Photo by Markus SPISKE on Unsplash

LES PUBLICATIONS

Capacités offensives cyber : quels objectifs pour les services de renseignement russes ?

[DOSSIER] LES CAHIERS DU COMITÉ ASIE N°19

Par Adrien BENRABIA

LES JEUNES IHEDN

À PROPOS DE L'ARTICLE

La Russie se positionne comme un acteur incontournable du cyberespace. Les services de renseignement russes usent d'armes cybernétiques afin de servir leurs objectifs régionaux et internationaux. Cet article discute des moyens de ces services via l'étude de certains cas récents et essaie d'entrevoir l'évolution d'utilisation des cyber armes par le renseignement russe.

À PROPOS DE L'AUTEUR

Adrien BENRABIA est étudiant en Master 2 GSI à l'Institut Catholique de Paris. Passionné de géopolitique et de cybersécurité, il participe à l'activité des Jeunes IHEDN depuis septembre 2020 au sein du comité Asie.

Capacités offensives cyber : quels objectifs pour les services de renseignement russes ?

L'implication des services de renseignement russe à travers les affaires Skripa[1] puis Navalny[2] a suscité le vif intérêt des observateurs internationaux. Si ces deux attaques ont fait l'objet d'utilisation d'agents chimiques, les services de renseignement russes s'illustrent depuis maintenant plusieurs années par l'emploi de capacités cyber offensives, dont la technicité a également rapidement évolué.

La Russie, via ses services de renseignement, aurait employé des armes cybernétiques lors de l'attaque des systèmes d'information estonien en 2007[3], puis en appui aux attaques conventionnelles contre la Géorgie en 2008[4]. Dans ces deux cas, on peut déjà observer une évolution des modus operandi employés par les services de renseignements russes, qui se sont adaptés à leurs adversaires comme l'ont amèrement constaté les Etats-Unis lors des élections présidentielles de 2016[5]. Cet article pose ainsi la question de la manière dont ces capacités offensives cyber peuvent servir aux services de renseignement russes afin de « sécuriser » les frontières occidentales de la Russie et servir son agenda géopolitique international.

Dans une volonté projectiviste propre au thème de cette nouvelle édition des Cahiers du Comité Asie 2021, cet article a comme objectif en premier lieu d'établir des relations entre les acteurs des capacités d'attaques russes en matière cybernétique. En second lieu, cet article entreprend également d'expliquer le schéma des modes d'action offensifs cyber russes en tentant de définir de potentielles cibles pour ses services de renseignement. La notion d'action offensive comprend toute action menée par une organisation contre une ou plusieurs autres afin de nuire à son intégrité à court, moyen ou long terme (reconnaissance, intrusion, attaque

1 R. (2019, 1er juillet). Bellingcat : Top GRU Officer Coordinated Skripal Attack From London. RadioFreeEurope/RadioLiberty. https://www.rferl.org/a/skripal-novichok-poisoning-attack-gru-officer-sergeyev-bellingcat-report/30029474.html.

2 B.I. (2020, 17 décembre). FSB Team of Chemical Weapon Experts Implicated in Alexey Navalny Novichok Poisoning. Bellingcat. https://www.bellingcat.com/news/uk-and-europe/2020/12/14/fsb-team-of-chemical-weapon-experts-implicated-in-alexey-navalny-novichok-poisoning/.

3 Rain Ottis, Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

4 Gotsiridze, A. G. (2019). The Cyber Dimension of the 2008 Russia-Georgia War. GFSIS. https://www.gfsis.org/blog/view/970.

5 Lipton, E., Sanger, D. E., & Shane, S. (2020, 19 octobre). The Perfect Weapon : How Russian Cyberpower Invaded the U.S. The New York Times. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

directe). La question des limites capacitaires de Moscou dans un cyberespace en cours de régulation se pose dans une dernière partie, mettant en perspective ces éléments dans le cadre d'une croissance anarchique des capacités cybernétiques dans les conflits actuels.

Guerre et état des forces cybernétiques du renseignement russe

L'armée russe aurait pris conscience de l'importance de repasser sur une stratégie de guerre hybride à la suite des Printemps Arabes (2010-2012) et du conflit en Ukraine (2014). Les gradés Chekinov et Gerasimov[6] insistent en effet sur la nécessité pour l'armée nationale de s'adapter au caractère changeant de la guerre, allant jusqu'à souligner la primauté des mesures non-militaires dans les conflits à venir7, comme ont pu le confirmer les événements en Estonie. Ce caractère changeant est notamment dû à l'emploi de mesures non militaires dans les actions de guerre.

Les changements révélés dans les documents de doctrine stratégiques russes abondent ainsi dans ce sens8. La mise en œuvre intégrée de mesures militaires, politiques, économiques et informationnelles sont des facteurs prépondérants des conflits actuels et illustrent ce tournant dans la perception russe de la guerre moderne avec le concept de guerre non linéaire

Cette perception de l'utilité de la guerre non linéaire n'est cependant pas nouvelle, au même titre que l'usage de méthodes de renseignement technique par la Russie. Le terme « cybersécurité » est principalement employé par l'Occident et se réfère à la sécurité des systèmes d'information. La Russie préfère la terminologie de « sécurité de l'information », comme composante de la guerre de l'information. La guerre de l'information est définie par les officiels russes comme la combinaison de la technique, liée à la sécurité d'un système d'information et de la psychologie qui implique l'influence d'individus[9].

Les capacités cyber offensives russes prennent racine au sein des services de renseignement dont les opérations, notamment extérieures, favorisent l'utilisation. Le renseignement en Russie se décompose en trois organisations majeures : le services de sécurité intérieur (le FSB), le

[6] Respectivement colonel de réserve et général de l'armée russe.
[7] Lilly, B. (2020, 22 octobre). *The Past, Present, and Future of Russia's Cyber Strategy and Forces*. RAND. https://www.rand.org/pubs/external_publications/EP68319.html.
[8] Thomas, T. T. (2018, juin). *Russia's Forms and Methods of Military Operation : The Implementers of Concepts*. Army University Press. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2018/Russias-Forms-and-Methods-of-Military-Operations/.
[9] *Ibid*.

service de sécurité extérieur (le SVR) et le renseignement militaire (le GRU). Le FSB pris la place du KGB à la suite de la chute de l'URSS en 1991[10]. Ce sont les premières opérations du FSB qui ont permis la naissance du programme militaire cyber russe. Le développement des capacités américaines en la matière, avec l'officialisation de la création du Cyber Command en 2009 et la découverte du malware Stuxnet en 2009-2010, ont forcé la main de Moscou qui a elle-même poursuivi le développement de ses capacités cybernétiques militaires. En 2013, l'armée russe entame ainsi sa première campagne officielle de recrutement d'ingénieurs avec l'emphase mise sur les opérations cyber, l'intelligence du signal et la guerre électronique. Seule la section informatique fut l'apanage exclusif du GRU. Depuis lors, le GRU s'est vu attribuer une part importante des cyber-attaques de grande échelle par les Etats occidentaux.

On trouve une constellation d'acteurs liés plus ou moins directement aux services de renseignement et le gouvernement russe. En termes d'influence, les organes médiatiques Sputnik ou encore Russia Today s'assurent de relayer une vision pro-russe de l'actualité, couplés à l'activité de *think tanks* tels que l'Internet Research Agency (IRA)[11]. Concernant les capacités cyber, des groupes de hackers aux compétences spécifiques gravitent autour des actions offensives associées aux services de renseignement. On retrouve dans cette catégorie à la fois des groupes de pirates chevronnés dont les liens avec le GRU et le SVR semblent se préciser, comme c'est le cas par exemple pour le groupe APT29[12]. Cette catégorie abrite également un public de hackers « patriotes », qui lorsqu'ils sont sollicités comme ce fut le cas lors de la guerre en Géorgie (2008)[13], participent aux attaques préparées par des organismes proches des institutions russes.

[10] Berg, E. (2020, 26 mars). Livre – Les Services secrets russes, des tsars à Poutine. Conflits. https://www.revueconflits.com/vladimir-poutine-russie-fsb-services-secrets-eugene-berg/.
[11] Rapin, A. (2020, 27 août). *Cyber, désinformation et subversion : nouveaux outils de la puissance russe*. Aerion24. https://www.areion24.news/2020/08/27/cyber-desinformation-et-subversion-nouveaux-outils-de-la-puissance-russe/.
[12] Reevell, P. (2020, 16 juillet). What to know about the Russia-linked hackers accused of stealing COVID vaccine data. ABC News. https://abcnews.go.com/International/russia-linked-hackers-accused-stealing-covid-vaccine-data/story?id=71819152.
[13] Shnygina, A. S. (2018, 7 août). It's our time to serve the Motherland. How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers. Meduza. https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland.

Les objectifs et les modes d'action de Moscou

Les modes d'actions des services de renseignement russes varient en fonction de l'objectif à atteindre. On peut également constater que ces modes d'actions ont gagné en technicité opération après opération. De ce fait, l'opération par déni de service distribué (DDoS) qu'a connu l'Estonie n'est en rien comparable aux récents *modi operandi* employés en 2016 lors de l'élection américaine, et plus récemment lors des révélations sur le malware Sunburst[14]. Au-delà de l'intérêt spécifique que l'on pourrait porter à chacun de ces cas, il semble intéressant de poser les questions de pourquoi cette modalité d'attaque et pourquoi spécifiquement ces cibles. Concernant le cas estonien, et partant de l'hypothèse que les attaques à l'encontre de l'Etat balte proviennent bien de la Russie, il semblerait qu'il faille associer cette attaque à une volonté russe de « taper fort », en employant une méthode dévoilant une intensité jamais vue, face à un pays frontalier dont les ambitions otaniennes entraient en conflit avec les intérêts géopolitiques de Moscou. En outre, il s'agit faire respecter la puissance de l'Ours dans une région qu'il considère comme son pré-carré.

Les élections américaines de 2016 illustrent la perspective russe de guerre hybride. Durant la période des élections, l'IRA aurait utilisé 50 258 comptes Twitter[15] dirigés par des bots afin de relayer des tweets en faveur de Donald TRUMP. Ce *think tank* financé par l'oligarque[16] Evgeni Prigojine[17] opère en parallèle d'opérations similaires fomentées par le FSB et le GRU, selon les enquêtes réalisées par le Sénat américain[18]. Cet exemple démontre une forme d'interconnexion entre les acteurs du cyberespace russe, leur permettant de coordonner leurs efforts et de combiner leurs savoirs faire. Deux intérêts peuvent transparaitre de cette opération. D'une part, influencer l'élection d'un candidat favorable aux intérêts de Moscou. D'autre part, démontrer

[14] Manens, F. (2021, 3 février). *SolarWind : l'opération de cyberespionnage massive en cache une autre*. Cyberguerre. https://cyberguerre.numerama.com/10076-solarwinds-loperation-de-cyberespionnage-massive-en-cache-une-autre.html.
[15] Twitter. (2018, janvier). *Update on Twitter's review of the 2016 US election*. Twitter. https://blog.twitter.com/en_us/topics/company/2018/2016-election-update.html.
[16] Il est également intéressant de noter les liens étroits de cet oligarque avec l'entreprise de sécurité privée Wagner avec laquelle il aurait travaillé en tant que contractuel.
[17] Neil MacFarquhar, « *Yevgeny Prigozhin, Russian Oligarch Indicted by U.S., Is Known as 'Putin's Coo'* ». New York Times, February 16, 2018. https://www.nytimes.com/2018/02/16/world/europe/prigozhin-russia-indictment-mueller.html.
[18] United States Senate. (2019). *Russian active measures, campaigns and interference in the 2016 U.S. election* (volume 2). https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

aux Etats-Unis que la Russie dispose elle aussi des moyens d'influencer des élections comme les Américains l'ont eux-mêmes réalisé par le passé[19].

Limites capacitaires et cadre juridique

Bien que des tentatives aient émergé afin de réguler le cyberespace, il s'agit encore d'un monde où prime une certaine anarchie du fait notamment de l'incapacité des instances internationales à trouver un cadre normatif commun[20]. Le manuel de Tallin[21], mandaté par l'OTAN, au même titre que les tentatives russes et chinoises de proposer un cadre normatif au cyberespace, notamment en matière d'encadrement des dispositifs offensifs, ne semblent pas voués à aboutir, que ce soit à court ou à moyen terme.

De ce fait, les récentes opérations russes sur ses frontières Ouest, en Moldavie, en Ukraine ou encore en Pologne, sont autant de signaux faibles indiquant de potentiels cibles pour les services de renseignement russes et leurs organes médiatiques. La région russophone de Transnistrie située en Moldavie bénéficie ainsi d'une large autonomie vis-à-vis du pouvoir central. Cette région accueille ainsi depuis 1992 des troupes russes sur son territoire. En 2014, les discussions d'association de la Moldavie avec l'OTAN[22], sous l'impulsion de l'ex-président américain Barack Obama, ont provoqué des avertissements de la part de Moscou. Le concept de cybersécurité étant en cours de développement en Moldavie[23], la mise en œuvre de stratégie et de plans d'action est de fait sujette à une certaine fragilité.

***

[19] Jones, O. (2018, 9 février). *Americans can spot election meddling because they've been doing it for years*. The Guardian. https://www.theguardian.com/commentisfree/2017/jan/05/americans-spot-election-meddling-doing-years-vladimir-putin-donald-trump.

[20] Cheravitch, J. (2020, 23 décembre). *Russia's Cyber Limitations in Personnel Recruitment and Innovation, Their Potential Impact on Future Operations and How NATO and Its Members Can Respond*. RAND. https://www.rand.org/pubs/external_publications/EP68400.html.

[21] Étude académique menée par Michael N. Schmitt du *Naval War College* formalisée dans un manuel définissant la façon dont le droit international pourrait s'appliquer au cyberespace.

[22] *Vu de Moldavie. Plan de l'OTAN : le pire cauchemar de Poutine*. (2014, 8 septembre). Courrier international. https://www.courrierinternational.com/article/2014/09/08/plan-de-l-otan-le-pire-cauchemar-de-poutine.

[23] Conseil de l'Europe. (2021, 19 mars). *CyberEast : Table ronde sur les politiques et plans d'action en matière de cybercriminalité et de cybersécurité avec les autorités moldaves*. Conseil de l'Europe - Cybercriminalité. https://www.coe.int/fr/web/cybercrime/-/cybereast-roundtable-discussion-on-cybercrime-and-cybersecurity-policies-and-action-plans-with-moldovan-authorities.

Il semble ainsi probable que l'évolution de l'utilisation des capacités cyber par les services de renseignements russes se fera en adéquation avec la culture de chaque service. Si ce constat peut paraitre trivial, la prééminence supposée du GRU dans les dernières attaques associées à la Russie témoigne d'une volonté d'attitude offensive à l'encontre, non-seulement des adversaires de la Russie, mais également des anciens pays satellites de l'URSS. Lorsqu'il s'agit du cyberespace, la difficulté d'identification des protagonistes d'une attaque ne permet pas de réaliser une analyse exhaustive de l'outil capacitaire d'une organisation disposant de moyens financiers et humains quasiment illimités.

Selon une étude publiée par la China Cyber Policy Initiative en 2020[24], la Russie se classerait 4ème dans la liste des pays disposant des cyberarmées les plus développées[25]. S'appuyant sur des capacités offensives éprouvées, la Russie dispose de capacités défensives d'isolation, s'alignant ainsi sur les standards d'autres pays autoritaires. Ces dernières années, la mise en place d'un internet souverain a été l'un des centres de dépenses de la Russie. Au même titre que l'Iran et la Chine, la Russie a passé avec succès les derniers tests de déploiement d'un réseau internet national, c'est-à-dire un réseau capable d'isoler le pays de l'internet extérieur et de fonctionner en vase clos. Moscou a ainsi intégré toute l'importance d'une maitrise exhaustive du cyberespace. Les services de renseignement russes et leurs réseaux apportent une capacité d'attaque des plus efficaces à Moscou, qui, combinée à des possibilités défensives restrictives, font de la Russie un acteur central des futures conflits liés au cyberespace.

[24] J. Voo., I. Hemani, S. Jones, W. DeSombre (2020), N*ational Cyber Power Index, Methodology and Analytical Considerations.* https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf.
[25] Ð. (2017, 9 janvier). *Аналитики оценили количество хакеров на госслужбе*. Kommersant. https://www.kommersant.ru/doc/3187320.

publication@jeunes-ihedn.org