Lettre n°42 - **septembre 2015** - **disponible sur omc.ceis.eu**

"Overall, the United States is the strongest country in terms of cyber-strength. China is the world's biggest country in terms of the number of web users. (…) We have broad common interests but we need to strengthen cooperation and avoid confrontation, and nor should we politicise this issue."
Déclaration de Xi Jinping, président de la République populaire de Chine faite le 25 septembre 2015 lors d'un sommet avec le président Obama.

Table des matières

LES RELATIONS TRANSFRONTALIERES ET LES INFRASTRUCTURES CRITIQUES

La frontière est souvent définie comme « *ce qui permet de circonscrire un ensemble spatial donné, une région, une construction sociale et politique* »[1]. Une frontière terrestre établit des limites de territoire ; au-delà de ce dernier, ce ne sont pas les mêmes lois qui s'appliquent, ni la même souveraineté qui s'exerce. Dans le cyberespace, l'idée même de frontière se révèle floue et ambiguë, car elle diffère selon les couches matérielles, logiques, sémantiques.

Sur la couche matérielle, le concept de frontières est susceptible de s'appliquer : les différents équipements, tels que les routeurs, les serveurs ou les points d'interconnexion réseaux sont hébergés dans un lieu physique, où une juridiction nationale s'applique. Ils sont localisables et cartographiables. Des pays comme la Chine ou la Russie affichent une volonté de contrôle de leur cyberespace national à travers une maitrise des équipements, comme en témoigne notamment le Grand Firewall de Chine.

Sur la couche logique, constituée des données, il n'existe pas de frontières : la donnée ne « sait » pas quand elle passe d'un pays à un autre, elle ne « connaît » pas l'idée de juridiction. Il existe néanmoins des règles, définies par les protocoles d'échanges et les codages, permettant une interopérabilité de toutes ces données.

Sur la couche sémantique, enfin, relative au contenu informationnel, certains Etats, parmi lesquels la Chine, affichent une volonté très forte de mettre en place une « frontière » du contenu de l'information, euphémisme souvent utilisé pour cacher la censure sur les nouveaux supports numériques.

Le cyberespace possède donc des frontières d'un point de vue technique, dont s'affranchissent les données, ce qui n'est pas sans poser un casse-tête aux Etats cherchant à maintenir une souveraineté de l'information sur leur territoire.

Selon Bernard Reitel et Patricia Zander[2], « *le passage du frontalier au transfrontalier renvoie à l'idée que le lien l'emporte sur la séparation et que des échanges structurés, organisés et durables s'effectuent sur de courtes distances de part et d'autre de la frontière (distincts des échanges transnationaux)* ».

Les relations transfrontalières permettent de renforcer des collaborations économiques et technologiques structurées et durables dans différents domaines : énergie, transports, communication, finance, médias, etc. Pour ce dernier secteur, l'affaire du piratage de la chaîne de télévision internationale francophone TV5 Monde en avril 2015 représente un bon exemple des impacts transnationaux d'une cyberattaque.

Cet article étudie les impacts de ces relations transfrontalières sur les infrastructures critiques.

[1] http://books.openedition.org/pufr/2396?lang=fr

[2] http://www.hypergeo.eu/spip.php?article207

Le cas européen

De nombreux pays sont dépendants des infrastructures critiques étrangères, comme pour la fourniture d'énergie ou les systèmes d'informations et de communications.

Parmi les Etats membres de l'UE, seuls trois ont pris en compte ces dépendances transfrontalières dans leur législation[3] : l'Espagne, l'Estonie et la Hongrie. Ces Etats ont mis en place des obligations juridiques spécifiques pour évaluer et réduire les dépendances transfrontalières des infrastructures d'information critiques. En Estonie, par exemple, les fournisseurs de services vitaux sont tenus par la loi d'assurer la continuité de service d'une manière et par des moyens qui ne dépendent pas des systèmes d'information situés dans des pays étrangers. Par ailleurs, les fournisseurs de services vitaux sont tenus d'effectuer une analyse des risques sur la continuité de services qui prenne en compte également les risques informatiques.

Par ailleurs, d'autres gouvernements abordent la question de la protection des infrastructures critiques transfrontalières dans le cadre de leur réflexion stratégique. En Allemagne, par exemple, la stratégie nationale pour la protection des infrastructures critiques[4] précise l'importance d'une coopération internationale sur la partie transfrontalière.

Cependant, la plupart des pays européens ne prennent pas en compte la problématique dans leurs textes officiels.

En 2009, la Commission européenne a publié sa politique sur la protection des infrastructures[5]. Bruxelles concluait à l'époque que les approches nationales sur le sujet étaient disparates et non coordonnées. La Commission européenne a donc proposé différentes mesures afin de faciliter la collaboration entre les pays, avec un plan d'action visant à renforcer la coopération sur les plans tactique et opérationnel au niveau européen : nouveau modèle européen de gouvernance pour les infrastructures d'information critiques, ateliers conjoints des différents CERT gouvernementaux, etc.

En 2006, la Commission européenne a lancé le Programme Européen pour la Protection des Infrastructures Critiques[6], soulignant la nécessité de coordination entre Etats membres et entre Opérateurs d'Importance Vitale (OIV) en vue de renforcer la sécurité de ces infrastructures. Dans ce cadre, le réseau d'alerte CIWIN (*Critical Infrastructure Warning Information Network*) a été lancé début 2013. Il s'agit d'un portail numérique permettant aux acteurs européens de la protection d'infrastructures critiques d'échanger de l'information sur les vulnérabilités et menaces, ainsi que sur les bonnes pratiques.

En 2014, a été lancé un autre projet, ECOSSIAN[7] (*European COntrol System Security Incident Analysis Network*). Soutenu par la Commission européenne, il porte sur la réalisation d'une plateforme dont l'objectif est d'améliorer la détection et la gestion des cyber-attaques contre les infrastructures critiques, en

---

[3] https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCMQFjAAahUKEwiW0Mfcz6PIAhUJiRoKHY2vBic&url=https%3A%2F%2Fccdcoe.org%2Fmultimedia%2Fregulating-cross-border-dependencies-critical-information-infrastructure.html&usg=AFQjCNHyxMQbjbjbUofrnwEnjCa83Lvylg&sig2=o2n8Z0pwCkN45aB_ii334A

[4] http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

[5] https://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip

[6] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:l33260

[7] http://www.ecossian.eu/

s'appuyant sur un système d'alerte à l'échelle européenne (SOC ou *Security Operation Center* communautaire) et une base de connaissances collaborative.

Le cas des Etats Unis et du Canada

L'Europe n'est pas la seule à avoir pris en compte ces risques transfrontaliers. Outre-Atlantique, de nombreuses réglementations ont aussi été mises en place.

Le Canada et les Etats-Unis entretiennent ainsi une relation étroite d'échanges transfrontaliers. En matière de produits énergétiques, pour ne citer que cet exemple, 17% du pétrole et 18% du gaz naturel importés aux Etats-Unis proviennent du Canada. Les perturbations des infrastructures essentielles ont donc de fortes incidences directes sur les entreprises de part et d'autre de l'immense frontière canado-américaine. Reconnaissant l'importance des infrastructures essentielles, les Etats-Unis et le Canada ont établi des stratégies pour renforcer la cybersécurité dans leurs pays respectifs.

Aux Etats-Unis, cette stratégie a été définie dans le *National Infrastructure Protection Plan*[8] (NIPP), tandis qu'au Canada, *la Stratégie Nationale et le plan d'action pour les infrastructures essentielles*[9] prennent en compte cette problématique. Une véritable politique commune a été mise en place en octobre 2012, avec la publication du *Joint Cybersecurity Action Plan*[10], qui se concentre sur les points suivants :

- le renforcement de la collaboration de la gestion des cyber-incidents entre le *National Cybersecurity & Communications Integration Center* américain et le *Cyber Incident Response Center* canadien ;
- l'engagement conjoint et le partage d'informations avec le secteur privé sur la cybersécurité ;
- et la poursuite de la coopération en matière de cybersécurité lors des efforts de sensibilisation du public.

En 2014, le DHS américain et le Public Safety canadien ont réalisé différentes opérations conjointes, notamment des réunions d'informations pour les parties prenantes dans le secteur de l'énergie et des services publics, ainsi qu'une lettre d'information commune proposant des informations sur les indicateurs de l'activité des menaces cybernétiques.

Enfin, dans de récentes réflexions autour de la stratégie de cybersécurité[11], le Canada souligne l'importance et la prise en compte de ce sujet transfrontalier par le pays : « *Les perturbations touchant les infrastructures essentielles et les cybersystèmes peuvent avoir une incidence directe sur les activités et les collectivités de part et d'autre de la frontière entre le Canada et les États-Unis. Les attaques contre des réseaux cybernétiques interreliés peuvent avoir un effet en cascade sur tous les secteurs de l'industrie et sur la frontière. Pour cette raison, le Canada jouera un rôle actif dans le cadre de forums internationaux afin de promouvoir la protection des infrastructures essentielles et la cybersécurité* ».

[8] http://www.dhs.gov/national-infrastructure-protection-plan

[9] http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-fra.aspx

[10] http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-eng.aspx

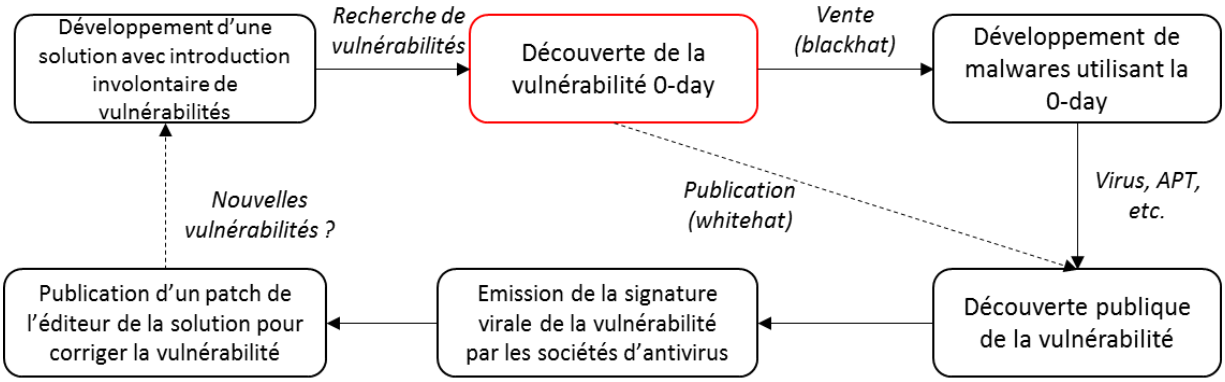
[11] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-fra.aspx

En conclusion, une coopération s'est progressivement mise en place entre les pays transfrontaliers autour de la problématique de la cybersécurité des infrastructures critiques. En raison d'un nombre élevé d'Etats membres, qui chacun défend ses intérêts stratégiques, une certaine lenteur affecte les travaux lancés par l'Union européenne, par opposition à l'efficacité apparente du tandem Etats-Unis / Canada. Le cas de l'Europe est toutefois intéressant, car il permet d'observer le façonnement d'une véritable politique européenne en terme de cybersécurité. Avec la protection des données personnelles et la réglementation e-IDAS, la protection des infrastructures essentielles représente un enjeu majeur, où l'existence même d'une coopération européenne prend tout son sens.

0-DAYS : UN MARCHE EN PLEIN BOULEVERSEMENT

Dans le domaine de la cybersécurité, la recherche de vulnérabilités au sein des différentes solutions équipant les systèmes d'information (logiciels et équipements) est essentielle. Ces vulnérabilités peuvent en effet être exploitées par des pirates dans l'objectif de pouvoir attaquer ces systèmes. On comprend donc aisément l'intérêt de ces recherches, tant pour les sociétés que pour les personnes malveillantes. On nomme 0-days ces vulnérabilités nouvellement découvertes, des failles de sécurité qui n'ont ni fait l'objet d'une publication, ni bénéficié d'un correctif : par conséquent, aucune protection n'est disponible pour s'en protéger. Par exemple, le ver Stuxnet ayant permis d'attaquer les centrifugeuses iraniennes en 2010 comportait 4 vulnérabilités de type 0-day et ne pouvait donc pas être détecté par les systèmes de protection des centrales nucléaires, comme les antivirus.

En effet, la majeure partie des antivirus du marché réalisent des analyses par signature, un morceau de code ou une chaîne de caractères du virus permettant de l'identifier. L'antivirus doit connaitre obligatoirement la signature du virus pour pouvoir le détecter. On constate rapidement les limites de cette méthode avec les vulnérabilités 0-days ou encore les virus dits polymorphes, dont la signature change à chaque réplication. Brian Dye, senior vice-président chez Symantec, co-leader sur le marché des antivirus avec Kaspersky, avait même déclaré en mai 2014 : « *l'antivirus est mort et condamné à l'échec* »[12]. D'autres méthodes de détection existent, moins standard, comme l'analyse heuristique qui se base sur le comportement des applications.

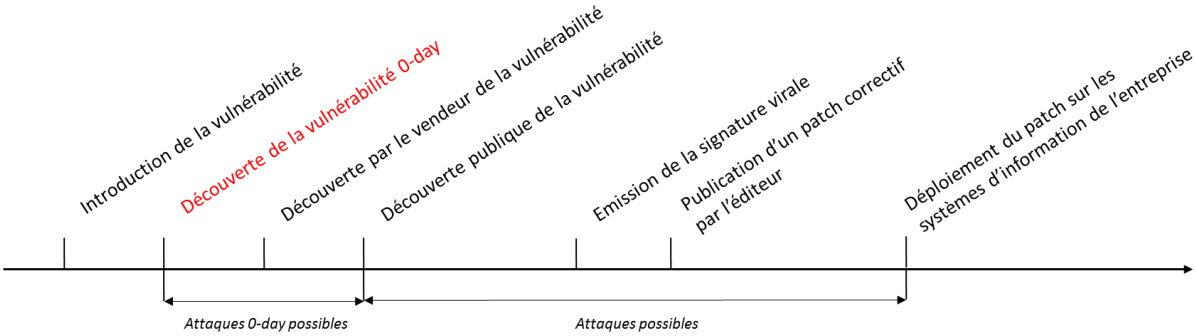


Source: CEIS

Dans certains forums du Dark Web, ces vulnérabilités 0-days se négocient à des prix très variables : ainsi, les vulnérabilités d'Adobe Reader, assez fréquentes, sont proposées à des prix plutôt faibles, entre 5 000 et 30 000 dollars. Plus le nombre de vulnérabilités est faible, plus le prix augmente. L'affaire du piratage de HackingTeam a montré par exemple que le prix d'achat d'une de leurs vulnérabilités 0-days sur l'application Flash est de 45 000 dollars. Par contre, les vulnérabilités 0-days plus rares, comme pour le système d'exploitation iOS de l'iPhone, se vendent entre 100 000 et 250 000 dollars. La start-up Zerodium, très

[12] http://www.wsj.com/news/article_email/SB10001424052702303417104579542140235850578-lMyQjAxMTA0MDAwNTEwNDUyWj

proche de l'ancienne société de sécurité Vupen, vient même de proposer la somme d'un million de dollars pour la personne qui leur fournira une faille sur la nouvelle version, iOS 9[13].



Source: CEIS

La publication de patchs correctifs suite à la découverte d'une 0-day peut aussi amener une nouvelle vulnérabilité : les 1-day. Grâce à des méthodes de *binary diffing* sur les patchs, il est en effet possible de comprendre les vulnérabilités qui sont corrigées et ainsi de pouvoir produire une attaque sur cette vulnérabilité. Les victimes sont les personnes n'ayant pas mis à jour leur solution. Ce type d'attaque peut être évité à l'aide d'une véritable stratégie de gestion des correctifs au sein d'une organisation.

Un marché bientôt menacé par une restriction américaine ?

Les vulnérabilités de type 0-day ayant de forts impacts sur la sécurité des systèmes d'information, les Etats n'ont pas tardé à se protéger. Aux Etats-Unis par exemple, un processus pour les achats de vulnérabilité au sein du gouvernement a été mis en place en 2008 : le VEP (*Vuln Equities Process*)[14]. La NSA achète les vulnérabilités et coordonne leur distribution aux autres agences du gouvernement afin d'éviter une concurrence interne dans l'objectif d'obtenir les meilleures vulnérabilités.

Le marché des 0-days évolue aujourd'hui avec la mise à jour de l'arrangement de Wassenaar. En 1996, 41 pays ont décidé de signer cet arrangement, qui est un accord multilatéral de contrôle de leurs politiques en matière d'exportations d'armements conventionnels et de biens et technologies à double usage (civil et militaire). L'Europe, l'Amérique du Nord et la Russie ont signé ce traité, contrairement à l'Afrique, la Chine, ou encore le Moyen-Orient. L'objectif premier de cet accord était la non-prolifération des armes de destruction massive et des armes chimiques. Le domaine de la cryptographie a aussi été intégré au périmètre de cet accord en 1996.

En décembre 2013, le commerce de l'exploitation des vulnérabilités informatiques fait son entrée dans l'arrangement de Wassenaar[15], ainsi que différentes solutions de sécurité informatique. Y figurent :

[13] https://www.zerodium.com/ios9.html

[14] https://www.eff.org/files/2015/09/04/document_71_-_vep_ocr.pdf&usg=ALkJrhgi0UXp_WyKlNsmc4MGmyIbA8AM8Q

[15] http://www.wassenaar.org/controllists/2013/WA-LIST%20%2813%29%201/WA-LIST%20%2813%29%201.pdf

- *5. A. 1. j. Systèmes IP de surveillance des communications du réseau ou de l'équipement, et composants spécialement conçus ;*

- *4. A. 5. Systèmes, équipements et composants conséquents, spécialement conçus ou modifiés pour la production, l'exploitation, ou livraison de, ou la communication avec, « des logiciels d'intrusion » ;*

- *4. D. 4. « Logiciel » spécialement conçu ou modifié pour la production, l'exploitation, ou la livraison de, ou la communication avec, des « logiciels d'intrusion » ;*

- *4. E. 1. c. « Technologie » pour le « développement » des « logiciels d'intrusion ».*

Un contrôle du gouvernement est donc obligatoire pour autoriser l'exportation de chacun de ces types de solutions. Le gouvernement prend ainsi une place centrale dans la commercialisation de ces technologies et a un droit de veto sur les ventes à des organisations étrangères (sociétés, Etats) à l'instar d'autres domaines, comme le militaire ou le spatial.

Le 20 mai 2015, le BIS (*Bureau of Industry and Security*) américain a proposé une transposition dans la loi américaine de cette nouvelle version de l'arrangement de Wassenaar, avec un appel à commentaires. Plusieurs voix se sont élevées contre cette transposition, les règles du BIS proposant des règles supplémentaires à l'arrangement original[16].

Le BIS ajoute en effet à la liste des équipements contrôlés les éléments suivants :

- Les systèmes, équipements, composants et logiciels spécifiquement conçus pour la production, l'opération ou la fourniture, ou la communication avec des logiciels d'intrusion, dont les produits de test d'intrusion pour identifier les vulnérabilités des ordinateurs et des appareils capables de connexion réseau ;

- Les technologies pour le développement de logiciels d'intrusion comprenant la recherche exclusive sur les vulnérabilités et l'exploitation des ordinateurs et des appareils capables de connexion réseau.

Selon les déclarations de Randy Wheeler, directrice du BSI, les recherches théoriques de vulnérabilités ne seront pas contrôlées mais tout logiciel susceptible de contribuer à développer des exploits 0-days pouvant être vendus serait couvert par la proposition. Malheureusement, les *Proof of Concept*, utilisés par les chercheurs pour démontrer que les vulnérabilités trouvées sont valides et fonctionnent, sont identiques à des exploits 0-days à vendre, ce qui va donc poser de nombreux problèmes pour la recherche en sécurité informatique.

Les organisateurs de la célèbre conférence Blackhat[17] ont déclaré que dans sa rédaction actuelle, l'arrangement « *a le potentiel de restreindre significativement et/ou d'éliminer la profondeur et certains types de recherche examinés par de nombreux membres de [la] communauté de la sécurité, en particulier pour*

[16] https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

[17] https://www.blackhat.com/latestintel/07172015-wassenaar.html

ceux qui collaborent dans le monde entier ». Les sociétés Google[18] et Cisco[19] ont aussi critiqué cette transposition. Suite à ces retours négatifs, le BIS a décidé de promulguer une seconde itération de cette transposition[20] de 60 jours.

Cette décision pourrait poser de nombreux problèmes pour la commercialisation de 0-day par les différentes sociétés américaines, comme Zerodium[21] ou Absolute Zero Day Exploit Exchange[22], créée par Kevin Mitnick. Les Etats-Unis auraient ainsi un droit de regard sur le contenu de toutes les ventes de vulnérabilités informatiques à l'extérieur du pays et pourraient décider d'en bloquer l'exportation ou a minima d'en retarder l'acquisition.

Le développement du métier des 0-days

Avec l'explosion des solutions informatiques, et donc de leurs vulnérabilités potentielles, la pratique du bug bounty a aussi évolué. Cette dernière consiste pour une entreprise à demander à une communauté d'experts en sécurité informatique d'analyser et détecter des failles dans ses applications ou sites web moyennant une reconnaissance et une rémunération potentielle en fonction de la pertinence de la faille. Des centaines de sites mettent désormais en place un programme de bug bounty[23] : Google, Facebook, Avast!, Paypal, etc. Des sites, comme Internet Bug Bounty[24], qui proposent des primes pour les bugs affectant les implémentations de logiciels très divers, menaçant la stabilité de l'Internet au sens large, sont même sponsorisés par les sociétés Microsoft et Facebook.

On a aussi pu observer depuis 2014 une explosion des montants de ces primes : Mozilla a augmenté sa prime maximum de 3 000 à 10 000 dollars[25]. Sheryl Sandberg, COO de Facebook, a déclaré[26] que sa société avait dépensé des millions de dollars en 2014 pour son programme de primes. Microsoft a proposé des récompenses allant jusqu'à 15 000 dollars pour un programme de Bug Bounty sur son nouveau navigateur, Edge[27], pendant trois mois. Des sociétés se sont même créées sur ce marché, comme HackerOne ou Zerodium cité précédemment. Conçu par les responsables de la sécurité de Facebook, Microsoft et Google, HackerOne[28] est la première plate-forme de gestion de la vulnérabilité et de bug bounty. A ce jour, elle a déjà versé 4,29 millions de dollars de primes et permis la résolution de 12 919 bugs.

---

[18] http://googleonlinesecurity.blogspot.ch/2015/07/google-wassenaar-arrangement-and.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+GoogleOnlineSecurityBlog+(Google+Online+Security+Blog)&m=1

[19] http://blogs.cisco.com/gov/wassenaar

[20] http://www.theregister.co.uk/2015/05/20/us_export_controls_0days/

[21] https://www.zerodium.com/

[22] https://www.mitnicksecurity.com/shopping/absolute-zero-day-exploit-exchange

[23] https://bugcrowd.com/list-of-bug-bounty-programs

[24] https://internetbugbounty.org/

[25] http://www.programmez.com/actualites/mozilla-reevalue-les-recompenses-de-son-programme-bug-bounty-22813

[26] https://www.youtube.com/watch?v=e754y5dis00

[27] http://www.zdnet.fr/actualites/3-mois-de-bug-bounty-pour-le-projet-spartan-39818482.htm

[28] https://hackerone.com/

Zerodium[29], société créée par l'un des fondateurs de la société VUPEN, est un grossiste de failles de sécurité. Les chercheurs peuvent lui vendre des failles, spécifiées en amont par Zerodium. Contrairement aux autres organismes, l'objectif de la société n'est pas de remonter les vulnérabilités aux sociétés, mais de vendre aux plus offrants des failles.

Le marché des vulnérabilités 0-days est en pleine métamorphose : il est marqué par des vulnérabilités de plus en plus nombreuses et une volonté des Etats de contrôler au mieux ces armes d'un nouveau genre. La question est de savoir si cette volonté de contrôle ne va pas jouer un rôle négatif sur la recherche en cybersécurité.

[29] https://www.zerodium.com/

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.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com