Lettre mensuelle – Août 2018 - disponible sur omc.ceis.eu

Table des matières

ANALYSES

1. L'ECHEC DU *GROUP OF GOVERNMENTAL EXPERTS* (GGE) SUR LA CYBERSECURITE : CONSEQUENCES ET PERSPECTIVES

Introduction

Transcendant les frontières internationales traditionnelles, le cyberespace est l'un des nouveaux défis du droit international. Depuis le début des années 2000, l'essor des cyberattaques de masse et des campagnes de désinformation, nouvelles armes de guerre sur le champ de bataille du numérique, pousse les États à vouloir réglementer l'usage du cyberespace.

En 2004, le premier Groupe d'Experts Gouvernementaux (GGE) de l'ONU sur la cybersécurité est mis en place à l'initiative de la Russie. Quinze États y participent.[i] Quatre sessions successives se tiennent par la suite, dont deux donnent lieu à des rapports finaux en 2013 et 2015. Si le rapport de 2013 se contente de rappeler l'importance cruciale d'une coopération internationale dans le domaine de la cybersécurité[ii] , le rapport de 2015 liste quant à lui des principes précis quant à l'attitude que doivent adopter les États dans le cyberespace, tels que :

- L'interdiction d'attaquer les infrastructures critiques d'un État tiers en temps de paix ;
- L'interdiction d'attaquer les structures de réponse aux incidents (CERT, CSIRTS, etc) d'un État tiers ;
- L'obligation de porter assistance à un État attaqué par un groupe situé dans un autre État si celui-ci en fait la demande.[iii]

Le dernier GGE en date qui s'est tenu en juin 2017 n'a en revanche pas eu de résultat concret. Les 25 États participants ne sont en effet pas parvenus à trouver un accord sur le paragraphe 34 qui porte sur la manière dont le droit international devrait s'appliquer au cyberespace.

Les raisons de l'échec et ses conséquences

Trois questions ont fait figure de points d'achoppement entre les Etats :

- Un État peut-il mettre en place des contre-mesures en cas de cyber-agression ?
- Comment le droit humanitaire international doit-il s'appliquer au cyberespace ?
- Une cyberattaque rempli-t-elle les critères d'une attaque armée, permettant d'enclencher la légitime défense ?

Les divergences quant aux réponses à apporter à ces questions font s'opposer deux visions qui reflètent des différences profondes dans la lecture du système et du droit international : une interprétation occidentale qui se focalise avant tout sur la promotion et l'extension des normes internationales existantes à toutes les sphères et tous les domaines d'opération possibles, y compris le cyberespace ; et une interprétation Sino-Russe qui

conçoit les structures internationales existantes comme des mécanismes permettant de maintenir la paix et la sécurité internationale mais refuse d'étendre leurs compétences au cyberespace.[iv]

Par exemple pour la Russie, la Chine et Cuba, l'article 51 de la Charte des Nations Unis octroyant aux Etats un droit naturel à la légitime défense ne devrait pas pouvoir s'appliquer au cyberespace où la notion d'agression armée reste plus floue[v]. La Chine, [vi] la Russie et Cuba considèrent ainsi que la possibilité d'avoir recours aux principes d'auto-défense et de contre-mesures dans le cyberespace reviendrait à légitimer les conflits cybernétiques. [vii] De fait, leurs arsenaux militaro-politique respectifs font tous état d'un un haut niveau de sophistication technique et intègrent déjà des dispositifs leur permettant d'agir dans le cyberespace : groupes de hackers éventuellement sponsorisés, campagnes de désinformation, cyberattaques soutenant leurs agendas politiques,… L'application du droit international au cyberespace permettrait donc à leurs adversaires de prendre des contre-mesures juridiques et cyber-militaires contraires à leurs intérêts.

Le principe de souveraineté a également cristallisé les tensions.[viii] Pour la Russie comme pour la Chine, la souveraineté est un concept absolu qui ne peut souffrir de remise en cause. Chaque pays devrait donc avoir le droit de gérer son propre cyberespace conformément à sa législation intérieure. Par ailleurs, les différences de capacités cybernétiques entre les États[ix] rendent difficile l'établissement de régulations internationales qui s'appliqueraient de la même manière à tous. Les pays aux arsenaux cyber les moins avancés craignent notamment de se voir appliqués les principes d'auto-défense et de contre-mesure alors même qu'ils cherchent à tester leurs nouvelles capacités.

Si cette tension entre deux visions du système international et du cyberespace, explique en grande partie l'échec du dernier GGE, ce dernier n'a pas eu que des conséquences négatives. Il a par exemple amené de nouveaux acteurs à s'impliquer davantage dans la régulation du cyberespace.

Perspectives d'évolution suite à l'échec du GGE

Cet « échec » a posé les problématiques du format et de la faisabilité d'un groupe de travail sur ces questions. Le secteur public comme le secteur privé ont soumis plusieurs suggestions quant à de possibles alternatives au GGE.

Les initiatives étatiques

Plusieurs Etats ont fait des suggestions sur l'avenir des GGE[x]. Les délégations cubaines, russes et chinoises ont proposé la création d'un « *working group of the General Assembly* » ouvert à tous les Etats volontaires (et non plus seulement à 25 commissaires), pour assurer une totale transparence sur les sujets abordés et une participation égale de chacun aux discussions et prises de décisions. Cela pourrait être envisageable, mais en pratique l'obtention d'un consensus sera d'autant plus difficile dès qu'il s'agira de traiter de sujets sensibles en matière de défense ou de sécurité nationale, où chaque état souhaite rester souverain.

Deux conceptions émergent : d'un côté celle de la Russie et du Brésil qui privilégient une coopération régionale, et de l'autre celle qui promeut une coopération bilatérale soutenue par l'Inde et la Suisse.

- Russie

La Russie a proposé l'adoption d'un traité global sur la cybercriminalité pour remplacer la convention de Budapest, dont elle conteste l'article 32 qui permet à un État étranger d'accéder ou de recevoir des données

stockées sur le territoire d'autres États s'il obtient le consentement du propriétaire de ces données. L'adoption du nouveau traité n'autoriserait plus ce type de pratiques.

- Brésil

Le Brésil a évoqué un nouveau cadre juridique qui interdirait en priorité l'usage offensif des capacités cyber, par exemple par l'introduction délibérée de vulnérabilités dans différents types de supports dans l'objectif de compromettre la sécurité des informations d'autres États. Cette position privilégie une utilisation défensive des capacités cyber et appelle à la mise en place d'une réglementation contraignante pour lutter principalement contre la cybercriminalité par une coopération internationale renforcée.

- Inde

Suite aux désaccords du GGE sur la cybersécurité, un comité a été formé au sein de *l'India National Security Council Secretariat* (NSCS) pour suggérer les orientations stratégiques et les politiques à mettre en œuvre pour le développement de nouvelles normes en matière de cybersécurité[xi]. En collaboration avec la Suisse, elle a aussi proposé la création d'un « *Cyber Committee of the General Assembly* » sur le modèle du « *Committee on the Peaceful Uses of Outer Space »* créé en 1959. Il était alors composé de 84 membres et de différents sous-comités spécialisés (juridique, scientifique, etc.).

La France penche également pour des accords bilatéraux, tout comme les États-Unis qui ont d'ailleurs adopté leur propre « *Cyber Incident Severity Schema* », un tableau classant les cyberattaques suivant leur degré de sévérité en fonction de leurs impacts humains ou matériels. La France se questionne également sur l'application d'un tel tableau, dans sa récente Revue Stratégique de Cyberdéfense[xii].

Constatant que les États n'arrivaient pas à trouver un accord et que leurs propositions mettaient en avant des intérêts essentiellement souverains au détriment de l'intérêt commun, des initiatives ont également émergé de la part du secteur privé.

Les initiatives privées

En février 2017, Brad Smith, Président de Microsoft Corporation, annonce la création d'une « *Convention de Genève Digital* » n'ayant pour le moment remporté qu'un succès mitigé auprès des États. Dans le but de rassembler alors le secteur privé, 40 entreprises leaders du numérique tels que Dell, Facebook, Oracle ou Trend Micro signent le *Cybersecurity Tech Accord*, proposé par Microsoft. Le principe retenu est celui du « *Strong defense, No offense* » : l'accord n'autorise que des opérations défensives. En cas de menaces, les entreprises s'engagent à répondre collectivement pour protéger les utilisateurs. Cependant, plusieurs géants du numérique manquent à l'appel comme Google, Apple ou Amazon. Cette absence montre bien que si cet accord est perçu comme plus protecteur pour les utilisateurs, il ne fait pas l'unanimité au sein des entreprises leaders du numérique, et suggère que les entreprises signataires souhaitent avant tout protéger leurs consommateurs et donc leurs intérêts économiques.

A l'initiative de deux *think tank* hollandais et américain est créée la « ***Global Commission on the stability of cyberspace*** »[xiii]. Cette commission est composée de 26 commissaires de professions diverses (universitaires, ONG, entreprises) et a pour objectif de promouvoir une compréhension commune des enjeux

du cyberespace permettant de renforcer la stabilité et la sécurité. Elle vise à encadrer aussi bien les actions étatiques que celles issues d'acteurs non-étatiques

Il reste difficile à déterminer aujourd'hui si ces initiatives seront globalement acceptées et poursuivies. Cependant, « l'échec » du GGE a permis de démontrer :

- Qu'il subsiste toujours des différences de lecture entre Etats sur la manière d'appliquer le droit international au cyberespace ;
- Qu'il existe une réelle prise de conscience globale sur la nécessité d'enclencher des mécanismes juridiques propres au cyberespace.

NOTES

[i] Nommément : la Russie, les États-Unis, le Mexique, le Brésil, l'Afrique du Sud, le Mali, la France, le Royaume-Uni, l'Allemagne, le Jordanie, la Biélorussie, l'Inde, la Chine, la Corée du Sud et la Malaisie.

[ii] https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf

[iii] https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html

[iv] http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf

[v] Selon le manuel de Tallinn, une cyber-attaque est une opération informatique, offensive ou défensive, susceptible de causer des blessures ou la mort d'une personne, ou des dommages voire la destruction d'objets et d'infrastructures https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html

[vi] https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

[vii] https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf

[viii] http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf

[ix] https://thewire.in/tech/un-cyber-norms-india-asoke-mukerji-nsc

[x] https://carnegieendowment.org/2018/03/02/outlook-on-international-cyber-norms-three-avenues-for-future-progress-pub-75704

[xi] https://thewire.in/tech/un-cyber-norms-india-asoke-mukerji-nsc

[xii] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

[xiii] https://cyberstability.org/

2. LA SECURITE DES LIAISONS SATELLITES

Les liaisons satellites sont aujourd'hui considérées comme acquises dans beaucoup de pays, et de nombreux secteurs économiques en dépendent ou sont amenés à en dépendre : agriculture de précision, logistique, transactions financières, télévision, Internet… Du côté militaire, les satellites sont également employés dans les télécommunications, la surveillance, le guidage des munitions ou encore le contrôle des drones. Les armées ont aussi été amenées à faire appel aux satellites civils pour bénéficier localement d'une plus grande capacité en bande passante : aujourd'hui, plus de 80% des besoins en capacité satellitaires du DoD sont par exemple couverts par les satellites de communication civils[i].

Si les grandes puissances possèdent depuis longtemps des capacités offensives avancées, l'essor des technologies de radio logicielle (SDN pour *Software-Defined Radio*) apporte son lot de nouvelles menaces et fait considérablement augmenter le risque de piratage des liaisons satellites par des acteurs non étatiques. Ces technologies permettent en effet de s'affranchir de l'acquisition de matériels spécialisés pour établir des communications radio sur diverses fréquences, ce qui rend impossible le contrôle de ces capacités. Ainsi, en 2009, lors d'une conférence *BlackHat* à Las Vegas, le chercheur en sécurité Adam Laurie fit la démonstration d'une écoute de flux transmis par satellite en s'armant simplement d'un matériel commun et accessible à tous[ii]. Une communauté SDR importante s'est développée depuis et il existe désormais de nombreux outils open-source très puissants à disposition de tous.

Face à l'émergence de nouvelles menaces, cette dépendance aux liaisons satellites conduit à s'intéresser à la résilience des fonctions que les satellites assurent.

Les cybermenaces aux liaisons satellitaires

Le brouillage (jamming)

L'attaquant utilise une antenne directionnelle pour produire un signal d'interférence qui surcharge le signal légitime, empêchant sa réception par le récepteur. Le brouillage peut être « flagrant »[iii] (le récepteur reçoit un signal audible) ou « subtil » (un signal d'amplitude opposée est envoyé par l'attaquant, sur la même fréquence et avec une puissance adaptée). Ce second type de brouillage reste très situationnel et complexe à mettre en œuvre. Les signaux descendants sont plus vulnérables au brouillage, la force du signal satellite étant relativement faible. A ce titre, les liaisons GPS sont particulièrement vulnérables et souvent attaquées, d'autant que l'on peut aujourd'hui obtenir pour 50 € des brouilleurs GPS alimentés sur allume-cigare capables de créer une bulle d'interférence d'une centaine de mètres de diamètre[iv].

Les satellites commerciaux sont également utilisés par certaines armées pour renforcer les capacités de géolocalisation. L'entreprise Iridium a ainsi lancé en 2016 un nouveau service permettant de renforcer le système GPS[v] et d'augmenter la résilience face aux risques de brouillage et d'usurpation grâce au système STL (Satellite Time and Location[vi]), qui nécessite l'utilisation de micropuces à intégrer aux dispositifs au sol, fait usage des satellites Iridium pour authentifier les signaux GPS. Ce renfort permet en outre de diminuer le risque de black-out si les satellites militaires venaient à être ciblés (d'autant que cette redondance diminue l'intérêt d'une telle démarche).

L'interception

On trouve assez facilement sur le web des tutoriels décrivant des techniques d'interception de transmissions par satellite à l'aide de matériel disponible dans le commerce, qu'il s'agisse de transmissions télévisuelles, de conversations téléphoniques ou de trafic internet. L'un des cas les plus connus d'écoute de liaison satellite implique le logiciel SkyGrabber, vendu par l'entreprise russe Sky Software au prix de 26$. Le logiciel a été utilisé en Irak et en Afghanistan pour capturer des flux vidéo non chiffrés de drones *Predator*.

Le piratage du satellite ou des stations de contrôle au sol

Le piratage correspond à l'utilisation non autorisée d'un satellite pour effectuer une transmission, ou à la prise de contrôle du système TT&C (*Tracking*, *Telemetry* & *Control*). Les données transmises peuvent être écoutées par des attaquants et modifiées en chemin afin de prendre le contrôle de tout ou partie de l'architecture satellitaire, permettant au pirate de manœuvrer voire détruire le satellite. La prise de contrôle d'un satellite est cependant particulièrement difficile car les mesures de sécurité protégeant les satellites sont très efficaces. Le risque se situerait davantage au niveau des stations de contrôle au sol, dont l'équipement de contrôle fait généralement emploi d'une informatique classique sous Linux. Cependant en 2008, des pirates ont pu prendre le contrôle d'un satellite d'observation terrestre de la NASA (Terra EOS) pendant plusieurs minutes. En 2014, des chercheurs d'IOActive ont en outre identifié des failles et des erreurs de conception au sein des micrologiciels des dispositifs SATCOM les plus populaires qui permettaient d'intercepter, manipuler, bloquer et même prendre le contrôle total des systèmes de communication localisés dans des stations de contrôle, des aéronefs et des vaisseaux[vii].

Le piratage des terminaux connectés au satellite

Ces menaces englobent une variété de méthodes permettant d'accéder aux connections réseaux satellitaires en vue de les exploiter, ce qui n'implique pas nécessairement d'interaction avec le satellite. Elles comprennent par exemple l'usurpation DNS, le vol de session TCP ou encore les attaques sur le protocole GRE[viii]. L'usurpation de signaux GPS reste le cas le plus courant d'exploitation de vulnérabilité de liaison satellitaire. Il s'agit d'envoyer de faux signaux GPS à des récepteurs GPS pour fausser la géolocalisation. Contrairement au brouillage, la cible ne réalise pas qu'elle est victime d'une attaque et peut ainsi penser qu'elle se situe en un lieu différent, à un moment différent. Ce type d'attaque est suspecté d'avoir eu un rôle dans la capture d'un drone américain par l'armée iranienne en 2011, et dans la série de collisions ayant impliqué des navires américains en Asie du Sud-Est ([ix].

De nombreuses techniques permettent cependant d'éviter de telles attaques, notamment l''usage de plusieurs systèmes de géolocalisation, les discriminations de signaux basées sur l'amplitude, le moment et l'angle de réception, la polarisation ou encore une authentification cryptographique[x]

Un difficile maintien en conditions de sécurité

L'ajout et la mise à jour de fonctionnalités de sécurité sont particulièrement limités dans le domaine SATCOM. Le rétrofitage[xi] du matériel est inenvisageable en orbite, aussi seules les mises à jour au niveau logiciel sont possibles et celles-ci ne sont pas sans risque pour le satellite.

Les vulnérabilités régulièrement découvertes au sein des protocoles de chiffrement – ou dans leur application – renforce cette difficulté de maintien en conditions de sécurité, notamment pour les satellites les plus anciens. A ceci s'ajoute le fait que le chiffrement n'est pas systématiquement activé par les opérateurs de satellite quand bien même de tels systèmes sont à leur disposition, à l'exception des liaisons satellites civiles à disposition des militaires. Le chiffrement des données au sein des transmissions satellitaires représente en effet un coût important (implémentation, mise à jour, formation du personnel) et peut avoir un impact fort sur les performances du système notamment lorsqu'il s'agit d'intégrer de telles capacités à des satellites dont la conception n'incluait pas de telles fonctionnalités.

Conclusion

L'évolution de la menace a fait de la question de la sécurité des systèmes satellitaires une priorité au sein de la stratégie cyber des Etats. Si les entreprises civiles ont réalisé des efforts significatifs pour intégrer cette exigence dans le cycle de vie des produits satellitaires, le niveau de sécurité global reste limité par le cycle de renouvellement des satellites déjà déployés.

S'agissant du besoin des armées d'accroître la bande passante disponible, les satellites commerciaux les plus récents sont évidemment les plus à même d'en proposer à un niveau et à un coût satisfaisant, et ceux-ci sont censés être les plus à jour en termes de dispositifs de sécurisation de la fonction satellite dans son ensemble (selon la maturité de l'opérateur sur la question). Concernant les problématiques de géolocalisation, l'usage de constellations tierces (Galileo, Glonass, Compass mais également d'autres constellations civiles telles qu'Iridium), peut permettre de répondre aux risques d'usurpation de signaux. La réponse à la question de l'authentification de ces signaux passe cependant par l'ajout de nouvelles puces sur les dispositifs au sol.

Une réponse juridique aux menaces interétatiques d'attaques sur les liaisons satellites semble plus éloignée que jamais. Le code de conduite international pour les activités spatiales proposé par l'Union Européenne en 2007 et mis à jour pour la dernière fois en 2015, se voulait une base pour un futur traité d'interdiction d'armement dans l'espace mais est resté à ce jour à l'état de projet. Si l'administration Obama est revenue en arrière sur la politique de domination spatiale de l'administration Bush[xii] au profit d'une coopération multilatérale, les Etats-Unis se sont cependant opposés à la proposition sino-russe[xiii] de traité d'exclusion d'armement dans l'espace[xiv] et l'administration Trump semble au contraire s'engager sur une militarisation de l'espace, avec notamment la création d'une force spatiale de l'armée distincte de l'US Air Force.

L'US Special Operations Command (USSOCOM) a pris la mesure sur la réduction continue de leur avantage issu de leurs capacités satellitaires qui se trouvent de plus en plus menacées. Si elle cherche à renforcer la sécurité des liaisons satellitaires traditionnelles, elle explore et développe des solutions alternatives, notamment les nano-satellites CubeSat et autre systèmes pseudo-satellitaires type drones (UAV) de haute altitude et haute endurance (HALE).

[i] http://www.defenseone.com/technology/2013/09/why-military-needs-commercial-satellite-technology/70836/

[ii] Avec un simple ordinateur, un décodeur satellite type Dreambox et grâce à des logiciels téléchargeables sur Internet.

[iii] Pour peu de posséder un dispositif adapté. L'utilisateur d'un téléphone satellitaire civil victime d'un brouillage n'aura pour seule information que le réseau semble être hors de portée.

[iv] http://www.militaryaerospace.com/articles/2016/06/gps-jamming-satellite-navigation.html

[v] http://www.reuters.com/article/us-iridium-gps/iridium-launches-timing-location-service-as-gps-back-up-idUSKCN0YE1HZ

[vi] http://investor.iridium.com/releasedetail.cfm?releaseid=972324

[vii] Les produits concernés par l'étude d'IOActive étant produits ou vendus par Harris, Hughes Network Systems, Cobham, Thuraya Telecommunications, Japan Radio Company et Iridium Communications.

[viii] https://fr.wikipedia.org/wiki/Generic_Routing_Encapsulation

[ix] https://www.japantimes.co.jp/news/2017/08/23/asia-pacific/experts-doubt-human-error-four-times-row-others-call-gps-hack-unlikely/

[x] A l'instar du système STL précédemment mentionné.

[xi] Le rétrofitage consiste à ajouter, modifier ou restaurer des fonctions technologiques sur des systèmes vieillissants.

[xii] http://www.nytimes.com/2010/06/29/science/space/29orbit.html

[xiii] http://freebeacon.com/national-security/u-s-opposes-new-draft-treaty-from-china-and-russia-banning-space-weapons/

FOCUS INNOVATION

ENTRETIEN AVEC SEBASTIEN DUPONT-RAOSETA, CO-FONDATEUR ET CEO UNIRIS

Présentation

UNIRIS a été fondée en février 2017 par des spécialistes de la Cyber-sécurité et de la Finance qui se sont intéressés très tôt à la technologie « Blockchain ». Cette jeune start-up très prometteuse a développé une solution particulièrement innovante d'authentification biométrique basée sur le réseau veineux et couplée à une blockchain ultra-rapide et sécurisée.

Incubée au sein de centres de recherche prestigieux et accélérée par le programme « X-up » de l'École Polytechnique en 2017, UNIRIS a vu sa technologie – protégée par 11 brevets – saluée au cours de plusieurs concours récents (Challenge Plus de HEC, Label GENERATE du GICAT, 1er prix de l'Université d'été du MEDEF, etc.).

La société est aujourd'hui composée d'une dizaine de personnes et ses effectifs sont en train d'augmenter.

L'innovation

La technologie d'authentification d'UNIRIS, alliance de deux technologies de chiffrement, se base sur deux innovations majeures :

D'une part, un dispositif d'authentification biométrique, par scan infrarouge et échographique du réseau veineux, qui est par définition unique et infalsifiable : le réseau veineux devient alors la clé cryptographique qui permet à l'individu d'accéder au système et de garantir son identité. Concrètement, l'utilisateur pose son doigt sur un dispositif équipé d'un senseur qui reconnaît le réseau veineux. Le dispositif vérifie également qu'il est bien en présence d'un doigt humain et vivant (et non un doigt sectionné ou en silicone, par exemple). De plus, un capteur analyse le rythme cardiaque, afin de s'assurer que la personne n'est pas sous contrainte et ne présente pas un état de stress anormal. Enfin, le système apprend automatiquement les évolutions bio-morphologiques de la personne.

D'autre part, une blockchain[1] développée spécifiquement pour son activité qui offre un très haut niveau de sécurité total et des performances supérieures dans l'exécution des transactions.

Par ailleurs et surtout, les clés issues du scan biométrique sont générées automatiquement puis effacées, sans ne jamais être stockées ni sur le dispositif biométrique ni sur la blockchain, assurant ainsi sécurité et confidentialité des données des utilisateurs (compatibilité CNIL/GDPR by design).

Les usages

Les usages d'une telle solution, qui permet de prouver l'identité d'une personne localement ou à distance et d'assurer un très haut niveau de sécurité, sont multiples (paiement en ligne, droits d'accès à des documents / des bâtiments sensibles, gestion des données de santé, etc.). Certains sont particulièrement pertinents dans un contexte Défense. La solution d'UNIRIS pourrait par exemple permettre le contrôle et la sécurisation des accès cybernétiques et physiques, ainsi que la gestion des habilitations. La solution assure à la fois la confidentialité et la traçabilité des accès.

UNIRIS travaille actuellement activement sur l'industrialisation de sa solution. Son adaptation est en cours auprès de nombreux clients aux profils industriels variés : aéroports, automobile, banques, objets connectés, etc.

[1] La blockchain est un système de gestion distribuée de bases de données. Il s'agit d'une chaîne de « blocs », liés entre eux par des liens cryptographiques. Les blocs contiennent de la donnée. L'ajout d'un nouveau bloc ne peut se faire que s'il y a consensus entre les participants à la chaîne. Une fois le bloc validé, horodaté et ajouté à la chaîne, il devient immuable : les données qu'il contient ne peuvent plus être modifiées. Une blockchain est donc un historique des transactions infalsifiable et sécurisé ne dépendant pas d'un organe central de contrôle.

CALENDRIER

Séminaire national des réserves « cyber » – lundi 24 septembre 2018

Le Séminaire national des réserves « cyber » aura lieu le lundi 24 septembre 2018 à la Direction générale de la Gendarmerie nationale, 4 rue Claude Bernard à Issy-les-Moulineaux.

Accueilli par le GAR Richard Lizurey, Directeur général de la Gendarmerie nationale, le comité de direction des réserves « cyber » – constitué du Commandant de la Cyberdéfense le GDI Olivier Bonnet de Paillerets, du Directeur général de l'ANSSI l'IGA Guillaume Poupard – exposera la nouvelle organisation des réserves "cyber" et précisera ses missions. Quelques exemples de travaux menés au sein des réserves seront ensuite présentés. L'après-midi sera dédié à des groupes de travail sur divers sujets de réflexion.

Pour toute demande d'information ou d'inscription, merci de contacter florence.esselin@gendarmerie.interieur.gouv.fr

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 des Armées
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com