diploweb.com La revue géopolitique
ISSN : 2111-4307

Comment l'écosystème cyber ukrainien s'est-il adapté à la guerre ?

vendredi 18 août 2023,par Anastasia KRYVETSKA

Citer cet article / To cite this version :
Anastasia KRYVETSKA, **Comment l'écosystème cyber ukrainien s'est-il adapté à la guerre ?** *, Diploweb.com : la revue géopolitique, 18 août 2023.*

Depuis 2014, le moteur du développement du cyberespace ukrainien est la guerre avec la Russie. Même si les autorités ne sont pas parvenues à agir efficacement dans le cyberespace dès le début du conflit, ce dernier a fait émerger un écosystème cyber qui a su s'adapter au contexte de guerre. Cet écosystème a contribué à la défense du pays à toutes les échelles, tant au niveau des citoyens que des acteurs étatiques et privés. Bien que de très nombreux objectifs doivent encore être atteints, l'invasion de l'Ukraine est un catalyseur pour le développement du cyber, qui est devenu un acteur essentiel du ministère de la Défense. Illustré de trois graphes.

L'UKRAINE est un exemple de la guerre hybride [1] au XXIème siècle. L'expérience acquise pour faire face à la guerre d'agression de la Russie depuis 2014 lui permet aujourd'hui de résister à un Etat dont la superficie est vingt-huit fois supérieure et dont l'armée était supposée être la deuxième au monde. Outre le terrain cinétique, l'Etat ukrainien doit affronter l'ennemi tant dans son espace informationnel [2] que dans le domaine cybernétique [3], terrains qui étaient fréquemment considérés comme secondaires dans un conflit armé de haute intensité. Or, il est tout à fait possible de gagner la guerre sans combattre, comme ce fut le cas pour la Russie en Crimée. Par ailleurs, il convient de ne pas se désintéresser du rôle des diversions et du sabotage cybernétiques, ainsi que du cyber-espionnage, ceux-ci ayant été partie intégrante du conflit. Prises de court par l'absence d'une cybersécurité nationale et d'une politique claire vis-à-vis de la pollution de son infosphère [4], les autorités ukrainiennes ont été amenées à fournir des efforts colossaux dans le domaine du cyber. Néanmoins, l'émergence d'autres acteurs patriotiques a renforcé la capacité de résistance de l'Ukraine.

Ce qui nous conduit à la problématique suivante : **comment l'écosystème cyber ukrainien s'est-il adapté à la guerre depuis 2014 ?**

Cette question sera d'abord abordée en étudiant le domaine cyber comme un moyen de guerre asymétrique, notamment avec l'émergence des « cyber-volontaires » et la mise en lumière des problématiques de cybersécurité en temps de guerre. Ensuite, il conviendra de s'intéresser aux réformes nationales du cyberespace ukrainien qui sont orientés politiquement vers un avenir européen, et dont la mise en place est complexifiée par de multiples acteurs, tels que les fournisseurs d'accès internet et les oligarques pro-russes.

I. Le cyber comme moyen de guerre asymétrique

Considérons successivement La genèse des « cyber-volontaires » ukrainiens (A) ; L'application « Diia » : un exemple d'incompétence ? (B)

A. La genèse des « cyber-volontaires » ukrainiens

Le phénomène que l'on observe aujourd'hui en Ukraine avec la création d'une cyberarmée de volontaires (« *IT-Army of Ukraine* ») ne date pas de l'invasion du 24 février 2022. La genèse de ce type de groupements cyber remonte à la guerre dans le Donbass, dont les effectifs ont été simplement plus modestes. **Que devons-nous entendre par « cyber-volontaire » ?** Il s'agit d'un individu participant volontairement à la défense de son pays par le biais du cyberespace sans contrepartie pécuniaire.

Il peut s'agir tant d'un « simple » citoyen que d'un hacker expérimenté. Généralement, deux catégories sont observées : des formations autonomes regroupant des personnes de tout niveau d'un côté, et de l'autre des groupes de hackers chargés d'effectuer des cyberattaques sophistiquées sur les infrastructures ennemies. Dans le premier cas, les participants suivent les conseils et instructions d'un expert dans le domaine. Par ailleurs, depuis l'invasion de l'Ukraine, les cyber-volontaires ont rendu de très nombreux modes opératoires publics en les publiant sur des sites-web. Lors d'une interview, un des volontaires s'est notamment confié en partageant quelques missions qu'il a réalisées, telles que des attaques de déni de service distribué [5] (DDoS) ainsi que des appels et envois automatisés de messages sur les téléphones des séparatistes dans le but de les rendre hors service.

Quant aux groupes de hackers, ils restent généralement anonymes, notamment par peur de représailles juridiques [6]. Une des exceptions connues est le groupe de hacktivistes [7] **Cyber Alliance Ukrainienne** [8] (« *Ukrainian Cyber Alliance (UCA)* »), ayant travaillé pour les services ukrainiens. Ces derniers s'appuient notamment sur des structures de volontaires dont le but est d'informer et de diffuser des preuves de l'ingérence russe en Ukraine (*InformNapalm*) et les identités des criminels russes ou pro-russes (*Centre Mirotvorets'*). A titre d'exemple, une des cyberattaques réussies par les hackers ukrainiens en 2016 est la pénétration des boîtes mails de Vladislav Sourkov, conseiller du président Poutine, ayant permis de confirmer l'ingérence du Kremlin dans le Donbass.

Néanmoins, ces hacktivistes affirment que « l'ennemi » (les hackers russes) est « comme à la maison » dans les systèmes informatiques de l'Ukraine, où il expérimente différents modes opératoires, en commençant par du cyber-espionnage (« *Uroboros* », 2013) et du vol de données, et finissant par s'attaquer aux infrastructures critiques dans les secteurs stratégiques (« *Black Energy* », 2015). En effet, les hackers critiquent les autorités ukrainiennes, auxquelles ils ne font pas confiance, en les accusant de ne pas prendre assez en considération les problèmes de cybersécurité.

B. L'application « Diia » : un exemple d'incompétence ?

Une des principales cibles de critiques de la part du groupe *UCA* est le ministère de la transformation numérique de l'Ukraine. Fondé pendant le mandat du président Volodymyr Zelenskyi en 2019, ce ministère est chargé de la numérisation des services publics. Aux yeux des experts en cybersécurité, c'est l'application gouvernementale « *Diia [9]* » qui a le plus décrédibilisé cette institution, dont le ministre exagérait le succès. Elle a été l'une des cibles d'une cyberattaque le 13 et 14 janvier 2022, la rendant hors service. Peu après, les membres de la Cyber Alliance auraient trouvé des milliers de données de cette application en vente sur le Darkweb, tandis que les autorités ukrainiennes ont déclaré qu'aucune fuite des données n'avait eu lieu.

Après l'invasion, d'autres hackers ont affirmé que ces données compromises auraient servi aux services de renseignement russes à « trier » la population ukrainienne à des fins de ciblage, en identifiant des activistes sur les territoires occupés. Pourtant les autorités ukrainiennes ont été alertées sur la « dangerosité » de cette application à plusieurs reprises, notamment du fait de sa gestion par une entreprise ayant potentiellement des liens avec la Russie. De plus, aucun rapport d'audit technique n'a été publié par les autorités. Aucun élément ne permet donc d'assurer que le code source ne contient pas de porte dérobée (« *back-door [10]* »), permettant

par exemple aux services de renseignements d'accéder aux données personnelles dans un but de surveillance.

Quand bien même cette application est critiquable, elle a fait ses preuves en matière de confidentialité depuis l'invasion de l'Ukraine. En effet, l'un des services accessibles sur *Diia* permet aux citoyens de géolocaliser et de décrire les déplacements des troupes russes. **Cela permet à l'armée ukrainienne d'avoir un avantage tactique considérable** : connaître les mouvements des troupes ennemies afin de corriger des frappes aériennes ou d'artillerie, et plus généralement d'adapter sa manœuvre en temps réel. Cette application est finalement devenue en temps de guerre un des capteurs importants du renseignement militaire ukrainien.

II. Les réformes nationales du cyberespace

Penchons-nous sur Une stratégie de cybersécurité politiquement orientée (A) puis Une multiplicité d'acteurs (B).

A. Une stratégie de cybersécurité politiquement orientée

Pour la première fois en 2001, le législateur ukrainien a consacré au domaine cybernétique six articles [11] du Code Pénal de l'Ukraine sur la cybercriminalité, que la ratification de la *Convention sur la Cybercriminalité* vient consolider peu après. Cependant, l'Etat ukrainien demeure en retard dans ce domaine. Ce n'est qu'en 2015 qu'une unité de cyberpolice est créée. Les termes de « cybercrime » et « cybercriminalité » sont définis légalement en 2016. Enfin, de réels changements sont amorcés avec l'arrivée au pouvoir du gouvernement de Zelenskyi, notamment avec la création du *Centre national de coordination de la cybersécurité*, sous l'autorité directe du *Conseil national de la sécurité et de la défense de l'Ukraine*.

Ce centre s'inscrit dans l'application de la stratégie ukrainienne de cybersécurité fixée dans le *Décret sur la stratégie de la cybersécurité de l'Ukraine* de 2021. Ce dernier découle de la stratégie plus large de la sécurité et de la défense nationale adoptée par la *Loi sur la sécurité nationale* en 2018. Par ailleurs, avec la révision constitutionnelle de 2019 [12] et l'identification de la Russie comme « *la première source de dangers liée à la cybersécurité ukrainienne* [et internationale] » dans sa stratégie de cybersécurité, l'Etat ukrainien oriente d'autant plus sa politique extérieure vers l'Union européenne.

B. Une multiplicité d'acteurs

1. Les fournisseurs d'accès internet

La mise en œuvre des politiques publiques dans le domaine cyber est rendue difficile en raison des lacunes de l'Etat ukrainien en matière de législation sur le sujet. Or, une législation mise à jour faciliterait la gestion de la multiplicité des acteurs faisant partie de l'écosystème cyber. Il s'agit notamment de prendre en considération le rôle des Fournisseurs d'accès internet (FAI), que les autorités ukrainiennes se voient dans l'obligation de contrôler puisque ceux-ci agissaient de prime abord dans leurs propres-intérêts. Ainsi, deux ans après l'interdiction [13] des services du groupe russe *Mail.ru* [14] ainsi que des réseaux sociaux très populaires dans l'espace post-soviétique *Vk.ru* et *Odnoklassniki*, la moitié des FAI n'avait pas bloqué l'accès

aux sites mentionnés dans le décret. Puis, en 2021, le *Conseil de la défense et de la sécurité de l'Ukraine* ordonne le blocage de 560 sites, appartenant tous au segment russe du cyberespace comme le démontre le graphe [15] « *Les blocages des sites pro-russes dans le cyberespace ukrainien – une lutte contre la propagande* ». Plus précisément :

. les réseaux sociaux (Vk.com, Ok.ru) ;

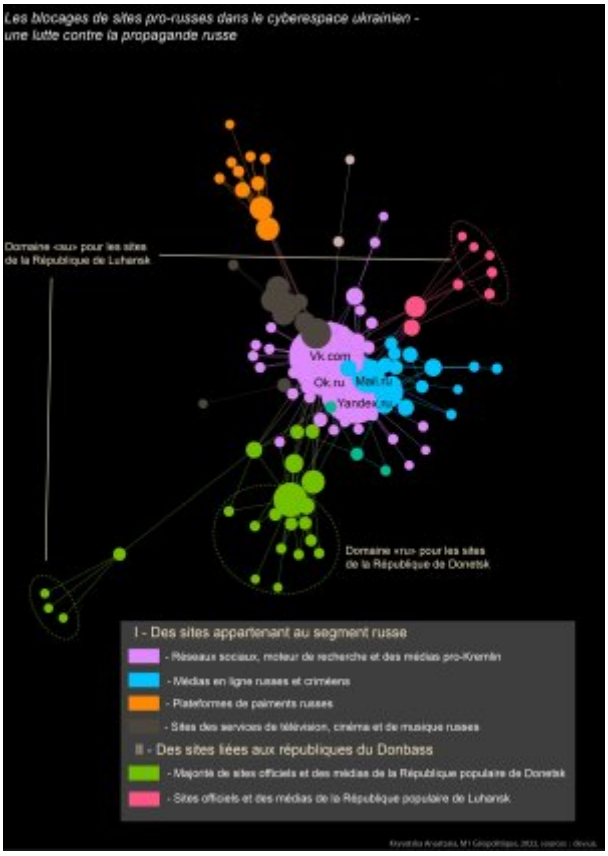
. les médias pro-Kremlin (Ntv.ru, Ria.ru) ;

. les médias pro-séparatistes (Govdnr.ru, Lug-Info.com, Novoross.info) ;

. les médias pro-criméens (Gazetacrimea.ru, Yalta-tv.eu) ;

. les plateformes de paiements russes (Webmoney.ru, Wmtranser.com) ;

. divers services de cinéma et de musique (Domkino.tv, Muz1.tv).



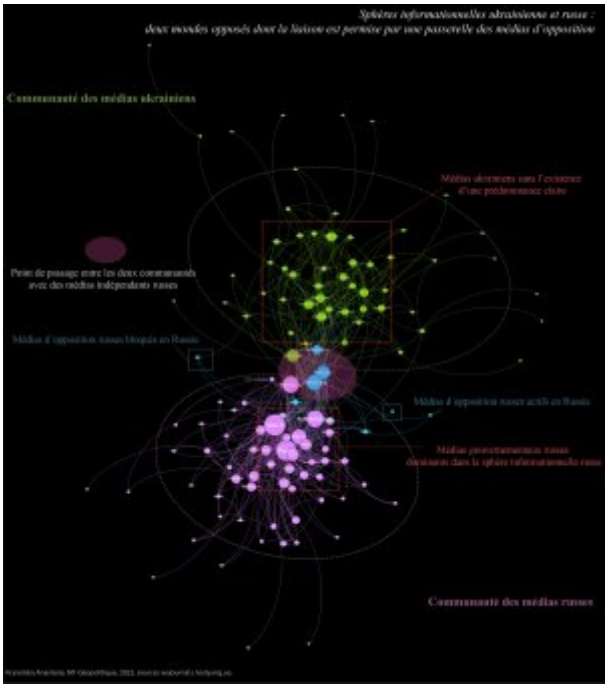
Graphe. Les blocages de sites pro-russes dans le cyberespace ukrainien, une lutte contre la propagande russe

Cliquer sur la vignette pour agrandir le graphe. Conception et réalisation Anastasia Kryvetska *Kryvetska/Diploweb.com*

> Méthode de lecture : les cercles proportionnels appelés nœuds représentent les ressources en ligne (sites web) classées par couleurs selon leur groupe d'appartenance. Ces groupes sont formés par le biais d'un algorithme ayant pour fonction de détecter les différentes

> communautés. Les liens entre les nœuds représentent les liens hypertexte, permettant de passer d'un site web à un autre.

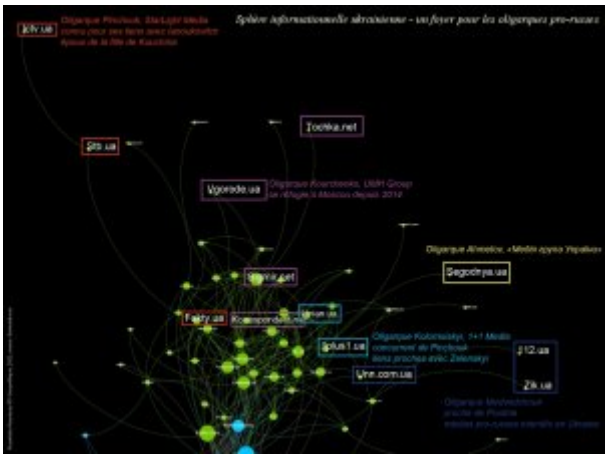
Bien que certains s'opposent à ces blocages par peur que les FAI ne fonctionnent par la suite comme l'organe russe *Roskomnadzor* [16], il s'agit d'abord d'une réelle volonté d'étouffer la propagande diffusée par certains médias appartenant aux oligarques pro-russes et de couper la sphère informationnelle ukrainienne de son homologue russe. Par ailleurs, les sphères informationnelles de l'Ukraine et de la Russie sont connectées majoritairement grâce à l'existence des médias d'opposition russes, comme le représente le graphe [17] *« Sphères informationnelles russe et ukrainienne : deux mondes dont la liaison est permise par une passerelle des médias d'opposition (russes) ».*



Graphe. Sphères informationnelles ukrainienne et russe : deux mondes opposés dont la liaison est permise par une passerelle des médias d'opposition
Cliquer sur la vignette pour agrandir le graphe. Conception et réalisation Anastasia Kryvetska.
Kryvetska/Diploweb.com

2. Les oligarques pro-russes et la sphère informationnelle

Avant l'invasion de l'Ukraine, non seulement les oligarques pro-russes (russes ou ukrainiens) faisaient prospérer leurs affaires sur son territoire, mais ils étaient également très présents dans le secteur médiatique. En effet, ils étaient majoritaires dans l'actionnariat de plusieurs entreprises ukrainiennes de télécommunication ainsi que des chaînes télévisées et des médias en ligne comme l'illustre le graphe « *Sphère informationnelle ukrainienne – un foyer pour les oligarques* ».



Graphe. Sphère informationnelle ukrainienne, un foyer pour les oligarques pro-russes
Cliquer sur la vignette pour agrandir le graphe. Conception et réalisation Anastasia Kryvetska.
Kryvetska/Diploweb.com

Durant le mandat de Zelenskyi, dont l'une des lignes directrices est la lutte contre l'oligarchie, la diffusion des chaînes télévisées détenues par l'oligarque Medvedtchouk, proche de Poutine [18], a été interdite en Ukraine. Celui-ci soutenait également la fédéralisation de l'Ukraine et souhaitait un rapprochement avec la Russie. Par ailleurs, depuis le 24 février 2022, onze partis politiques pro-russes ont été interdits en Ukraine, notamment « *Plateforme d'opposition – Pour la vie* », financé à 57% par des oligarques. Ce parti se positionnait comme « anti-nationaliste » en prêchant pour une résolution du conflit dans le Donbass grâce au respect des accords de Minsk. La politique de l'Etat ukrainien vise donc aujourd'hui une neutralisation de la présence russe dans la sphère informationnelle et dans le domaine des affaires, où les oligarques sont très présents et dont une partie a collaboré avec la Russie.

*****

Depuis 2014, le moteur du développement du cyberespace ukrainien est la guerre avec la Russie. Même si les autorités ne sont pas parvenues à agir efficacement dans le cyberespace dès le début du conflit, ce dernier a fait émerger un écosystème cyber qui a su s'adapter au contexte de guerre. Cet écosystème a contribué à la défense du pays à toutes les échelles, tant au niveau des citoyens que des acteurs étatiques et privés. Bien que de très nombreux objectifs doivent encore être atteints, l'invasion de l'Ukraine est un catalyseur pour le développement du cyber, qui est devenu un acteur essentiel du ministère de la Défense.

Publication initiale le 30 avril 2023

Plus

. Dossier géopolitique : Russie et Ukraine, quelles relations ?

. **AB Pictoris, Un an de guerre en Ukraine. Carte évolutive**
Le 24 février 2022, la Russie relançait son offensive en Ukraine. Un an après, quels ont été les étapes majeures de cette guerre ?

P.-S.

Etudiante à l'Institut Français de Géopolitique (IFG) de l'Université Paris 8, Anastasia Kryvetska est spécialisée dans la géopolitique de l'Ukraine et de la Russie. Ukrainophone et russophone, ses recherches actuelles portent sur les acteurs et les problématiques relatives au domaine du cyberespace ukrainien, sous le prisme de la guerre d'agression russe depuis 2014. Pour toute question relative à ses travaux, elle est joignable à l'adresse email : contact.anastasia protonmail.com

---

Notes

[1] « Un pays peut utiliser des moyens qui portent atteinte à la sécurité et à la stabilité d'un autre pays. Et il ne s'agit pas de moyens militaires, mais, par exemple, de cyber-attaques ou du lancement d'une vague massive de tweets allant à l'encontre de la position d'un gouvernement particulier. C'est ce qu'on appelle la guerre hybride », *BBC News Afrique*. https://www.bbc.com/afrique/monde-60331255

[2] Une des couches du cyberespace, la couche informationnelle, ou cognitive, est le domaine visible de l'Internet avec divers contenus disponibles en ligne (réseaux sociaux, vidéos, photos…). Il convient de noter que la sphère informationnelle est strictement distincte du domaine cybernétique dans la législation ukrainienne.

[3] Domaine entendu à l'échelle des ordinateurs, réseaux et systèmes informatiques. Désigne globalement les couches physique et logique du cyberespace. La couche physique est formée de tous les supports physiques visibles (câbles sous-marins, ordinateurs…). La couche logique sert en quelque sorte de relais entre les deux autres couches ; elle est composée de tous les logiciels et protocoles qui régissent la circulation et l'échange des informations.

[4] Entendu au sens « espace informationnel ».

[5] « Attaque informatique destinée à perturber voire rendre indisponible une ressource Web pour ses utilisateurs légitimes. Elle consiste à inonder la cible de requêtes de connexion afin de surcharger le trafic de telle sorte que le système de soir plus capable de les gérer et se mettre hors service. » Source : Hérodote.

[6] Le 24 mars 2022, les articles 361 et 361-1 ont été révisés, permettant aux spécialistes cyber de rechercher des vulnérabilités au sein les infrastructures gouvernementales.

[7] Contraction des termes « hacker » et « activisme » : un hacktiviste est un « militant numérique » qui organise des opérations d'envergure motivées par des objectifs politiques. *Hacktivisme : vers une complexification des cyberattaques*, Thierry Berthier, Revue Défense

Nationale 2015/9.

[8] Il s'agit de la fusion de deux groupes de hackers, à savoir Trinity et FalconFlames, rejoints plus tard par le groupe RUH8 et quelques membres du groupe CyberHunta. Cette création a eu lieu dans le contexte de la guerre en Ukraine en 2014 afin de former un groupe de cyber-combattants du côté de l'Ukraine.

[9] Confiée au ministère de la transformation numérique, cette application conserve sur un smartphone tous documents officiels ainsi que la signature électronique. Elle permet également l'accès à de multiples services administratifs en ligne, telles que les aides financières ou les demandes de documents officiels.

[10] « Un accès tenu secret vis-à-vis de l'utilisateur légitime aux données contenues dans un logiciel ou sur un matériel », CNIL.

[11] Articles 361, 361-1, 361-2, 362, 363 et 363-1 du Code pénal de l'Ukraine.

[12] Cette révision exige la conformité des politiques intérieures avec les exigences statuées dans les normes de l'Union européenne ou de l'OTAN. Toute loi contraire aux mesures permettant une intégration dans ces institutions est déclarée anticonstitutionnelle.

[13] Décret sur la mise en œuvre des mesures restrictives spéciales, personnelles et économiques (http://3mob.ua/application/news/detail/key/168).

[14] Portail web et un moteur de recherche russe.

[15] Méthode de lecture : les cercles proportionnels appelés nœuds représentent les ressources en ligne (sites web) classées par couleurs selon leur groupe d'appartenance. Ces groupes sont formés par le biais d'un algorithme ayant pour fonction de détecter les différentes communautés. Les liens entre les nœuds représentent les liens hypertexte, permettant de passer d'un site web à un autre.

[16] Organe de la Fédération de Russie chargé de surveiller et de bloquer certains contenus dans la sphère informationnelle. La censure a débuté dans un but de protection des utilisateurs contre le contenu choquant. Puis, avec le temps, les interdictions ont pris une tournure beaucoup plus politique.

[17] Op.cit. méthode de lecture.

[18] Poutine est le parrain d'une des filles de Medvedtchouk.