LE RUBICON

Le combat cyberélectronique russe en Ukraine

Anthony Namor | 8 juillet 2022

12 février 2015, en pleine bataille de Debatselve, dans le Donbass, des militaires ukrainiens reçoivent sur leur téléphone personnel des messages les dissuadant de poursuivre le combat. 24 février 2022, à l'instant précis où la Russie fait entrer ses troupes en Ukraine, l'attaque informatique de l'opérateur satellite *ViaSat* rend impossible toute communication sur son réseau. Depuis près de dix ans, l'Ukraine est le théâtre de guerres hybride et conventionnelle, qui ont vu la mise en œuvre d'opérations numériques variées couvrant un large éventail allant de la guerre électronique tactique aux attaques informatiques stratégiques. Que nous apprennent les actions russes dans le cyberespace ukrainien ? Quels effets la Russie a-t-elle cherché à y produire ? Dans les contextes très différents de 2014 et 2022, est-elle parvenue à combiner ces effets avec son action au sol, de façon à en démultiplier l'efficacité ?

De la conquête des champs immatériels dès le temps de paix à l'appui de l'engagement cinétique, les actions russes dans le cyberespace (« maillage de l'ensemble des réseaux permettant l'interconnexion informationnelle des êtres vivants et des machines » d'après la définition concise et généraliste donnée par Stéphane Dossé et Aymeric Bonnemaison dans « Attention : Cyber ! ») sont autant d'éclairages sur la nature du combat de demain. Si les effets cyber sont encore loin d'être maîtrisés et intégrés à la manœuvre dans un engagement conventionnel, ils sont parfaitement adaptés à la guerre hybride (combinaison de modes d'actions réguliers et irréguliers) . De l'importance de la connaissance et du modelage anticipés du cyberespace à la nécessaire décentralisation de compétences cyber transverses au niveau tactique, le cas ukrainien est riche d'enseignements pour les forces terrestres.

Compétition géopolitique, contestation stratégique : gagner la guerre avant la guerre ?

Véritable champ de compétition géopolitique et de contestation stratégique, le cyberespace fait l'objet de l'attention russe depuis bien avant 2014. Tandis que la doctrine occidentale met le combat réseau-centré (doctrine faisant reposer le succès des opérations sur la supériorité informationnelle sur le champ de bataille) et l'infovalorisation (recherche de l'exploitation optimale de l'information par son partage et son traitement en temps réel) au cœur de sa stratégie depuis près de vingt ans, la Russie mise en réaction sur l'arme informationnelle. De fait, le ratio coût – efficacité de l'arme cyber est particulièrement intéressant

pour une puissance moyenne, au regard de l'importance qu'a pris la boucle de *command and control* (C2) occidentale et de sa vulnérabilité.

Compétition : La conquête des champs immatériels dès le temps de paix

L'appropriation d'un espace numérique repose d'abord sur la maîtrise physique du cyberespace. Ainsi, la Russie emploie l'installation de câbles assurant le trafic internet par Rostelecom dans le prolongement de sa politique extérieure. En 2014, Dmitry Medvedev avait ordonné la pose d'un câble traversant le détroit de Kertch dès l'annexion de la Crimée, achevant la conquête militaire de cet espace par une intégration numérique. Par ailleurs, le Kremlin œuvre depuis au moins 2013 à la mise sur pied d'un internet « souverain ». Il a créé à cet effet un cadre légal centralisant la régulation de l'internet par l'État et a monté son propre serveur DNS (les serveurs *Domain Name Service* (DNS) servent à aiguiller les requêtes des utilisateurs en faisant l'association entre le nom d'une page web et son adresse numérique. L'internet mondial repose sur 13 serveurs racines, dont 9 sont gérés par des entités américaines.). Celui-ci a été rendu incontournable pour les sites web étatiques le 11 mars 2022, ouvrant ainsi la voie à une fragmentation de l'internet en un sous-espace contrôlé par l'État russe. Enfin, l'action russe dans le champ sémantique est riche et souvent offensive. Elle s'inscrit dans un cadre conceptuel faisant de la nation russe une entité qui transcende les ethnies et fédère les groupes nationaux sous une vision politique unique présentant l'Occident comme un adversaire existentiel. Cette politique d'influence repose notamment sur la langue dont la défense de ses pratiquants est un des motifs d'intervention utilisés par les Russes.

Contestation : la cyberguerre sous le seuil

En amont des interventions cinétiques de 2014 et 2022, la Russie agit dans le cyberespace dans la continuité d'une politique parfois coercitive vis-à-vis de l'espace postsoviétique (les pays du format Bucarest 9 : Bulgarie, Estonie, Hongrie, Lettonie, Lituanie, Pologne, République tchèque, Roumanie et Slovaquie). Ces opérations, parfois très offensives, se caractérisent par l'emploi courant de *proxies* et la dénégation de toute implication étatique. Elles peuvent être classées en deux catégories :

- **La préparation de l'action stratégique.** D'abord par le renseignement mené via des campagnes d'APT (*advanced persistent threats)* ; un virus pénètre le réseau d'une organisation pour en exfiltrer des informations sensibles en toute discrétion, parfois pendant plusieurs années sans être décelé. Si de tels virus peuvent être conçus par des groupes cybercriminels (assemblage de modules exploitant des failles divulguées ou achetées), la coordination et la collecte des informations nécessite sans doute une contribution étatique (les groupes maîtrisant ces techniques tels que Sandworm, Turla, APT28 et APT29, pour ne citer qu'eux, sont connus pour être très proches voire intégrés aux services de renseignement russes).
- **Les actions de déstabilisation.** Dans ce domaine, l'attaque complexe contre les élections nationales en 2014 est une bonne illustration. Les *hackers* ont procédé méthodiquement, cherchant à supprimer des fichiers de comptage, à modifier l'affichage des résultats et à empêcher le site de la commission électorale de communiquer les résultats (déni de service). En 2015 et 2016, également, deux attaques ont visé des centrales électriques ukrainiennes, privant plusieurs centaines de milliers de foyers d'électricité. En 2018, enfin, une installation ukrainienne de purification d'eau au chlore était ciblée par le malware russe *VPNFilter*. Ces attaques d'une grande sophistication (coordination parfaite, suppression des traces et attaques simultanées des moyens de secours), contribuent autant à l'intimidation de l'Ukraine qu'à la démonstration au monde que la Russie maîtrise un arsenal similaire à celui prêté aux États-Unis lors de l'opération *Stuxnet*.

Bien que très offensives, ces opérations souvent prêtées par les autorités russes à des groupes indépendants, ont été menées sous le seuil menant à la violence étatique déclarée. Elles sont autant d'outils permettant de préparer l'appui numérique à l'intervention cinétique.

Confrontation : l'arsenal numérique russe dans les opérations aéroterrestres

La Russie dispose ainsi de renseignement technique sur les opérateurs vitaux adverses, d'une série de *malwares* conçus par des groupes cyber criminels expérimentés prêts à l'emploi et de modes d'action de guerre électronique éprouvés. Ses opérations au sol en 2014 et 2022 ont ainsi pu être appuyées par un arsenal numérique complet, avec plus ou moins de succès.

De l'appui cyberélectronique ciblé en guerre hybride de 2014…

En 2014, l'intervention russe avait bénéficié d'un appui numérique ciblé et efficace, s'intégrant parfaitement dans le mode de guerre hybride alors privilégié. Celui-ci avait essentiellement consisté en une série de dénis de services menés par des groupes non étatiques visant les téléphones des parlementaires ukrainiens ou saturant les sites officiels, l'exacerbation des tensions internes et l'installation d'un soutien virtuel à la sécession notamment en Crimée, ainsi que de fuites d'information visant à révéler l'implication de l'OTAN au profit de Kiev. Une fois l'environnement informationnel modelé, des troupes russes étaient

intervenues en Crimée et dans le Donbass, appuyées par des actions de guerre électronique. L'armée russe avait alors démontré sa capacité à leurrer le GPS, brouiller dans les gammes radio tactique V/UHF voire satellitaires, employer des charges d'appui-électronique sur des drones Orlan 10 pour cibler la téléphonie mobile ou détecter et brouiller les radars de contre-batterie ukrainiens, et même désactiver massivement à distance des postes radios ukrainiens de fabrication russe. Des actions combinées de guerre électronique et d'influence ont également été rapportées : diffusion ciblée des messages d'intimidation sur les téléphones personnels de soldats ukrainiens ou envois ciblés de SMS contenant une charge utile permettant l'interception (voix et texte) du téléphone.

… Aux attaques informatiques insuffisantes du conflit conventionnel de 2022

En 2022, la Russie sort clairement de l'hybridité et s'engage en Ukraine de manière conventionnelle et plus massive. L'appui cyberélectronique, bien que plus perfectionné dans la couche logique, semble bien moins efficace dans la couche physique qu'en 2014.

En complément des moyens rattachés à chaque brigade interarmes, la Russie aurait engagé ses cinq brigades terrestres de guerre électronique et six unités autonomes. Disposant globalement des mêmes capacités qu'en 2014, celles-ci ne semblent pas avoir entravé efficacement la défense ukrainienne. Bien que les infrastructures télécoms aient été la cible de frappes d'artillerie, les Ukrainiens semblent avoir conservé une connexion au réseau de téléphonie mobile grâce à la mobilisation des équipes techniques pour le rétablissement des antennes et les accords de *roaming* entre différents opérateurs (permettant aux utilisateurs d'utiliser indifféremment leurs infrastructures). La connectivité par satellite a été visée par une attaque complexe parfaitement coordonnée dès le 24 février 2022. Une station au sol de l'opérateur *ViaSat* aurait ainsi été leurrée afin de lui faire envoyer une charge endommageant irrémédiablement les terminaux associés. En réponse, la mise à disposition de téléphonie satellitaire via *starlink* a favorisé les connexions internet indépendantes du réseau tout en ouvrant un risque important de géolocalisation des terminaux associés. Les systèmes informatiques ont quant à eux été la cible de virus produisant des effets durables : les *wipers*. Ils s'attaquent aux mêmes secteurs sensibles des disques durs que les *ransomwares,* mais ne permettent aucune récupération de données sur rançon : leur objectif est de détruire du matériel informatique pour un effet à plus long terme. Des attaques moins complexes, mais plus massives ont également été lancées pour perturber les services, telles que les attaques de déni de service (DoS). Les cibles (sites internet du gouvernement ukrainien, de banques et de l'armée) étaient publiées afin que des volontaires saturent leurs serveurs d'hébergement de requêtes inutiles. L'*IT ARMY* (groupe d'attaquants informatiques volontaires qui agit sous le commandement de l'armée ukrainienne depuis le 26/02/2022) a réalisé de telles actions contre des sites internet officiels en Russie.

Enfin, des effets d'influence ont été recherchés par défacement (modification d'une page web à l'insu de ses administrateurs) et fuites de données. Au-delà des campagnes de niveau politique et stratégique, la désinformation cible à un niveau plus tactique le renseignement en source ouverte (OSINT), très largement développé en 2022. L'essor des médias sociaux associé au développement de capteurs et d'outils d'analyse grand public ouvre de nouvelles perspectives : connexion à distance à des cartes radiologicielles par des radioamateurs pour intercepter voire localiser des communications russes, partage d'images satellites, *reporting* participatif en ligne. Reposant sur un grand nombre de contributeurs, cette source peut s'avérer précise et exhaustive. Sa fiabilité est cependant à interroger pour les mêmes raisons : l'OSINT fait aussi l'objet de campagnes de désinformation. Ainsi plusieurs vidéos truquées ont été diffusées sur les réseaux par les Ukrainiens et certains sites prétendant débusquer les fausses informations sont en réalité des instruments de propagande. La fiabilisation de l'information, qui repose sur le recoupement de sources variées, est rendue plus difficile par la fragmentation d'internet. Suivant le découpage physique du réseau mondial, des sphères d'information alternatives pourraient ainsi se développer de part et d'autre de la ligne de front.

Enseignements

À ce stade du conflit, nous pouvons livrer les quelques analyses suivantes de l'emploi de moyens cyber en appui des opérations aéroterrestres.

La cyberguerre commence avant la guerre

En 2014 comme en 2022, les troupes russes interviennent dans un environnement cyber connu et préalablement modelé. Le succès des actions numériques dépend en grande partie de la qualité du renseignement (notamment technique) préalablement collecté, y compris par des méthodes actives largement en amont. Le modelage de l'environnement est mené dans les domaines économique, politique, sémantique, mais aussi informatique : la cyberattaque d'opérateurs vitaux vise à se positionner parmi les puissances maîtrisant une technologie, à l'instar de la démonstration d'un tir balistique. Pour autant, le choix de démontrer ou cacher une telle capacité est un véritable dilemme pour un décideur. À l'inverse d'un missile, une attaque cyber est

difficilement déclenchable sur court préavis et l'adaptation réactive de la défense plus rapide et moins coûteuse que le déploiement d'un bouclier antimissile. C'est en somme un fusil à un coup. Aucune autre attaque de système industriel vital n'a été constatée en appui tactique direct des opérations cinétiques de 2014 et 2022. Pour l'heure, ces actions se cantonnent donc à la démonstration de force, sur des centrales au fonctionnement bien connu des Russes. Ce qui n'exclut pas la maîtrise du même type d'action contre des installations plus lointaines employant des technologies occidentales. En 2011, les États-Unis avaient renoncé à l'emploi d'attaques cyber contre les défenses anti-aériennes libyennes, pour éviter de dévoiler cette capacité et créer un précédent. Tout l'enjeu est ainsi d'en montrer suffisamment pour être crédible, mais suffisamment peu pour conserver un effet de surprise sur des défenses faillibles et rester sous le seuil de l'offensive déclarée. Ce dernier point est facilité par l'emploi russe de modes d'action hybrides.

Les effets cyberélectroniques sont encore loin d'être intégrés et maîtrisés

La plupart des attaques informatiques de 2014 et 2022 ont constitué un bruit de fond, plus ou moins intense, permanent et parfois coordonné avec les objectifs tactiques. Il a indéniablement perturbé la capacité de l'État ukrainien à répondre aux crises qu'il a traversées. Bien que les attaques informatiques et cinétiques tendent peu à peu à converger vers des cibles communes en 2022, l'appui cyber n'est pas encore un démultiplicateur de force à même de faciliter la manœuvre aéroterrestre russe, dont il a été majoritairement décorrélé jusqu'alors. Ce pour plusieurs raisons :

1. L'efficacité de l'attaque cyber ne peut être garantie, car l'effet est difficilement maîtrisable ;
2. Son intégration à la manœuvre dès sa conception semble peu plausible au regard des acteurs qui la mettent en œuvre à un échelon centralisé, non militaire, loin du champ de bataille ;
3. Les cibles sont essentiellement civiles : aucune attaque réussie d'un système d'information militaire n'est ouvertement connue à ce jour.

Si la combinaison d'attaques informatiques et de guerre électronique est particulièrement bien adaptée à la guerre hybride face à un État déjà fragilisé, il l'est moins dans un conflit symétrique de haute intensité. L'arsenal informatique s'étoffe cependant et constitue une menace bien réelle pour les centres de commandement.

La guerre électronique aurait pu quant à elle conférer un avantage tactique à la manœuvre russe, mais semble n'avoir pas tenu ses promesses en 2022. Pour l'heure, les hypothèses suivantes peuvent être avancées quant à cet échec :

1. Il s'agit d'un appui à la fois très technique et manœuvrier qui requière un haut niveau d'instruction et d'entraînement. Or cette fonction est largement armée par des conscrits : un quart des militaires formés à la guerre électronique en 2014 étaient professionnels;
2. L'engagement massif de 2022 nécessitait une coordination interarmes et une expertise tactique avancées. Mal maîtrisé par des opérateurs peu expérimentés, l'usage des brouilleurs aurait surtout gêné les systèmes russes, menant les chefs tactiques à sous-employer cette capacité ;
3. La proximité des systèmes ukrainiens et russes, utilisant des fréquences proches, aurait renforcé cette difficulté ;
4. Les sanctions à l'encontre de la Russie auraient compliqué le maintien en condition opérationnelle des équipements qui s'étaient montrés très efficaces en 2014. La plupart a été livrée entre 2013 et 2017, or dans ce domaine les mises à jour doivent intervenir au bout de 3 puis 5 ans, puis être renouvelées après 8 ans pour conserver leur supériorité technologique ;
5. L'armée ukrainienne, forte de son expérience face aux Russes et appuyée par plusieurs États et organisations internationales, aurait développé une résilience en apprenant à manœuvrer en contexte cyberélectronique dégradé.

Ces éléments soulignent l'importance, pour la guerre électronique, de disposer d'une troupe spécialisée sélectionnée sur des critères propres, bien instruite dans son cœur de métier et entraînée aux côtés des autres fonctions opérationnelles (mêlée, artillerie, etc.). Il est tout aussi important d'acculturer les chefs tactiques à l'emploi et à la coordination avec cet appui. L'échec dans ce domaine ne doit pas pour autant être considéré comme définitif : il est probable que la Russie apprenne de ses erreurs comme elle l'avait fait en 2008 après ses échecs relatifs en Géorgie. Enfin, la résilience informationnelle ne s'oppose pas à l'infovalorisation : elle la complète. Il est aujourd'hui aussi important de savoir utiliser une connexion satellitaire qu'un téléphone filaire TA57 de l'ère soviétique.

Limites et perspectives : quel appui cyberélectronique pour les opérations aéroterrestres ?

Le panel des outils techniques cyberélectroniques du chef tactique s'étoffe, en particulier dans la couche logique du cyberespace (le domaine des logiciels et des protocoles informatiques). Pour autant, leur maîtrise fine, leur combinaison et intégration à la manœuvre aéroterrestre demeurent très embryonnaires au niveau tactique. Cette difficulté tient, d'une part, aux

compétences transverses à développer à cet échelon et, d'autre part, à la nature des cibles concernées. Comme le souligne Bertrand Boyer dans *Cybertactique*, les infrastructures numériques civiles et militaires sont fortement imbriquées, rapprochant en cela le combat cyber du combat en zone urbaine. Si la Russie exploite cette zone grise en s'appuyant sur des *proxies* non militaires, cela ne correspond pas à l'éthique du modèle français. Pour l'investir, ce dernier devra sans doute intégrer les principes fondamentaux du droit international dans la conception de sa manœuvre cyber.

Des compétences sont à développer au sein des armées afin de défendre les moyens de commandement comme d'en exploiter les vulnérabilités. Pour y parvenir de manière optimale et pleinement intégrée à la manœuvre, il conviendra sans doute de placer une partie de ces capacités aux plus bas niveaux tactiques, afin d'appréhender l'épaisseur cyber du champ de bataille, à l'image de l'aviation légère de l'armée de Terre pour la troisième dimension. En cohérence avec une capacité stratégique à même de connaître et modeler l'environnement cyber avant l'engagement, cette composante tactique devra mobiliser des compétences variées dans les trois couches (physique –ondes et infrastructure – logique – code et protocoles – sémantique – influence et opérations psychologiques) du cyberespace pour répondre au besoin que le chef tactique doit apprendre à formuler, ou pour saisir des opportunités sur le champ de bataille.

Le combat cyberélectronique ne permet pas, seul, de remporter la victoire. Mais mal maîtrisé, il pourrait bien la laisser échapper.

Crédit : Rodrigo Abd / The Associated Press

•— ••— — • ••— •—• •••

Anthony Namor

Anthony Namor (@anthony_namor) est chercheur associé au centre de recherche des écoles de Coëtquidan (CREC). Officier saint-cyrien, il a essentiellement servi et commandé en unités de guerre électronique et de cyberdéfense militaire. Il réalise une thèse sur le combat numérique et la théorie des jeux.

Comment citer cette publication

Anthony Namor, « Le combat cyberélectronique russe en Ukraine », *Le Rubicon*, 8 juillet 2022 [https://lerubicon.org/le-combat-cyberelectronique-russe-en-ukraine/].