Lettre mensuelle – Novembre 2020 – Disponible sur omc.ceis.eu

Table des matières

ANALYSES (1/2)

Le *persistent engagement* : vers une cyberdéfense plus offensive des États-Unis ?

***Article réalisé au profit du Commandement de la cyberdéfense*.**

Créé en 2010, l'United States Cyber Command (USCYBERCOM) s'est initialement développé autour d'une approche réactive et défensive. Le concept d'*active defense* (2011), qui cantonnait ses cyber-opérations offensives à la défense des réseaux du département de la Défense (DoD) et au soutien des opérations militaires, s'est révélée inadapté à la fréquence et la sophistication accrues des cyberattaques[1].

Les États-Unis ont été la cible de plusieurs cyber-opérations d'envergure au cours des dernières années. Parmi lesquelles, les vols de données de l'Office of Personnel Management[2] (2013), Anthem Inc.[3] (2014) et United Airlines[4] (2015), qui n'ont pas fait l'objet de représailles américaines car situées en dessous du seuil de l'agression armé. Ces attaques ont pourtant pu avoir des implications importantes car les assaillants ont été en mesure de collecter des informations sensibles sur certains responsables américains.

Dans ce contexte, l'ingérence russe dans les élections présidentielles américaines de 2016 a été décisive dans l'infléchissement stratégique de l'USCYBERCOM. Arrivé à sa tête en 2018, le désormais général d'armée (GA) Paul Nakasone s'est inscrit en rupture de la doctrine *d'active defense*, en proposant une posture plus proactive et offensive. Son approche fait écho à la *National Security Strategy* (NSS-2017) de l'administration Trump qui, outre la désignation d'adversaires de la Maison-Blanche dans le monde (Chine, Russie, Corée du Nord, Iran et le terrorisme djihadiste), fait état d'une compétition susceptible de bouleverser l'équilibre stratégique international en faveur des États-Unis[5].

Selon le GA Nakasone, l'inaction inhérente à la posture réactive et défensive promue par le concept d'*active defense* présente des risques face aux efforts adverses qui se poursuivront sans relâche. La question n'est plus de savoir s'il faut agir mais comment[6]. La stratégie cyber du DoD de 2018 appelle à cet égard à contrer les menaces à leur source via le concept de *defense forward*. Il s'agit de prévenir, vaincre ou dissuader les cyber-activités malveillantes qui visent les infrastructures critiques, qu'elles aient un impact ou non sur les capacités militaires[7]. Le *defense forward* est une forme d'application dans le cyberespace du principe, reconnu par les États-Unis, de légitime défense préventive et préemptive.

Dans le cadre du *defense forward*, le GA Nakasone a conceptualisé dans divers articles la persévérance et la confrontation continue (*persistent engagement*), qui doit permettre d'augmenter la sécurité nationale et de conforter la supériorité stratégique des États-Unis dans le monde. Partant du principe que les États sont en

[1] Paul Nakasone, « How to Compete in Cyberspace », *Foreign Affairs* [en ligne], 25 août 2020.
[2] Josh Fruhlinger, « The OPM hack explained », *CSO* [en ligne], 12 février 2020.
[3] M. McGee, « Anthem Cyberattack Indictment Provides Defense Lessons », *Bank Info Security* [en ligne], 13 mai 2019.
[4] « United Airlines data breached by China-backed hackers: Bloomberg », *Reuters* [en ligne], 29 juillet 2015.
[5] The White House, *National Security Strategy*, Décembre 2017, pp. 2-3.
[6] Op. cit. Paul Nakasone, *Foreign Affairs*, 2020.
[7] US Departement of Defense, *Cyber Strategy (Summary)*, 2018, p. 2.

contact permanent avec leurs adversaires dans le cyberespace, leur défense y est déterminée par « *la façon dont ils se donnent les moyens d'agir et agissent* ». Pour le général Nakasone :

> Agir « *implique d'opérer en dehors de ses propres frontières, d'être en dehors de ses propres réseaux, pour s'assurer de comprendre ce que les adversaires font. Un État a perdu l'initiative et l'avantage dès lors qu'il se retrouve à défendre à l'intérieur de ses propres réseaux*[8] ».

En d'autres termes, le *persistent engagement* traduit la nécessité de reprendre l'initiative, en affirmant la supériorité opérationnelle américaine par la conduite préventive et continue de cyber-opérations offensives contre les adversaires, dans le but d'affecter leurs capacités d'action et les empêcher ainsi d'atteindre leurs objectifs. Ce concept, en affirmant la supériorité opérationnelle américaine, a vocation à dissuader le potentiel adverse. Les États-Unis mettent l'accent sur la collecte de renseignements et sur les opérations dans les réseaux étrangers, afin de découvrir et de contrer les menaces avant qu'elles n'atteignent les réseaux nationaux et nuisent aux intérêts américains.

L'USCYBERCOM adopte avec le *persistent engagement* une posture plus proactive, voire assumée, qui est susceptible d'avoir des impacts sur les tiers concernés (partenaire, allié, neutre et adversaire) et sur la régulation de la conflictualité dans le cyberespace.

1. Une posture davantage proactive pour contrer les cybermenaces à leur source

Conformément au *defense forward*, le *persistent engagement* nécessite de collecter du renseignement à l'étranger afin de partager des *indications & warning* (I&W), qui permettront au gouvernement américain (USG) de renforcer sa cybersécurité et aux entreprises privées d'améliorer leurs solutions[9].

1.1. Une restructuration des dispositifs nationaux de la cyberdéfense américaine

Pour le GA Nakasone, la répartition des efforts de l'USCYBERCOM dans le cadre du *persistent engagement* est la suivante : deux-tiers doivent être consacrés à doter les entités liées à l'USG et le secteur privé de moyens d'agir et un tiers au renforcement de sa propre capacité d'action[10]. La coopération avec le public et le privé est cruciale. Alors que le périmètre de l'USCYBERCOM chevauche celui de la NSA ou du département de la Sécurité intérieure (DHS), le rôle d'animation de l'écosystème cyber lui permet de se distinguer, en plus d'accroître ses ressources, son prestige et son autonomie[11]. En se plaçant au cœur de la cyberdéfense nationale, l'USCYBERCOM confirme sa montée en puissance.

À cet égard, la sécurisation des élections de mi-mandat (2018) illustre la façon dont le commandement a permis à d'autres entités gouvernementales d'agir. Le *Russia Small Group*, un groupe de travail destiné à contrer les cyberattaques de la Russie contre les États-Unis, a permis à l'USCYBERCOM et à la NSA de partager leurs informations au FBI et au DHS, qui ont ainsi été en mesure d'empêcher une interférence dans le processus démocratique. Au niveau technique, l'USCYBERCOM a investi dans des plateformes de partage

[8] « An Interview with Paul M. Nakasone », *Joint Force Quarterly*, n°92, 2019, p. 7.
[9] US Departement of Defense, *Cyber Strategy (Summary)*, 2018, p. 2.
[10] *Op. cit.* « An Interview with Paul M. Nakasone », *JFQ*, 2019, p. 6.
[11] Stéphane Taillat, « Cyber opérations offensives et réaffirmation de l'hégémonie américaine : une analyse critique de la doctrine de Persistent Engagement », *Géopolitique de la datasphère*, Hérodote, n°177-178, 2020, p. 321.

d'informations entre les gouvernements fédéraux, étatiques et locaux, dans des domaines très variés. Par exemple, la norme de signalisation des évacuations médicales (9-line) a permis de rationaliser l'ensemble des interventions de la National Guard sur tout le territoire américain[12].

Comme le secteur privé est désormais à l'origine de la plupart des innovations technologiques, la recherche de partenariats est indispensable à l'amélioration de la défense collective et à l'obtention d'informations sur les menaces. Avec la création de l'incubateur DreamPort[13], l'USCYBERCOM s'est doté d'un lieu dédié entre autres à l'organisation de réunions non classifiées avec des entités non affiliées à l'USG. Outre le recueil de bonnes pratiques, DreamPort accueille des stagiaires qui alimentent l'innovation cyber[14]. Néanmoins, le GA Nakasone s'est pour le moment peu appesanti sur la manière d'associer l'industrie, parfois encore réticente à coopérer avec la puissance publique. Alors que des entreprises regrettent que le partage d'informations avec l'USG soit à sens unique[15], celles qui recherchent des parts de marché à l'étranger peuvent être réticentes d'avoir une réputation de travailler avec le DoD[16].

1.2. Une affirmation de la capacité à agir dans les réseaux étrangers

Dans son *Command Vision* de 2018, l'USCYBERCOM indique qu'il opérera désormais « *à l'échelle mondiale de manière transparente et continue* » et non plus régionalement ou ponctuellement. Le document insiste sur la « supériorité par la persévérance » (*superiority through persistence*), qui vise à conserver l'initiative en confrontant les adversaires en permanence et partout où ils manœuvrent[17].

> Le département de la Défense (DoD) fragmente le cyberespace en trois groupes[18] :
>
> - « bleu », qui englobe le réseau du DoD, la partie du cyberespace protégée par les États-Unis et les portions à défendre dans le cadre d'opérations (celles des alliés) ;
> - « rouge », qui désigne les portions contrôlées par des nœuds adverses ;
> - « gris », qui regroupe les portions qui ne sont ni « bleues », ni « rouges », donc tout le cyberespace qui n'est contrôlé ni par les États-Unis, ni par leurs adversaires.

S'exprimant sur les cyber-opérations au *Joint Force Quarterly*, le GA Nakasone a écrit :

> « *Si nous ne faisons que défendre dans le cyberespace bleu, nous avons échoué. Nous devons au contraire manœuvrer de manière transparente dans l'espace mondial interconnecté de combat, aussi près que possible des adversaires et de leurs opérations, et le modeler en permanence pour nous créer un avantage opérationnel, tout en le déniant aux adversaires*[19] ».

---

[12] Op. cit. Paul Nakasone, *Foreign Affairs*, 2020.
[13] « L'innovation en défense cyber : le modèle américain », *OMC* [en ligne], 4 novembre 2019.
[14] Op. cit. Paul Nakasone, *Foreign Affairs*, 2020.
[15] « Key Private and Public Cyber Expectations Need to Be Consistently Addressed », *GAO* [en ligne], 15 juillet 2010.
[16] Joshua Rovner, « More Aggressive and Less Ambitious: Cyber Command's Evolving Approach », *War on the Rocks* [en ligne], 14 septembre 2020.
[17] « Achieve and Maintain Cyberspace Superiority », *Command Vision for US Cyber Command*, 2018, p. 6.
[18] Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12, 8 juin 2018, pp. I-(4-5).
[19] Paul Nakasone, « A Cyber Force for Persistent Operations », *Joint Forces Quarterly*, n°92, 2019, pp. 12-13.

Les ambitions de l'USCYBERCOM dans ces différents espaces n'est pas clair, notamment s'il cherche à créer des tensions dans le cyberespace rouge ou à rivaliser avec ses adversaires en prenant le contrôle du cyberespace gris. Il en ressort que ses activités ont vocation, dans les deux cas, à dépasser les réseaux nationaux des États-Unis. Si l'USCYBERCOM cherche à opérer uniquement dans le cyberespace rouge, ses opérations seront *de facto* de plus en plus mondiales à mesure que les adversaires étendront leurs nœuds de réseaux. S'il ne souhaite agir que dans le cyberespace gris, cela implique qu'il prenne le contrôle d'infrastructures neutres vis-à-vis de l'adversaire[20].

Les États-Unis agissent ainsi en « observateur » sur les réseaux d'un pays partenaire pour y recueillir des renseignements sur les activités adverses[21]. Ils peuvent également y agir en tant que « passant », en y transitant dans le but d'affecter les systèmes et les réseaux des adversaires. Lors de l'opération Glowing Symphony (2016), l'USCYBERCOM a notamment agi, dans le cadre d'une coalition alliée, dans des réseaux allemands pour y supprimer un serveur qui hébergeait des contenus de propagande de l'État islamique[22].

La diplomatie est alors indispensable pour apaiser les inquiétudes des partenaires des États-Unis qui craignent que ces derniers utilisent le *persistent engagement* pour agir sans autorisation dans leurs réseaux. Pour obtenir leur consentement, le GA Nakasone a conceptualisé le *hunt forward*, par lequel des équipes américaines se rendent dans des pays partenaires pour travailler conjointement sur des menaces communes. L'USCYBERCOM partage ensuite ses conclusions aux acteurs américains compétents. Outre l'Ukraine et la Macédoine, les États-Unis ont effectué une mission de ce type au Monténégro (2019) afin de préparer la sécurisation des élections présidentielles américaines de 2020[23]. Depuis son adhésion à l'OTAN, le pays fait en effet l'objet d'un harcèlement régulier de la Russie.

Certains partenaires étrangers peuvent malgré tout rester réfractaires à l'idée de laisser leurs réseaux devenir un théâtre d'affrontement entre pays-tiers. Même s'ils rejoignent les États-Unis sur la nature des cybermenaces, ils peuvent être réticents au *hunt forward* pour des questions de souveraineté[24].

2. De nouvelles règles du jeu dans la régulation de la conflictualité dans le cyberespace ?

Susceptibles d'alimenter l'instabilité mondiale, les cyber-opérations offensives menées dans le cadre du *persistent engagement* pourraient à terme placer les États-Unis en porte-à-faux vis-à-vis des positions qu'ils adoptent dans les instances internationales sur la stabilité du cyberespace.

2.1. L'utilisation de cyberattaques pour façonner les comportements adverses

L'administration Trump considère le cyberespace comme un milieu dans lequel ses adversaires sont déterminés à agir contre les intérêts américains. La tâche de l'USCYBERCOM est de les contrer et non plus de les influencer. Le statut des cyber-opérations offensives a été clarifié dans ce sens par une loi d'autorisation

[20] Max Smeets, *U.S. Cyber strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection*, Center for Security Studies, ETH Zurich, 15 février 2020, pp. 3-4.
[21] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Oxford, 2017.
[22] Ellen Nakashima, « US Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate Over Alerting Allies », *The Washington Post* [en ligne], 9 mai 2017.
[23] G. Graff, « The Man Who Speaks Softly – and Commands a Big Cyber Army », *Wired* [en ligne], 13 octobre 2020.
[24] *Op. cit.* Joshua Rovner, 2020.

de la Défense nationale (2018), qui autorise le DoD à prendre des mesures proportionnelles et appropriées afin de « perturber, défaire et dissuader » les opérations de la Russie, la Chine, la Corée du Nord et l'Iran[25]. En deux ans sous le GA Nakasone, l'USCYBERCOM a certainement conduit plus de cyber-opérations offensives que lors du reste de son histoire. Trois ont notamment été rendues publiques avec celles qui ont ciblé l'Internet Research Agency[26] (Russie), l'Iran[27] et le botnet Trickbot[28].

Agir en tant que « passant » dans des réseaux de pays tiers pour affecter les systèmes d'adversaires soulève également un une interrogation quant à la légalité. Bien que le DoD revendique une application du droit international au cyberspace, du moins de son interprétation américaine, de telles opérations pourraient aller à l'encontre de la Charte des Nations Unies et du principe de souveraineté.

2.2. Vers un abandon pragmatique de la dissuasion dans le cyberespace ?

Selon le *Command Vision* de 2018 de l'USCYBERCOM, les actions continues (*persistent action*) permettent à terme d'influencer les calculs adverses, de dissuader les agressions, ainsi que de clarifier la distinction entre les comportements acceptables ou pas dans le cyberespace[29]. Néanmoins, selon Richard Harknett, spécialiste de la dissuasion, agir contre l'agresseur ne consiste pas à modifier en amont les calculs de ce dernier mais à endommager immédiatement ses systèmes et ses réseaux. Il s'agit de marquer le seuil de ce qui est acceptable et de façonner ainsi le comportement de l'adversaire[30].

Cette approche est reprise par le GA Nakasone qui apparaît maintenant plus modeste sur la capacité de l'USCYBERCOM à influencer en amont d'autres acteurs. Le mot « dissuasion » n'apparaît plus dans ses dernières interventions relatives au *persistent engagement*. Plutôt que d'essayer de changer le comportement de ses adversaires, l'USCYBERCOM cherche désormais à réduire l'efficacité de leurs cyber-capacités. En effet, il considère que la coercition via des cyber-opérations ponctuelles ne peut défaire les adversaires et que seule une confrontation continue peut les empêcher d'atteindre leurs objectifs dans le temps[31]. Selon cette vision, des cyberattaques préventives et régulières permettraient de diminuer l'intensité et la fréquence des attaques adverses. Cette possibilité d'agir de manière préemptive donnerait ainsi aux États-Unis une liberté d'action qui peut être utilisée pour nuire aux adversaires[32].

Certains observateurs craignent toutefois que cette posture ne contribue au contraire à augmenter la conflictualité et les risques d'escalade en renforçant le dilemme de sécurité[33]. Face au *persistent engagement* des États-Unis, les conceptions chinoise et russe d'un Internet national et souverain pourraient par exemple considérer les actions offensives américaines comme une forme d'ingérence non acceptable. Pour autant, les opérations menées dans le cadre du *persistent engagement* pourraient également créer des précédents susceptibles de remplacer les normes de comportements responsables, aujourd'hui acceptées par une grande majorité, dans la régulation du cyberespace.

---

[25] 115e Congrès, 2018, sec. 1642.
[26] A. Greenberg, « US Hackers' Strike on Russian Trolls Sends a Message », *Wired* [en ligne], 27 février 2019.
[27] J. Barnes, T. Gibbons-Neff, « U.S. Carried Out Cyberattacks on Iran », *New York Times* [en ligne], 22 juin 2019.
[28] « Report: U.S. Cyber Command Behind Trickbot Tricks », *KrebsonSecurity* [en ligne], 10 octobre 2020.
[29] « Achieve and Maintain Cyberspace Superiority », *Command Vision for US Cyber Command*, 2018, p. 6.
[30] R. Harknett, « Deterrence is not a credible strategy for cyberspace », *Orbis*, vol. 61, 2017, pp. 299-444.
[31] Op. cit. Paul Nakasone, *Foreign Affairs*, 2020.
[32] *Op. cit.* Stéphane Taillat, 2020, p. 316.
[33] *Op. cit.* Joshua Rovner, 2020.

L'USCYBERCOM a par ailleurs admis l'idée que ces normes internationales étaient régulièrement ignorées par ses adversaires, qui ont montré qu'ils n'avaient aucun intérêt à les respecter. Dans ce cadre, le commandement estime qu'empêcher les adversaires belliqueux d'agir, en affectant de manière continue leurs cyber-capacités, ne peut que contribuer à la stabilité du cyberespace[34].

Comme le souligne Stéphane Taillat, maître de conférences à l'École de Saint-Cyr Coëtquidan, « *l'activisme américain court donc le risque d'affaiblir les normes partagées obtenues par consensus au profit de normes fondées au mieux sur un consensus limité aux seuls États 'occidentaux' et au pire sur le recours aux opérations offensives sans freins évidemment ou immédiatement perceptibles*[35] ». Cet activisme se poursuivra-t-il sous la future administration Biden ?

ANALYSES (2/2)

L'affirmation de la cyber-puissance russe

Début 2020, la Géorgie a accusé le GRU, le service de renseignement militaire russe, d'être à l'origine de la cyberattaque massive qui a touché 15 000 sites Internet géorgiens, dont celui de la présidence, en octobre 2019. Les sites touchés ont été « défigurés » : ils affichaient une photo de l'ex-président géorgien Mikhaïl Saakachvili, inculpé pour corruption en 2013, accompagnée de l'inscription « *I'll be back* »[36]. Fin 2019, un rapport publié par la société Check Point Software Technologies a par ailleurs affirmé que des entités soutenues par l'État russe auraient investi dans le développement d'importantes capacités de cyber-espionnage, ce qui, selon la société, « *constitue[rait] un investissement sans précédent de la Russie dans le cyberespace offensif* »[37].

Ces événements récents soulèvent des questions sur la stratégie qui sous-tend les actions russes dans le cyberespace et, surtout, sur l'implication de l'État dans ces opérations. La conduite d'opérations cyber et informationnelles s'inscrit en Russie dans une conception particulière du cyberespace et de la cybersécurité, qui s'appuie sur le continuum espace informationnel et cyberespace. Si la Russie est accusée de mener des opérations offensives, les textes et doctrines officiels ne font toutefois état que d'une stratégie défensive, ce qui lui permet de présenter ses activités dans le cyberespace comme des actions de défense de ses intérêts face à un Occident agressif. Depuis le début des années 2010, la Russie opère ainsi un virage vers la professionnalisation et la structuration de ces capacités.

1. La Russie « cyber-ennemi » numéro un ?

Si la Chine était l'agresseur le plus redouté dans le cyberespace dans les années 2000, un basculement s'est opéré à la fin de la décennie, portant la Russie au rang de « cyber-ennemi » numéro un. Depuis, la Russie est régulièrement mise en cause dans des cyberattaques massives et parfois spectaculaires.

---

[34] *Ibid*.
[35] *Op. cit.* Stéphane Taillat, 2020, p. 326.
[36] https://www.rfi.fr/fr/europe/20200220-géorgie-alliés-occidentaux-accusent-gru-russe-cyberattaque
[37] *The Past, Present, and Future of Russia's Cyber Strategy and Forces*, RAND Corporation, 2020

La première cyberattaque de grande ampleur attribuée à la Russie est l'attaque massive contre l'Estonie en 2007, visant un grand nombre d'institutions publiques et privées, dont le gouvernement et les banques, et paralysant le pays pendant 48h. Bien qu'il n'y ait aucune preuve tangible de la participation de l'État russe à l'attaque, celle-ci servait ses orientations géopolitiques et politiques puisqu'elle est intervenue après la décision du gouvernement estonien de déboulonner le soldat de bronze de Tallinn, une statue dédiée aux libérateurs soviétiques de la Seconde guerre mondiale. Le second événement cyber majeur dans lequel la Russie a été mise en cause est la guerre en Géorgie en 2008. Plusieurs sites Internet gouvernementaux ont été rendu inaccessibles dès le début du conflit. Dans les deux cas, les cyberattaquants ont utilisé un *botnet* (réseau de machines infectées pouvant être utilisées pour des attaques informatiques), pour mener un grand nombre d'attaques DDoS (déni de service), paralysant complètement l'accès aux sites attaqués. Autres exemples emblématiques, une cyberattaque similaire menée en 2014 contre l'Ukraine pendant l'annexion de la Crimée ou encore la cyberattaque contre la Géorgie en 2020.

Pirates, mercenaires, soutenus ou non par Moscou… l'origine des cyberattaques dont la Russie est soupçonnée est floue, bien que les motivations soient souvent ouvertement nationalistes (affirmation du nationalisme russe) et font pencher pour un soutien de l'État à ces opérations. Les cyberattaques contre l'Estonie, la Géorgie et l'Ukraine sont caractéristiques d'opérations défendant les intérêts russes dans les anciennes Républiques soviétiques et pouvant avoir été soutenues par l'État.

Plusieurs d'entre elles ont d'ailleurs été explicitement attribuées à la Russie par des pays occidentaux, posture essentiellement politique puisque l'attribution « technique » est difficile. Le 30 juillet dernier (2020), l'Union européenne a même, pour la première fois, sanctionné quatre ressortissants russes ainsi que le GRU, accusés d'avoir participé et coordonné la cyberattaque ayant visé l'OIAC (Organisation pour l'interdiction des armes chimiques) en 2018, deux cyberattaques survenues à l'encontre du réseau électrique ukrainien en 2015 et 2016, ou encore la cyberattaque du Bundestag allemand en 2015. Il s'agit de mesures restrictives à l'encore de ces individus et entités, comprenant l'interdiction de pénétrer sur le territoire de l'UE, un gel des avoirs, et l'interdiction faite aux personnes et entités de l'UE de mettre des fonds à leur disposition.

Les opérations cyber, outils de la guerre de l'information

Au cours des dernières années, la conceptualisation de la guerre en Russie a peu à peu évolué pour intégrer des moyens non militaires à côté des moyens armés traditionnels. Preuve en est l'importance croissante que la doctrine russe accorde au concept de « guerre de l'information », de plus en plus souvent présentée comme faisant partie intégrante des conflits modernes. La doctrine ne fait toutefois aucune mention des capacités cyber-offensives de la Russie, dont la posture officielle dans le cyberespace est purement défensive.

La stratégie russe sous-tendant les cyberattaques s'appuie sur la vision russe d'un continuum entre cyberespace et espace informationnel, qui constituent deux domaines poreux qui s'entremêlent : la cybersécurité est en effet perçue comme une notion occidentale, tandis que le terme dédié en russe est « sécurité de l'information » (*informatsionnaya bezopastnost*). Dans la *Information Security Doctrine* russe de 2016, le terme « cyber » n'est d'ailleurs jamais utilisé – même dans la version anglaise –, tout comme « cyberespace », auquel est préféré le terme « sphère informationnelle ».

La stratégie cyber russe est ainsi intrinsèquement liée à sa stratégie de guerre de l'information, et en est même une composante. On en retrouve des éléments explicits dans la Doctrine Gerasimov[38] de 2014 : il s'agit d'utiliser les techniques traditionnelles de subversion et de désinformation afin de désorganiser et de semer la confusion chez l'ennemi. La stratégie russe est dans ce domaine celle des vases communicants : les campagnes de désinformation menées par des *trolls* russes s'accompagnent souvent de cyberattaques, et vice-versa, comme cela a été le cas pendant l'élection présidentielle américaine de 2016. La Russie est en effet accusée d'avoir orchestrée une vaste campagne de désinformation (utilisation de faux comptes sur les réseaux sociaux, achat de publicités, etc.) et de cyberattaques (vol et publication d'emails de responsables démocrates) afin de perturber le scrutin.

2. Vers une utilisation offensive et assumée de l'arme cyber ?

Bien que la posture officielle de la Russie soit défensive, le rôle des « cyberarmes » offensives dans la vision russe du conflit est régulièrement analysé dans les revues militaires russes. Le rapport *The Past, Present, and Future of Russia's Cyber Strategy and Forces*, publié par la RAND Corporation en 2020, fait le point sur les avantages que représentent les capacités offensives selon les écrits militaires théoriques russes[39] :

Des capacités polyvalentes :

- Les opérations cyber offensives permettent d'infliger des dommages à l'adversaire en temps de paix et sans déclarer la guerre, depuis n'importe où, et en affaiblissant les capacités de défense de l'adversaire ;
- En plus d'effets purement technologiques, les cyberattaques sont également en mesure de désorganiser les institutions étatiques et militaires, démoraliser la population et créer des mouvements de panique.

Des capacités efficaces :

- Les opérations cyber offensives sont favorisées par le flou juridique en la matière sur le plan international (les cyberattaquants ne sont pas nécessairement poursuivis, et encore faut-il les identifier) ;
- L'utilisation d'armes cyber offensives doit permettre d'atteindre la « suprématie informationnelle » sans pour autant avoir à traverser les frontières ou à établir une présence physique sur le territoire de l'adversaire ;
- Les opérations cyber-offensives sont des actions asymétriques pouvant permettre à un État faible économiquement et technologiquement à neutraliser un adversaire beaucoup plus puissant ;
- Plus le niveau d'automatisation des objets et des process cibles est élevé, plus les résultats d'une cyberattaque sont importants.

Des capacités abordables :

- Les armes cyber offensives présentent un coût moindre pour des dommages comparables à ceux des armes traditionnelles : une étude menée en 2012 par des universitaires russes avait conclu que les

[38] La Doctrine Gerasimov est un terme non officiel qui fait référence aux propos du général Valery Gerasimov, chef d'Etat-major des forces armées russes, dans lesquels il prône, en réponse à la « guerre hybride » américaine, une stratégie d'emploi coordonné des moyens de toute nature (psychologiques, informationnels, économiques, techniques, technologiques, militaires…).

[39] *The Past, Present, and Future of Russia's Cyber Strategy and Forces*, RAND Corporation, 2020

infrastructures informatiques des États-Unis et de la Russie pouvaient être rendues totalement dysfonctionnelles par seulement 600 cyberattaquants entraînés pendant 2 ans pour un coût n'excédant pas $100 millions.

Le rapport de la RAND Corporation suggère que ces éléments, ainsi que des concepts tels que le « *Defend forward* » du Cyber Command américain (2018), pourraient inciter la Russie à s'aligner sur la stratégie américaine et à inclure un volet relatif à l'usage offensif des armes cyber dans son *Information Security Doctrine*. Toutefois, la posture officiellement défensive adoptée par la Russie présente l'avantage de lui permettre de nier toute responsabilité dans des cyberattaques offensives et d'utiliser le narratif d'une défense nécessaire face aux pays occidentaux agressifs.

La stratégie américaine « *Defend Forward* » (« arrêter la menace avant qu'elle n'atteigne sa cible ») a été conceptualisée par l'US Cyber Command en 2018 en réponse aux menaces cyber qui pèsent contre les États-Unis, notamment d'origine russes, chinoises, nord-coréennes et iraniennes.

3. Renforcement des capacités : monté en compétence et professionnalisation

Les acteurs et agences impliqués dans les cyberopérations russes ont évolué en même temps que la perception des menaces générées par les technologies de l'information. Dans *The Past, Present, and Future of Russia's Cyber Strategy and Forces*, la RAND dresse une chronologie de la montée en puissance du rôle de l'État russe dans le recrutement des « cybercombattants » (pirates, trolls…) et dans la conduite des opérations cyber.

Au début des années 2000, le FSB (service fédéral de sécurité), principal successeur du KGB, recrutait des hackers et spécialistes indépendants pour mener des cyberattaques, ce qui lui a permis de contourner le manque de capital humain en la matière. La Russie souffre en effet depuis de nombreuses années d'une importante fuite des cerveaux, qui a conduit au manque de savoir-faire nécessaires au développement d'un écosystème numérique consistant. Cela explique entre autres la faiblesse de la Russie dans les domaines matériel et logiciel, ainsi que la nécessité de recourir à des mercenaires. A titre d'exemple, la cyberattaque emblématique contre l'Estonie en 2007 aurait été menée par un groupe hétérogène de pirates recrutés pour l'occasion et soutenus par l'État.

Dans les années 2000, la question d'un programme cyber militaire n'était pas à l'ordre du jour puisque les opérations menées discrètement par le FSB portaient leurs fruits. Un changement s'est opéré au début des années 2010, l'un des facteurs étant la création du Cyber Command de l'armée américaine en 2009, qui a commencé à creuser un fossé entre les ambitions et les capacités cybernétiques russes et américaines. En 2013, le ministre russe de la Défense, Sergueï Choïgou, a ainsi lancé une vaste campagne de recrutement de programmeurs afin de créer des « unités scientifiques militaires » (*voennye nauchnye roty*). La mission de ces unités est de faire progresser la recherche militaire en matière de cyberopérations et de guerre électronique. En 2014, une « force de cyber opérations » (*voyska informatsionnykh operatsiy*) a été créée et la doctrine militaire publiée la même année présentait le « *développement des forces et des moyens de confrontation de l'information* » comme une priorité pour la modernisation de l'armée russe. Le développement des capacités cyber-russes s'est donc structuré autour d'entités dédiées et de personnel recruté à cet effet.

Les 20 dernières années ont ainsi vu s'établir un nouvel équilibre dans le cyberespace avec l'affirmation de la cyber-puissance russe. La Russie assume aujourd'hui ses ambitions cybernétiques grâce à la structuration et

à la militarisation progressive de ses capacités cyber aux côtés de ses capacités de guerre de l'information, qu'elle utilise souvent de concert. Si l'attribution des cyberattaques n'est pas certaine, il est évident que les opérations cyber imputées à la Russie servent aujourd'hui ses intérêts et renforcent la conflictualité entre la Russie, les États-Unis et la Chine dans le cyberespace.

FOCUS INNOVATION

Moabi : l'audit by design

Présentation

Moabi est une start-up fondée en 2019 qui propose une solution de reverse engineering automatisée permettant non seulement de détecter les failles de logiciels, systèmes d'exploitation et firmwares mais aussi de proposer des mesures correctrices. Ses principaux secteurs d'application comprennent l'aéronautique, la défense, la sécurité et l'industrie, les objets connectés, notamment les véhicules connectés (drones, voitures, trains, satellites…) et les robots et automates industriels.

Les solutions

La solution de Moabi répond à deux enjeux : les risques résultant de la prolifération des objets connectés d'une part, et la nécessité de prendre en compte la sécurité dès la conception des produits (security by design) d'autre part.

Elle permet de mesurer, contrôler et renforcer la sécurité des logiciels et des objets connectés tout au long du cycle de développement d'un produit (conception, développement, intégration et maintenance) de façon automatisée et sans avoir besoin d'accéder aux codes sources. Sa particularité est qu'elle prend aussi bien en compte les langages utilisés par les sous-traitants pour développer leurs logiciels que les solutions de compilation mises en œuvre avant mise en production.

Le déploiement de cette solution peut prendre trois formes :

- En mode Saas, sur le cloud ;
- Sur un serveur déployé chez le client pouvant être connecté à internet de manière ponctuelle afin de faire les mises à jour (du logiciel, des bases de données et de l'OS) ;
- Sur un serveur déployé chez le client, sans aucune connexion internet, avec un protocole de mise à jour spécifique (qui répondre aux exigences spécifiques du domaine de la Défense).

Moabi se positionne ainsi en alternative aux outils d'analyses et de tests de code source dont l'impact peut être limité, et aux tests d'intrusion et analyses de sécurité manuelles souvent plus couteuses (pentests), effectués plus tardivement et ne permettant pas de tester tous les binaires (codes compilés) d'un logiciel. La solution de Moabi a donc vocation à identifier et proposer les corrections des vulnérabilités et tous points à risques avant la commercialisation des produits.

MOABI analyse chaque binaire à l'aune de 5 critères :

- La défense en profondeur (le durcissement) : évaluation des mécanismes de défense contre les vecteurs d'attaques courants ;
- La dette Technique : évaluation de la chaine de compilation et de l'architecture (compatibilité avec les systèmes d'exploitation, détection d'obsolescence etc.) ;
- La conformité : évaluation du respect des standards et bonnes pratiques ;
- La cryptographie : évaluation de la robustesse du chiffrement en identifiant les algorithmes de cryptographie utilisés (2300 répertoriés) et les fonctions de chiffrement (1200 connues) ;
- La vulnérabilité : détection des classes de vulnérabilité connues à partir du CVE (base de données maintenu par le département de la sécurité intérieur américain) et recherche de failles "0days".

Ces 5 critères sont agrégés dans une métrique globale appelée « surface de défense ». Ils permettent ainsi d'évaluer le niveau de cybersécurité de logiciels internes et externes, et de comparer des versions, ou des fournisseurs, sur la base de métriques stables et cohérentes. La solution de Moabi permet ainsi aux entreprises de réaliser un contrôle dans le temps de la qualité des prestations de ses fournisseurs, sur la base d'une norme de qualité commune.

Moabi accompagne ensuite les entreprises dans l'exploitation de ces rapports, afin qu'elles puissent en extraire les informations essentielles. La société travaille d'ailleurs sur la mise en place d'indicateurs clés de performance (KPI) pour chaque métrique, qui pourraient être modulables en fonction des politiques de sécurité de chaque entreprise (exigences de niveau de cryptographie, de robustesse des mécanismes de défense, etc.).

Applications

Les secteurs d'applications des solutions de Moabi comprennent :

- La Sécurité des logiciels des véhicules connectés (GPS, contrôle du moteur, communication, etc.) : 70 à 90% du code provient de fournisseurs et est intégré directement au produit. Il est important d'imposer des objectifs de sécurité communs aux fournisseurs et d'être en mesure de les mesurer directement sur du binaire.
- La transition vers l'IoT : l'augmentation du périmètre à défendre du fait de la connexion des chaines de production impose de travailler directement sur des firmwares binaires (automates industriels, capteurs, robots).
- Le secteur de la Défense : problématique cruciale d'intégration de codes venant de fournisseurs dont la maturité en termes de cybersécurité est très variable.

CALENDRIER

« Fake news » et manipulations de l'information : la démocratie en péril ? (15-16-17/12/2020)

Les fake news, et plus largement les manipulations de l'information, ont déjà démontré les dommages qu'elles pouvaient infliger aux Etats et aux systèmes démocratiques : déstabilisation des processus électoraux, fragilisation d'acteurs industriels et économiques, sans compter la pression sur les dispositifs étatiques de cyberdéfense chargés de s'en prémunir.

Dans un contexte politique et géopolitique de plus en plus tendu, marqué par la multiplication des campagnes et attaques informationnelles sur le plan international, par la sophistication grandissante des technologies de la désinformation et par la diversification des vecteurs de diffusion, quelles peuvent être les réponses, technologiques, politiques et sociétales, aux manipulations de l'information ?

Le forum se déroulera en 3 webinars indépendants de deux heures :

Atelier 1 - le mardi 15 décembre de 09h00 - 11h00

Fake news et manipulations de l'information, la prochaine épidémie ?

Les manipulations de l'information ne sont pas un phénomène nouveau, mais connaissent dans ce contexte de crise un regain particulier. Désinformation, mésinformation, propagation de rumeurs, fake news, etc constituent aujourd'hui une réelle menace pour les systèmes démocratiques. Quels sont les facteurs, structurels ou conjoncturels, qui expliquent la tendance à « l'infodémie » et permettent aux manipulations de l'information de prospérer ? Quelles évolutions peut-on prévoir, à court et moyen terme, à la fois sur la forme, le périmètre, et l'intensité des manipulations d'information ?

Atelier 2 - le mercredi 16 décembre de 09h00 - 11h00

Fake news et manipulations de l'information : La technologie, alliée ou ennemie ?

Qu'il s'agisse de propagande dite blanche (assumée), grise (sites conspirationnistes...) ou noire (utilisation de trolls et de bots), les manipulations exploitent un large éventail de méthodes et techniques de conception, de falsification et d'amplification. Mais la technologie constitue aussi un allié de taille dans la lutte contre les manipulations de l'information : outils de reconnaissance faciale, d'analyse des mouvements, de détection des altérations de l'image... sont eux aussi de plus en plus efficaces. Mais la réponse peut-elle être uniquement technologique ?

Atelier 3 - le jeudi 17 décembre de 09h00 - 11h00

La lutte contre les manipulations de l'information, quel rôle pour les États ?

La lutte contre les manipulations de l'information est désormais une priorité politique dans les États démocratiques. Les initiatives étatiques et inter-étatiques de toutes natures se multiplient : régulation des plateformes numériques et des médias, campagnes de sensibilisation et éducation, recours "fact checking", analyse technique…Quelles sont aujourd'hui les priorités politiques en matière de lutte contre les

manipulations d'information ? Quel peut-être l'apport et le rôle du secteur privé ? Quelle(s) coopérations(s) au niveau européen, international ?

Inscrivez-vous en cliquant ici. Pour plus d'informations, merci de contacter Amélie Rives (arives@ceis.eu).

ACTUALITÉ

L'association France Cyber Maritime voit le jour à Brest

Le Secrétariat général de la Mer (SGMer) a officialisé le 23 novembre la création de France Cyber Maritime. Fruit d'un travail conjoint entre « *les pouvoirs publics, les acteurs territoriaux et les filières* [cyber, maritime et portuaire] », cette association, présidée par Frédéric Moncany de Saint-Aignan (Cluster maritime français), fait suite à la décision en 2018 du Comité interministériel de la mer de structurer une réponse au risque cyber dans le secteur maritime. Ce dernier est de plus en plus exposé aux cybermenaces du fait de la numérisation accrue des navires et des ports, ainsi que du développement des drones et des navires autonomes.

France Cyber Maritime aura pour missions de créer :

- Un Maritime Computer Emergency Response Team (M-CERT), qui centralisera et coordonnera les cyber-incidents dans les secteurs maritime et portuaire. Ce CERT sectoriel vise également à favoriser le partage d'information entre les acteurs compétents afin de mieux anticiper les cybermenaces émergentes ;
- un centre national de coordination de la cybersécurité pour le monde maritime à l'horizon 2022.

En étroite coordination avec l'ANSSI et le SGMer, l'association vise également à développer l'écosystème national de la cybersécurité maritime. Pour son président, la fédération de tous les acteurs du monde maritime et de la cybersécurité, ainsi que des façades maritimes nationales, est cruciale pour soutenir « *cette forte ambition au service de secteurs stratégiques pour la souveraineté et l'économie françaises* ». France Cyber Maritime bénéficie d'ores-et-déjà du concours de plusieurs entités telles que Diateam, ENSTA Bretagne, Institut Mines-Télécom, Naval Group, Thales et Yes We Hack.

La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

À ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique (OMC)**, qui s'inscrit dans le contrat-cadre n°2018-02. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction générale des relations internationales et de la stratégie
60 boulevard du général Martial Valin | 75015 Paris

CEIS
Tour Montparnasse | 33 avenue du Maine | 75015 Paris
E-mail : omc@ceis.eu