaître l'emplacement et le type d'objets particuliers.

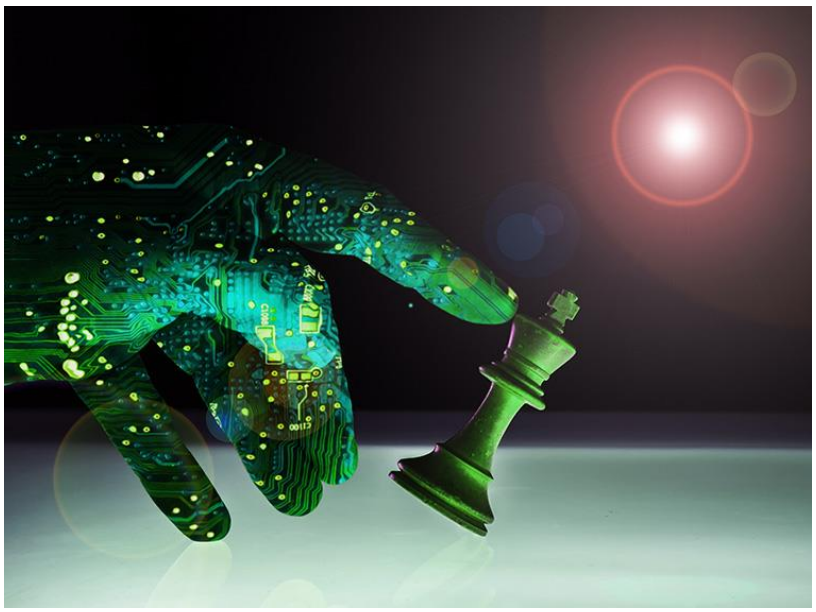


« **Y a ennemi » *(ieVorog)* : Quand un chatbot aide les forces armées ukrainiennes** » – DeskRussie: **gorozhanin.info**

« *On peut signaler où est l'ennemi grâce à l'application Diia » explique ainsi Mykhailo Fedorov, ajoutant qu'« un chatbot, s'appuyant sur la géolocalisation, a été créé pour aider les citoyens à connaître l'emplacement des troupes ennemies*. » [xxxi]
Les troupes Russes cherchent à s'emparer de ces téléphones riches en informations personnelles et persécutent ceux qui utilisent l'application.

Les Ukrainiens sont fiers de leur « adaptabilité réactive » et font confiance au « maître de l'électron » pour les aider à gagner les futures batailles.

« *La guerre actuelle de la Russie contre l'Ukraine est considérée comme une guerre réseau-centrée - le type de conflit militaire dans lequel l'une des parties prend le dessus non pas en raison de la supériorité de ses forces et de ses moyens de combat, mais grâce à la possession plus avantageuse d'informations. Comme l'a indiqué l'ONG Aerorozvidka, "l'un des principaux concepts d'une telle guerre consiste à obtenir un avantage en matière d'information en combinant des moyens techniques de renseignement et d'autres sources d'information en un seul réseau*." » [xxxii]



Le « maître de l'électron » face au « maître du feu » — Photo BS © John D

Actuellement, et selon le site war.ukraine.ua, les militaires ukrainiens disposent d'une douzaine de logiciels et d'applications installés sur des *smartphones* ou des tablettes dont Kropyva (appui-feu), MilChat (messagerie sécurisée), MyGun (calculateur balistique), ComBat Vision (renseignement)

« Kropyva » (« orties ») Outil numérique ukrainien pour appui-feu — Photo SOS Army

« Kropyva« : Automatic Tactical Management System" (ATMS) — Photo SOS Army

« *La créativité et l'initiative ukrainiennes sont patentes. Dans le cadre de leur formation sur l'artillerie américaine, les Ukrainiens complètent leur formation par la prise en main d'une application pour smartphone qui les aide à calculer les informations de ciblage sur le champ de bataille.*

L'application, créée par un civil ukrainien travaillant avec l'armée, aide les unités d'artillerie à calculer rapidement les coordonnées de tir en saisissant des informations telles que les conditions environnementales, les distances et les charges – ce qui change la donne dans les duels d'artillerie avec les forces russes. C'est l'un des nombreux exemples qui démontrent la capacité d'une organisation militaire à capitaliser sur l'ingéniosité et l'expérience opérationnelle dans le respect de la chaîne hiérarchique - un contraste frappant avec la culture et les pratiques militaires russes.»[xxxiii]

« *Le principe a déjà été exploité lors de conflits précédents. Le coup de génie ukrainien, c'est d'avoir changé d'échelle en misant sur le très haut degré de numérisation de sa population et en mobilisant son écosystème de développeurs. Chaque soldat, chaque citoyen est maintenant un «* combattant numérique *». Muni de son smartphone, chacun devient un maillon dans une boucle de décision accélérée, réduite, fluidifiée et un acteur dans l'atteinte d'un objectif central, celui de «* taper en premier ».

« Tout cela, les Ukrainiens l'ont parfaitement exploité *», relève un militaire français. Et, surtout, ils ont rapidement constaté le retard russe dans ce segment avec «* des communications militaires très classiques qui n'ont pas fonctionné *». Faute de mieux, les soldats russes se sont rabattus de manière anarchique sur des outils non sécurisés, rendant leur ciblage extrêmement facile.* »[xxxiv]

4. Vers une transfiguration de l'espace de bataille numérisé ?

L'emploi du *smartphone* non seulement change la face des combats en Ukraine mais pourrait révolutionner les concepts des armées occidentales en matière d'infovalorisation.

« *L'omniprésence des téléphones mobiles sur le champ de bataille crée un ensemble de pratiques médiatiques participatives uniques. Une variété d'usages personnels, tels que les communications privées et le divertissement, sont combinés dans le même appareil avec l'écoute électronique, le ciblage des feux, la cartographie des champs de mines et les transmissions tactiques. Les téléphones mobiles se substituent aux équipements anciens ou indisponibles et comblent les lacunes des matériels militaires ; ils deviennent ainsi des armes et ils sont l'exemple de l'hybridation entre le militaire et l'intime, entre la guerre et la paix. Les potentialités du téléphone mobile donnent une portée médiatique au champ de bataille et remettent en question la définition même d'un outil de combat*. »[xxxv]

Cependant, force est de constater que le *smartphone* peut rapidement présenter les défauts de ses qualités s'il est employé sans règles ni discipline d'emploi, tant pour son rayonnement électromagnétique que lumineux ou parce qu'il n'est pas, en règle générale, crypté.

« *Une situation plus courante est celle où l'artillerie cible de nombreux numéros de mobiles qui s'activent simultanément en un lieu inattendu, par exemple au milieu d'un champ ou d'une zone déserte. Pour les localiser, il faut avoir accès aux antennes relais ce qui ne pose souvent aucun problème sur une ligne de front numériquement poreuse. Un contact m'a dit qu'il est même possible d'évaluer l'effectif d'une unité en calculant le nombre de téléphones actifs (...)* »[xxxvi]

En outre, cet outil mulimédia de combat, qui peut servir à appeler ses enfants puis, sans transition, à neutraliser ses ennemis, possède un objectif qui fait de tout combattant un journaliste de guerre, capable, entre autres, de photographier les prisonniers et les morts, de les identifier sur les réseaux sociaux grâce à l'intelligence artificielle (Clearview AI) puis d'envoyer les clichés à leurs familles. Nous entrons dans une nouvelle dimension, encore inédite, de la guerre de l'information.[xxxvii]

5. Commentaires

« (…) *cette guerre est menée selon un tempo imprimé par le numérique civil. Ce terreau était déjà visible au Sahel, face à des adversaires n'ayant que très peu accès aux technologies de niveau militaire et recourant aux technologies civiles pour communiquer et mener des attaques informationnelles*. »[xxxviii]

Grâce à l'hybridation des technologies civiles et militaires, à la complémentarité des savoir-faire publics et privés des géants de l'informatique et des communications par satellite, les Ukrainiens ont mis peu de temps à développer plusieurs applications équivalant au « *blue force tracking* » et à mettre sur pied une boucle renseignement / OODA (*Observe, Orient, Decide, Act*) particulièrement performantes et faciles d'emploi alors que les industries de défense occidentales ont peiné à mettre au point des logiciels identiques sur des équipements purement militaires et beaucoup moins conviviaux.

La rapidité du cycle décisionnel, la précision et la vitesse de transmission du renseignement – technique ou de source humaine, couplés à l'emploi de drones armés et de munitions « intelligentes » a des effets dévastateurs sur les postes de commandement et les bases logistiques. Ainsi que l'écrit le Royal United Services Institute (RUSI) dans son retour d'expérience adressé au ministère britannique de la défense : « *There is no sanctuary* ».
La survie est dorénavant liée à la dispersion et à une organisation agile et réactive du commandement et du contrôle.

« *L'approche historique du Corps allié de réaction rapide et de la 3e division britannique consistant à ériger de véritables villes de tentes - des postes de commandement avec une grande empreinte physique - n'est pas viable en temps de guerre sur le champ de bataille moderne. Ces sites seront identifiés et feront l'objet de frappes. De plus, comme les Russes l'ont découvert à leurs dépens, les postes de commandement concentrés à l'intérieur de bâtiments civils réquisitionnés sont également vulnérables aux tirs de précision à longue portée, à moins que tout le personnel ne maintienne une discipline stricte en matière de communications. Même dans ce cas, la menace HUMINT impose dispersion et déplacements fréquents. La capacité technique de délocaliser le travail d'état-major signifie qu'il n'est plus nécessaire de le concentrer à un même endroit.* »[xxxix]

Militaire ukrainien installant un terminal Starlink **sur le terrain — Photo © ZSU**
Comment installer et que coûte à l'Ukraine Starlink ? Par Yevgeniya Smereka, (16 novembre 2022)

Cela dit, pour l'heure nous ne disposons pas d'informations quant

- aux techniques de vérification, de fusion et de gestion des importants flux de données provenant d'innombrables capteurs ;
- à l'organisation du travail collaboratif, distribué et délocalisé ;
- à l'organisation et au fonctionnement des états-majors et des systèmes de poste de commandement (PC) ;
- à la planification des opérations et au processus décisionnel ;
- à la diffusion des ordres et aux supports employés à cet effet – même si Starlink offre un service internet de grande qualité, une redondance rassurante et une bonne résilience.

Nous n'avons pas non plus de retour d'expérience quant à la fréquence et à la qualité des cyber actions ukrainiennes menées en accompagnement ou en appui des opérations, ni à la nature et au volume des renseignements acquis sur les forces russes, mis à part le commentaire peu amène de James A. Lewis du *Center for Strategic & International Studies*, qui ne concerne toutefois que les hackers :

« *Bien que célébrées dans les médias, les diverses cyber actions menées par des acteurs privés contre des sites Web n'ont eu aucune influence sur les opérations ou sur les capacités militaires russes, et, pour autant que l'on puisse en juger, sur les calculs stratégiques de Poutine. Les résultats des activités des hackers et leurs efforts contre la Russie sont exagérés. La Russie n'a pas changé de cap ou modifié ses plans suite à ces actions et sa capacité à s'engager dans des opérations offensives n'a pas été entamée par ces attaques sporadiques. L'opinion publique russe, qui soutient largement la guerre, ne semble pas affectée par les hackers. Par conséquent, l'hacktivisme n'a aucune incidence sur le déroulement de la guerre.* » [xl]

****

6. Conclusion

Dès 2014, alors qu'ils se demandaient si la cyberguerre aurait lieu, les colonels Bonnemaison et Dossé tiraient déjà les conclusions suivantes :

« *Le combat cyber-électronique n'est donc, ni plus ni moins, qu'un moyen d'action supplémentaire qui interagit hors et sur le champ de bataille. Il ne révolutionne pas la stratégie ou l'art opératif dont les principes demeurent. Le cyberespace investit le champ tactique avec une dynamique propre mais qui ne peut être efficace que dans le cadre d'une manœuvre interarmes, interarmées ou globale. Dans tous les cas, il contribue aux fondamentaux du combat c'est-à-dire à contraindre un adversaire, à contrôler le milieu et à influencer les perceptions. Si son action n'est généralement pas décisive, toute impasse dans ce domaine entraînera la défaite*. »[xli]

Bénéficiant du retour d'expérience des opérations qui viennent de se dérouler, James A. Lewis ne dit pas autre chose :

« *Dans les conflits impliquant des armées modernes, les cyberattaques sont utilisées de préférence en combinaison avec la guerre électronique (GE), les campagnes de désinformation, les attaques antisatellites et les munitions à guidage de précision. L'objectif est de dégrader l'avantage informationnel et les biens immatériels (tels que les données), les communications, les moyens de renseignement et les systèmes d'armes pour produire un avantage opérationnel. Les actions les plus dommageables combineraient des munitions à guidage de précision et des cyberattaques pour désactiver ou détruire des cibles critiques. Les cyber opérations peuvent également être utilisées à des fins politiques en perturbant la finance, l'énergie, les transports et les services gouvernementaux afin d'entraver le processus décisionnel des défenseurs et de créer des troubles sociaux. La Russie n'a été en mesure d'atteindre aucun de ces objectifs à une échelle significative.*

Il faut faire de réels efforts pour qu'une cyberattaque soit plus qu'une simple nuisance. Cela nécessite planification, développement d'outils ad hoc et moyens d'acquisition du renseignement, intégrés à

d'autres capacités offensives. On en mesurera l'efficacité par l'étendue des dommages et si l'adversaire est forcé à changer ses plans ou à faire des concessions. En outre, contrairement à une attaque qui fait mouche avec arme cinétique, les cyberattaques n'entraînent pas de dégâts apparents (un radar touché par un missile peut être vu comme une ruine fumante, mais de l'extérieur, une cyberattaque réussie sur un radar peut ne pas sembler différente d'une autre qui échoue, et tout dommage peut ne pas être permanent). »[xlii]

Son jugement sur les insuffisances russes est sans appel :

« *La Russie a montré comment ne pas utiliser les cyber opérations pour obtenir un avantage dans un conflit armé, mais ses efforts mettent en lumière les bonnes pratiques. La leçon la plus évidente est la nécessité d'une préparation adéquate pour effectuer des frappes coordonnées et simultanées sur des cibles critiques. La deuxième est d'obtenir une cyber-supériorité en paralysant les cyber-défenseurs. La troisième est de préparer le champ de bataille politiquement et psychologiquement et de contrôler autant que possible le récit public de la campagne.* »[xliii]

Cependant, et ainsi que le souligne James A. Lewis, les dommages imputables aux opérations cyber sont difficiles à évaluer. Selon Jon Bateman[xliv], les Ukrainiens ont intérêt à en minimiser la portée et à supprimer les preuves de toute cyber-perturbation d'équipements militaires ; les Russes cherchent à dissimuler leurs insuffisances et à relativiser les effets des cyber-perturbations sur les tierces parties; les alliés ont des intérêts commerciaux à présenter leur cyber-soutien à l'Ukraine comme très réussi et stratégiquement essentiel.
Pour trancher ces débats et en tirer des leçons, il faudra du temps et du recul car de nombreuses intrusions ont pu passer inaperçues. En définitive, un "brouillard de guerre cybernétique" continue d'envelopper même les cybers incidents les plus étroitement surveillés.
Cela dit, même si l'Ukraine et ses alliés, ont montré que dans le domaine cybernétique la défense bien organisée, « en profondeur », est supérieure à l'attaque, cette remarque de James A.Lewis pourrait sembler excessive :

« *Cela peut offenser la communauté cybernétique de le dire, mais les cyberattaques sont surfaites. Si elles sont inestimables pour l'espionnage et la criminalité, elles sont loin d'être décisives dans un conflit armé. Une pure cyberattaque, comme le notent la plupart des analystes, est inadéquate pour contraindre tout adversaire, sauf le plus fragile, à accepter la défaite.* »

Certes, son commentaire vaut pour un conflit armé, mais, jusqu'à maintenant, les cyber-attaques les plus élaborées prennent place en temps de paix, comme l'a montré Stuxnet en 2010.

« *La paternité de cette offensive n'est d'ailleurs pas officiellement connue. (…) De nombreux analystes supposent qu'il s'agirait d'une opération conjointe. Quoiqu'il en soit, son originalité est qu'elle militarise un procédé de cyber-criminalité pour le transformer en mode d'action stratégique, dans la profondeur du dispositif adverse. Elle ajoute ainsi aux opérations commandos clandestines et aux raids aériens la possibilité d'une stratégie subtile de sabotage par une action discrète, efficace et potentiellement non signée* » [xlv]
… donc sans recours possible à l'article 5 ou à l'article 42.7

Par conséquent tout reste encore possible en matière d'agressions, d'autant que nous n'avons certainement pas encore tout vu :

« *La Russie est presque certainement capable de cyber-attaques de plus grande envergure et de plus grande conséquence que les événements en Ukraine ne le laissent croire ", La guerre " n'a pas encore impliqué les deux parties employant l'une contre l'autre des cyber-capacités offensives haut de gamme* » [xlvi]

Enfin et surtout, il y a un adversaire potentiel de premier rang qui ne doit pas perdre une miette des opérations en cours, qu'elles soient cybernétiques ou classiques : la Chine.

« *Le conflit en Ukraine peut informer les États-Unis et leurs alliés sur la manière de se défendre contre les cyber-opérations offensives dirigées contre eux par des adversaires, mais la Chine ou même l'Iran peuvent également avoir appris de l'expérience russe. Pour les cyber-actions, l'Ukraine n'est probablement pas une référence dans le cas d'un conflit avec la Chine. La Chine est mieux équipée et dispose probablement d'une meilleure planification. Les États-Unis peuvent également ne pas vouloir compter sur l'ineptie de ces adversaires, même s'ils partagent un processus décisionnel autoritaire (et donc probablement atypique)* ».[xlvii]

Général de division (2s) Jean-Marc WASIELEWSKI

---

[i] « *Les possibilités les plus destructrices, selon M. Panetta, impliquent que " les cyber-acteurs lancent plusieurs attaques sur nos infrastructures critiques en même temps, en combinaison avec une attaque physique. " Il a décrit le résultat collectif comme un "cyber-Pearl Harbor qui causerait des destructions physiques et des pertes de vie, une attaque qui paralyserait et choquerait la nation et créerait un nouveau sentiment profond de vulnérabilité* », New York Times, 11 october 2012

[ii] Thibault Fouillet in « La vision stratégique de l'Armée de terre », Les cahiers de la Revue de la Défense Nationale, 2020

[iii] Field Manual 3-38 Cyberelectromagnetic activities, 2014

Des six branches des forces armées américaines seule l'*US Army* utilise la CEMA comme concept doctrinal pour fusionner distinctement ses missions de guerre cybernétique et électronique. Parmi les États membres de l'OTAN, la CEMA n'a été reproduite sur le plan doctrinal que par le ministère britannique de la Défense en 2016.

[iv] Colonel Patrick Justel « La guerre électronique : question du passé ou d'avenir ? » in Les cahiers de la Revue Défense Nationale, 2018

[v] https://www.linkedin.com/pulse/guerre-en-ukraine-orties-l-app-disruptive-au-service-du-fontanellaz?trk=public_profile_article_view

[vi] Audition du général Bonnemaison, compte rendu N° 27 de la Commission de la défense nationale et des forces armées du 7 décembre 2022

[vii] Keir Giles « Handbook of Russian information warfare », NATO Defense College, 2016

[viii] « Lessons from Russia's cyber war in Ukraine », The Economist, 30 November 2022

[ix] Général Bonnemaison, *op. cit*

[x] https://www.economist.com/podcasts/2022/12/06/the-surprising-ineffectiveness-of-russias-cyber-war

[xi] Nicolas Mazzuchi « La Russie et le cyberespace, mythes et réalités d'une stratégie d'Etat » in Revue Défense Nationale N° 802, été 2017

[xii] James A. Lewis, « Cyber war and Ukraine » Center for Strategic and International Studies (CSIS), June 2022

[xiii] The Economist, *op. cit*

[xiv] Aspirant Pierre Vallée, in La Note du Centre d'Études Stratégiques Aérospatiales (CESA), 06/2022

[xv] The Economist, *op. cit*
[xvi] James A. Lewis, *op. cit*
[xvii] https://www.businessinsider.com/russian-ew-campaign-in-ukraine-undermined-by-electronic-fratricide-2022-11?r=US&IR=T
[xviii] Royal United Services Institute (RUSI), Preliminary lessons in conventional warfighting from Russia's invasion of Ukraine : February-July 2022
[xix] Roman Horbyk, « The war phone" mobile communication on the frontline in Eastern Ukraine », in Digital War, 2023
[xx] James A. Lewis, *op. cit*
[xxi] The Economist, *op. cit*
[xxii] Jon Bateman, « Russia's wartime cyber operations in Ukraine : military impacts, influences, and implications », Carnegie endowment for international peace, December 2022
[xxiii] https://www.lesechos.fr/tech-medias/hightech/letonnant-flegme-des-developpeurs-informatiques-ukrainiens-1391972
[xxiv] James A. Lewis, *op. cit*
[xxv] « Guerre en Ukraine : les cyber-attaquants, l'autre armée de Vladimir Poutine », La Tribune, 27 décembre 2022
[xxvi] Audition du général Bonnemaison, *op. cit*
[xxvii] The Economist, *op. cit*
[xxviii] https://ukraine.ua/invest-trade/digitalization/
[xxix] La transformation numérique à l'appui de la reprise en Ukraine note de l'OCDE 1 juillet 2022
[xxx] https://mezha.media/en/2022/10/28/the-unique-ukrainian-situational-awareness-system-delta-was-presented-at-the-annual-nato-event/
[xxxi] https://www.lemondeinformatique.fr/actualites/lire-la-resistance-ukrainienne-passe-aussi-par-le-numerique-86736.html_11
[xxxii] https://war.ukraine.ua/fr/articles/armes-de-guerre-numeriques-applications-et-logiciels-qui-aident-l-ukraine-a-vaincre/
[xxxiii] https://rusi.org/explore-our-research/publications/commentary/us-led-security-assistance-ukraine-working
[xxxiv] https://www.forcesoperations.com/la-france-entre-surprises-et-lacunes-sur-le-combattant-numerique/
[xxxv] Roman Horbyk, *op.cit*
[xxxvi] Roman Horbyk, *op.cit*
[xxxvii] https://www.washingtonpost.com/technology/2022/04/15/ukraine-facial-recognition-warfare/
[xxxviii] https://www.forcesoperations.com/la-france-entre-surprises-et-lacunes-sur-le-combattant-numerique/
[xxxix] Royal United Services Institute, *op. cit*
[xl] James A. Lewis, *op. cit*
[xli] Colonel Aymeric Bonnemaison, colonel Stéphane Dossé « Attention : Cyber ! vers le combat cyber électronique », p189, Economica, 2014
[xlii] James A. Lewis, *op. cit*
[xliii] James A. Lewis, *op. cit*
[xliv] Jon Bateman, *op. cit*
[xlv] Colonel Aymeric Bonnemaison, colonel Stéphane Dossé, *op. cit*
[xlvi] The Economist, *op. cit*
[xlvii] James A. Lewis, *op. cit*