Russie-Ukraine : la ligne de front cybernétique ou la guerre sans restriction à l'ère numérique

Stéphane KOCH

Vice-président d'ImmuniWeb SA.

Dans le contexte de la dématérialisation croissante de notre société, le concept de guerre a évolué au-delà du champ de bataille traditionnel. Le numérique a permis aux belligérants et à leurs soutiens d'amener l'exterritorialisation des conflits et leur omnidirectionnalité à niveau encore jamais atteint. Il n'y a plus de distinction entre ce qui est ou n'est pas un champ de bataille. Tout comme il est difficile de définir si un pays qui fait l'objet d'attaques cybernétiques liées à un conflit en cours en devient implicitement un belligérant. L'espace numérique technologique, qui sert de lien entre les espaces naturels et sociaux de notre monde physique et son pendant numérique, est devenu un champ de bataille majeur. Les lieux d'échanges sociaux, la politique, l'économie, la culture et la psychologie sont également autant les armes que la cible d'une guerre cognitive, qui a pour objectif la conquête de notre cerveau.

Cette guerre cognitive se joue, en partie, au niveau de la conquête des opinions, de l'amplification de nos incertitudes, ou encore de la fragilisation du lien de confiance envers les institutions. Quelle que soit notre opinion ou notre religion, nous sommes pris en otages, pris à partie, pris à témoin ou encore désignés coupables. On pourrait penser qu'il suffit de tout éteindre pour se déconnecter d'un conflit… Cela ne sera pas suffisant, la guerre ne s'invite pas que sur nos écrans, que ça soit sur ceux de nos smartphones ou de nos télévisions, mais elle s'invite aussi parfois dans nos rues, où elle vient ancrer sa dimension traumatique, relayée mille fois déjà sur les médias sociaux. On peut se demander si ces prises de position, ces opinions, ces émotions que suscite l'horreur de ces situations que l'on dénonce nous appartiennent vraiment, ou, est-ce que ce sont juste l'aboutissement de stratégies guerrières modernes…

C'est dans cet espace « hors du périmètre physique du conflit » que les adversaires déploient des efforts considérables pour se battre, en utilisant des outils et des tactiques numériques plutôt que des armes traditionnelles. Un thème abordé aussi dans *Unrestricted Warfare*, un ouvrage publié en 1999 par Qiao Liang et

Wang Xiangsui, deux colonels de l'Armée populaire de libération (APL) chinoise, lesquels proposaient des tactiques pour compenser leur infériorité militaire dans une guerre de haute technologie. Les stratégies suggérées dans ce livre comprenaient déjà le piratage de sites Web, le ciblage d'institutions financières, l'utilisation des médias et la conduite d'une guerre urbaine. Bien que l'ouvrage ait fait l'objet de critiques [1], il est intéressant de faire un parallèle entre certaines des idées qui y sont développées et le contexte actuel de l'utilisation des plateformes sociales et des cyberattaques dans le cadre de la guerre que mène la Russie contre l'Ukraine.

Guerre cognitive et stratégie d'influence

Les plateformes sociales sont devenues le nouveau champ de bataille de la guerre de l'information et de la guerre psychologique. Les gouvernements et leurs forces armées, dont leurs « branches cyber » [2] utilisent de plus en plus des « unités d'opérations d'information » et des « unités d'opérations psychologiques » [3] pour influencer l'opinion publique, respectivement la perception d'un conflit et/ou les motivations supposées des belligérants. Sur ce nouveau théâtre d'opérations, les réseaux sociaux servent d'instruments d'influence et de manipulation.

La relation asymétrique qui existe au niveau des réseaux sociaux est un facteur critique dans cette nouvelle forme de guerre. Par exemple, la plateforme chinoise *TikTok* offre (théoriquement) un accès à des milliards de *smartphones* dans le monde. Cependant, les pays occidentaux n'ont pas le même type « d'accès » que la population chinoise, pour qui l'accès aux plateformes sociales américaines est restreint. Il en va de même en Russie. Si on la met en abyme avec les régimes autoritaires, qui interdisent à leurs citoyens d'utiliser des services de réseautage social étrangers, il y a une réelle asymétrie en termes de potentiel d'influence avec les régimes démocratiques où la liberté d'expression permet aux pays non démocratiques d'influencer les opinions occidentales.

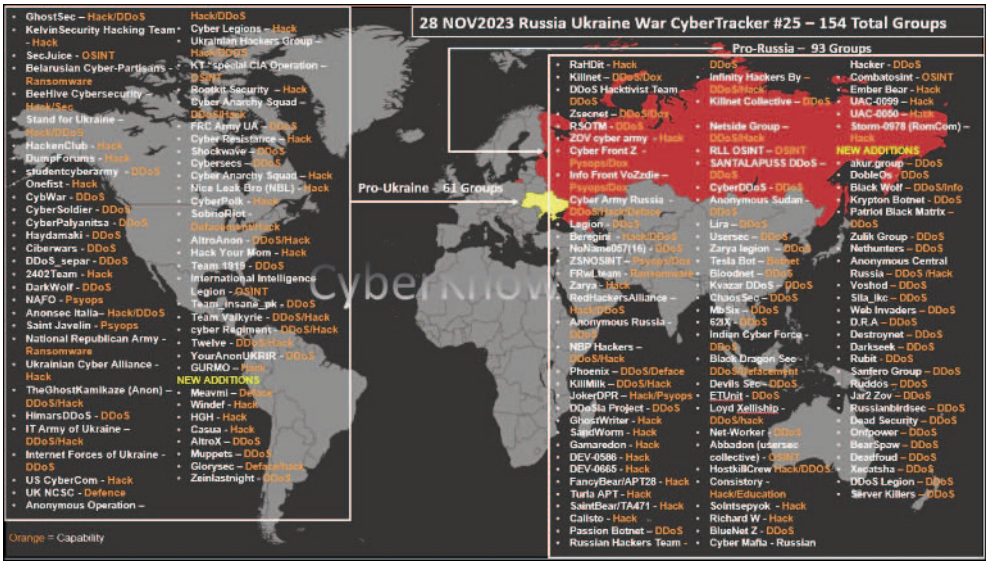
En effet, si les sociétés démocratiques valorisent et protègent la liberté d'expression, cette ouverture peut être exploitée par la Russie pour diffuser de la désinformation et distiller le doute au sein des populations européennes sur le bien-fondé du soutien à l'Ukraine. L'utilisation des plateformes sociales à des fins d'influence et les cyberattaques visant à perturber les services et à instiller la peur représentent un défi de taille pour les sociétés démocratiques.

---

[1] Ho David, « Autour de La guerre hors limites de Qiao Liang et Wang Xiangsui », *La Revue d'histoire militaire (LRHM)*, 16 août 2023 (https://larevuedhistoiremilitaire.fr/).

[2] Voir notamment la liste des forces de cyberguerre étatiques, *Wikipedia* (https://en.wikipedia.org/).

[3] Bradshaw Samantha et Howard Philip N., « The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation », 2019 (https://digitalcommons.unl.edu/).



Update 25. 2023 Russia-Ukraine War — CyberTracker, 28 November 2023 (https://twitter.com/Cyberknow20).

La récente *Opération Doppelgänger* [4] dénoncée par la France est aussi un exemple qui illustre bien cette notion de guerre sans restriction dont l'utilisation du champ informationnel représente un espace de prédilection pour la diffusion de fausses informations. Cette opération de désinformation, qui s'est appuyée dans un premier temps sur de faux sites miroirs de grands médias nationaux ou d'institutions gouvernementales, a visé des médias en France et dans neuf autres pays d'Europe, d'Amérique et du Moyen-Orient. L'objectif était de mener une campagne de désinformation d'ampleur contre l'opinion française. Dans un second temps, l'*Opération Doppelgänger* a visé à la production de dessins animés anti-Zelensky ou de narratifs pro-russes, relayés notamment par des sites aux noms à consonance française. De faux comptes ont été créés sur les réseaux sociaux, principalement Facebook et Twitter (X depuis juillet 2023), pour partager ces fausses informations. La France a accusé des ambassades et des centres culturels russes d'avoir relayé et amplifié cette campagne de désinformation.

Les cyberattaques : la nouvelle arme de prédilection

Les cyberattaques sont devenues un outil courant dans l'arsenal de la guerre sans restriction. Un exemple récent, qui illustre bien le concept, est celui des

[4] « Guerre en Ukraine : ce que l'on sait de l'opération de désinformation russe "*Doppelgänger*" qui a visé la France », *France Info*, 14 juin 2023 (https://www.francetvinfo.fr/).

attaques *DDoS* (attaque par déni de service) contre les sites *Web* du gouvernement suisse et d'autres dans le courant du mois de juin 2023, par un groupe de pirates informatiques Noname057(16) [5]. Pour renforcer sa capacité de nuisance, ce groupe pro-russe parmi les plus actifs dans ce domaine s'appuie sur le *DDosia Project* [6], un modèle de cyberattaque participatif basé sur la mise à disposition d'un logiciel permettant de participer aux attaques par déni de service sans nécessiter de connaissance technique et d'être rémunéré pour sa participation [7]. Le groupe a réussi à rendre inaccessibles au minimum une cinquantaine de sites *Web*, dont ceux du Parlement suisse, du Département militaire (DDPS), de l'Office fédéral de la police (Fedpol), du Département fédéral de justice et police (DFJP), d'administrations cantonales de plusieurs villes, mais aussi des Chemins de fer fédéraux suisses (CFF-SBB), de l'aéroport international de Genève, d'autres aéroports ou aérodromes suisses, ou encore ceux de l'Association des banquiers privés suisses (ABPS), de Genève place financière, et de l'Association suisse des banques (ASB), entre autres. Leurs attaques étant ensuite listées dans leur canal *Telegram* [8]. Ces attaques ont coïncidé avec l'adoption par la Suisse d'un nouveau train de sanctions de l'UE contre la Russie et avec les préparatifs d'un discours vidéo du président ukrainien Volodymyr Zelensky. Le but de ce type d'attaque n'est pas de voler des données, mais de rendre l'accès au service impossible en l'inondant de requêtes (un peu comme si on ajoutait subitement 100 000 voitures sur l'autoroute entre Genève et Lausanne à une heure de pointe).

Outre les attaques *DDoS*, des attaques par *Ransomware* ont également été utilisées pour cibler des entreprises et des organisations gouvernementales suisses. Les attaquants ont publié des données sensibles sur le *Dark web*, dont le caractère stratégique de certaines des données est à même de mettre en danger le modèle économique ou la capacité concurrentielle des entreprises concernées.

Cyberstratégie et asymétrie numérique dans le conflit russo-ukrainien

La guerre actuelle que la Russie mène contre l'Ukraine est un exemple concret de la manière dont le concept de guerre sans restriction peut s'appliquer à l'ère numérique. Les groupes identifiés comme pro-russes sont à l'heure actuelle plus nombreux que ceux identifiés comme groupes pro-ukrainiens, et ils améliorent autant leurs capacités que l'intensité de leurs attaques en dehors des limites du champ militaire opérationnel classique pour, selon toute vraisemblance, répondre à une dynamique du conflit sur son théâtre physique où le gouvernement russe

---

[5] Team Cymru, « Critical Insight: The Hacktivist Operation Targeting NATO and Affiliated Nations: NoName057(16), the pro-Russian hacktivist operator », *Medium*, 13 juin 2023 (https://medium.com/).

[6] Chlumecky Martin, « DDosia Project : How NoName057(16) is trying to improve the efficiency of DDoS attacks », *DECODED Avast.io*, 18 avril 2023 (https://decoded.avast.io/).

[7] Morrison Ryan, « Pro-Russian hacktivist group offers citizens financial rewards to join DDoS attacks », *TechMonitor*, 16 janvier 2023 (https://techmonitor.ai/technology/cybersecurity/noname057-russia-ukraine-hacktivist).

[8] Canal *Telegram* : NoName057(16) fra (https://t.me/s/noname05716eng).

semble peiner à atteindre les objectifs militaires qu'il s'est fixés [9]. Ces groupes se tournent de plus en plus vers la cybercriminalité, avec le soutien implicite et, dans certains cas, opérationnel, du gouvernement russe, ce qui ne peut qu'améliorer encore leurs capacités d'attaque. Fragiliser et affaiblir la dynamique et le potentiel économique d'un pays rentre tout à fait dans le concept de guerre sans restriction.

D'un autre côté, les groupes pro-Ukraine sont moins nombreux, néanmoins l'*IT Army* Ukraine [10] fédère en son sein différents courants et, à ce titre, compte un grand nombre de personnes susceptibles de soutenir l'Ukraine dans des activités hacktivistes ou des cyberattaques. De nombreux groupes affiliés aux *Anonymous* [11] opérèrent aussi en soutien à l'Ukraine dans le cadre de ce conflit sur d'autres cibles, mais ne s'en prennent pas exclusivement à la Russie. Nonobstant, les ressources cybernétiques citées telles que l'*IT Army* Ukraine ou les *Anonymous* n'ont pas, à ma connaissance, vocation à protéger les infrastructures informatiques des pays européens.

Souveraineté numérique et cybersécurité

La prévalence croissante des cyberattaques souligne l'importance de la souveraineté numérique pour toutes les Nations. La souveraineté numérique fait référence à la capacité d'un pays à contrôler son propre espace numérique, y compris ses données, son infrastructure et ses services numériques. Cela inclut la capacité à protéger son espace numérique contre les menaces extérieures, telles que les cyberattaques à large spectre auxquelles nous faisons face actuellement. Être « souverain numériquement » signifie aussi qu'il faut être en mesure de se remettre rapidement des attaques et d'en minimiser l'impact. Ce qui implique l'élaboration d'un plan solide de réponse aux incidents et l'investissement dans les technologies et les compétences en matière de cybersécurité.

Le concept de « *Cloud* souverain » s'inscrit dans cette notion plus large de souveraineté numérique. La cybersécurité nécessite une approche à plusieurs niveaux, combinant des mesures techniques avec des initiatives juridiques, organisationnelles et éducatives. L'importance de cette capacité de résilience face aux cyberattaques qui peuvent être menées contre les infrastructures régaliennes ne semble pas faire partie des considérations, du moins de manière explicite de « l'Étude

---

[9] Jubellin Alexandre, podcast « Partie 1 : Histoire provisoire de la guerre d'Ukraine : une invasion ratée », *Le Collimateur*, 6 juin 2023 (https://podcasts.google.com/).

[10] « Cette armée d'amateurs a été sollicitée par un gouvernement [ukrainien], pour participer à un conflit international, et elle a été rejointe en quelques jours par des centaines de milliers de volontaires ». Protais Marine, « IT Army : l'incroyable armée de hackeurs volontaires pro-Ukraine est-elle vraiment efficace ? », *L'ADN,* 15 mars 2022 (https://www.ladn.eu/tech-a-suivre/it-army-hacktivistes-volontaires-cyberguerre-ukraine/).

[11] Ce groupe organisé de pirates informatiques et d'activistes (« hacktivistes ») se fixe principalement comme objectif de défendre la liberté d'expression. L. Bastien, « Anonymous : tout savoir sur le groupe de hacktivistes », *Le Big Data*, 12 janvier 2024 (https://www.lebigdata.fr/anonymous-hebergeur-dark-web).

d'opportunités pour un *cloud* souverain » [12] parue en mai 2023, sur mandat de la Conférence latine des directrices et directeurs cantonaux du numérique.

Développer autant notre capacité de résilience que notre niveau d'éducation

Le concept de guerre sans restriction a trouvé un nouveau souffle à l'ère numérique. L'utilisation des plateformes sociales pour la guerre cognitive et les cyberattaques comme arme de choix soulignent la nécessité de mesures de cybersécurité solides et d'une bonne maîtrise de l'information. Alors que le champ de bataille continue d'évoluer hors de ses limites physiques, nos stratégies de défense et de résilience doivent elles aussi évoluer. D'autant plus que ce champ de bataille doit être compris aussi par rapport à des enjeux de guerre économique. La guerre actuelle entre la Russie et l'Ukraine nous envoie un signal fort sur les réalités de cette « nouvelle » forme de guerre et la nécessité d'une stratégie proactive (et non juste réactive), d'une adaptation constante face à l'évolution des menaces. L'augmentation des cyberattaques, notamment des attaques *DDoS*, montre clairement que la souveraineté numérique, y compris la notion de « *Cloud* souverain », doit inclure une résilience contre ces types d'attaques. Elle nous rappelle également que la cybersécurité et la lutte contre la désinformation sont des défis complexes qui nécessitent une approche globale et multicouche, dont l'éducation est un des piliers centraux et prioritaires.

À titre d'exemple, l'Estonie a utilisé efficacement l'éducation aux médias comme outil de sécurité nationale pour lutter contre la désinformation [13]. À la suite d'une campagne de désinformation et d'une cyberattaque en 2007, l'Estonie est devenue un *leader* en matière de cybersécurité et a mis en place une éducation aux médias de la maternelle au lycée, avec notamment un cours obligatoire de 35 heures sur les médias et l'influence pour les élèves de 10e année (équivalent de la classe de 2nde en France). L'approche de l'Estonie en matière d'éducation aux médias est globale : elle l'intègre dans différentes matières et laisse aux écoles une certaine marge de manœuvre pour atteindre les normes éducatives nationales.

Tant la littératie [14] numérique, celle touchant à la cybersécurité que celle informationnelle, sont devenues des enjeux démocratiques fondamentaux, tant pour préserver notre démocratie que pour faire des choix démocratiques éclairés sur le futur de la transformation numérique de notre société. ◆

---

[12] Savoy Nicolas, Buchard Anthony, Heiniger Fabian, Mueller Jesko et Vonlanthen Blaise, « Étude d'opportunités pour un *cloud* souverain », 11 mai 2023 (https://cldn.ch/).

[13] Yee Amy, « The country inoculating against disinformation », *BBC*, 31 janvier 2022 (https://www.bbc.com/future/article/20220128-the-country-inoculating-against-disinformation).

[14] NDLR : Aptitude à comprendre et utiliser l'information écrite dans la vie courante, à la maison, au travail et dans la collectivité en vue d'atteindre des buts personnels et d'étendre ses connaissances comme ses capacités.

Mots-clés : Influence, cyberattaque, désinformation, Russie.