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

Table des matières

ANALYSES

1. LA BLOCKCHAIN ET SES USAGES MILITAIRES

La blockchain est au cœur de l'actualité de l'innovation depuis quelques temps. Toutefois, la mise en œuvre à une échelle opérationnelle de grande ampleur reste à effectuer et les avis sont souvent partagés sur la question de son utilité et surtout de sa sécurité.

Signifiant littéralement « chaîne de blocs », la blockchain est un système de gestion distribuée de bases de données : pour simplifier, les membres d'une blockchain possèdent tous une copie à jour de la base de données complète mais ne peuvent pas en modifier les entrées existantes (appelées « blocs »), chaque nouvelle entrée devant être validée avant d'être être ajoutée à cette « chaine ».

Les « blocs », qui contiennent donc les données, sont reliés entre eux par des liens cryptographiques. Le concept de sécurité et de traçabilité des blockchains repose sur le fait que lorsqu'une transaction a été effectuée, elle est validée, horodatée et ajoutée à la chaîne de façon à ce qu'un bloc et les données qu'il contient ne peuvent ensuite théoriquement plus être modifiés sans que cela ne soit détecté.

Largement expérimentée dans le civil, la blockchain a d'abord été promue et utilisée par les start-ups et convainc maintenant peu à peu les grandes entreprises. Certains États (USA, Russie, etc.) et organisations internationales (ONU, OTAN, Union européenne, etc.) commencent à s'y intéresser également. L'ampleur du phénomène est réelle, même s'il n'existe pas, à ce jour, d'usages véritablement déployés à grande échelle en dehors des cryptomonnaies.

Cependant, comme pour toute nouvelle technologie a priori prometteuse, certains alertent sur le manque de visibilité quant à la résilience à long terme de la blockchain. Elle doit bien évidemment être expérimentée et soigneusement évaluée avant d'être introduite dans le milieu de la Défense française.

Typologie des blockchains

Il existe trois types de blockchain, dont les conditions de fonctionnement varient, ce qui a un impact notamment sur les modes de validation des opérations et donc sur la sécurité des données :

- Les blockchains publiques(comme celle qui sous-tend la cryptomonnaie Bitcoin) sont ouvertes à tous et accessibles via Internet. Elles ne présentent pas de barrière à l'entrée. La validation des transactions repose sur la notion de « consensus décentralisé », c'est-à-dire qu'elle est effectuée par ses membres et s'affranchit d'une autorité centrale de contrôle.
- Les blockchains hybrides sont des blockchains dont la gouvernance est partiellement décentralisée entre plusieurs entités qui forment un consortium (institutions financières ou entreprises, par exemple). L'accès en est donc limité aux entités membres de ce consortium et la validation des transactions est effectuée par eux sur la base de règles de type « vote majoritaire » : au moins la moitié des acteurs doivent valider les transactions.

- Les blockchains privées sont, elles, soumises à restriction d'accès et à une gouvernance centralisée. Pour les rejoindre, les participants doivent être préalablement acceptés par l'entité qui les administre. C'est cette entité centrale qui définit les règles de fonctionnement (droits d'écriture et de lecture) de la chaîne. C'est sans doute ce modèle de blockchain privée qui pourrait correspondre le mieux aux usages possibles pour la Défense.

Modes de validation

Les modes de validation des transactions sont les règles qui régissent le fonctionnement de la blockchain.

Dans le cas des blockchains publiques, le fonctionnement de la chaîne est assuré par les « mineurs », c'est-à-dre des individus (ou plutôt leurs machines) qui, en jouant le rôle de « nœuds » dans le réseau que constitue une blockchain, se chargent d'effectuer les calculs nécessaires à la validation des transactions et d'ajouter les blocs validés à la chaîne. La validation se fait essentiellement de deux façons :

- Par une « preuve de travail» (*proof of work*), un procédé cryptographique qui consiste à résoudre un problème mathématique complexe : le premier mineur qui réussi à résoudre le problème crée le prochain bloc et l'ajoute à la chaîne.
- Par une « preuve de détention» (*proof of stake*), qui demande aux mineurs de prouver la propriété d'un certain montant de cryptomonnaie ou d'un certain nombre d'actifs : la sélection du mineur est donc pondérée par la quantité de cryptomonnaie ou d'actifs qu'il possède.

Il existe néanmoins une trentaine d'autres méthodes de validation des transactions, moins connues et usitées, parmi lesquelles la « preuve d'autorité» (*proof of authority*), qui concerne les blockchains privées et de consortium. La preuve d'autorité consiste à définir à l'avance les nœuds qui feront autorité, donc qui seront en position d'ajouter des blocs. La blockchain, bien que restant distribuée, perd ainsi son caractère décentralisé.

Applications possibles de la blockchain pour la Défense

Les usages possibles de la technologie blockchain dans la Défense reposent sans doute principalement sur l'utilisation de blockchains privées, dont le fonctionnement et les accès seraient exclusivement déterminés et contrôlés par les services du ministère des Armées.

En dépit de quelques limites non négligeables (capacité de stockage limitée et vulnérabilité théorique à certaines attaques), la blockchain privée semble en effet présenter des caractéristiques indéniablement intéressantes pour la Défense française. Sa résilience (structure distribuée), sa disponibilité (données consultables à partir de chaque nœud de réseau) et son inviolabilité (une fois les données enregistrées dans les blocs, il est théoriquement impossible de les modifier) en font un atout significatif pour différentes applications. C'est la notion de sécurité et d'immuabilité qui la rend particulièrement pertinente pour le domaine militaire. La blockchain pourrait en effet offrir au secteur de la Défense une capacité de stockage des données ultra-sécurisé et consultable à tout instant par les individus accrédités.

- Messagerie sécurisée: une messagerie basée sur la blockchain pourrait présenter un intérêt pour les échanges internes aux Armées et, pourquoi pas, le partage rapide d'informations critiques en

opération. Ce dernier usage se heurte toutefois à la problématique de l'accessibilité aux réseaux sur certains théâtres d'opération.

- Gestion des identités numériques: un registre sécurisé des identités numériques des combattants pourrait par exemple être utilisé pour homogénéiser, si ce n'est remplacer, des documents tels que les journaux de marche de l'armée de Terre, les carnets de vols de l'armée de l'Air et les journaux de bord de la Marine. Une blockchain offrirait une base de données sécurisée et distribuée entre les différentes unités et consultable à tout moment par les participants à la chaîne. Elle permettrait également la validation (quasi) instantanée de la présence des combattants sur les théâtres d'opération.
- Logistique et suivi du matériel sensible: les Armées pourraient profiter d'un registre unique mais partagé de chaque transaction effectuée tout au long de leurs chaînes logistiques, notamment dans le cadre du suivi du matériel sensible (armes, substances toxiques, etc.). Chaque opération impliquant les pièces et les matériaux utilisés serait donc enregistrée et horodatée. En cas de problème ou de dysfonctionnement, cette traçabilité améliorée offrirait la possibilité de retrouver la pièce défectueuse et de connaître beaucoup plus rapidement et facilement le moment exact de son entrée dans la chaîne et son parcours tout au long de celle-ci.

2. PANORAMA DE L'ECOSYSTEME INDIEN DE LA CYBERSECURITE

L'Inde figure aujourd'hui parmi les pays les plus ciblés et les plus vulnérables aux cyberattaques. En 2017, l'Inde était le 2e pays le plus atteint par les attaques ciblées et les *malwares* visant les mobiles, le 4e pays le plus touché par les rançongiciels[1], et le 3e pays le plus affecté par *Wannacry*[2].

Pourtant, l'Inde a assez rapidement identifié la cybersécurité comme un enjeu majeur. Dès 2000 elle adopte l'*Information Act*, révisé et complété en 2008 pour devenir l'*Information Technology (Amendment) Bill.* La même année, l'*Indian Computer Emergency Response Team* (CERT-In) créé en 2004 voit ses prérogatives s'étendre de la simple réponse aux incidents à la collecte, l'analyse et le partage d'informations, l'anticipation et l'alerte la prise de mesures d'urgence et la coordination de la réponse à incident[3]. En 2013, la *National Cybersecurity Policy* (NCSP), non contraignante, appelle quant à elle, à la protection des informations et des infrastructures du cyberespace ou encore le développement des capacités de défense.

Les dirigeants indiens ont en effet bien conscience de l'effort à fournir pour protéger les systèmes d'information (SI) nationaux et développer une filière industrielle indienne de la cybersécurité. C'est tout l'objet des initiatives « *Make in India* » (2014) et « *Digital India* » (2015). La première vise à faciliter l'investissement et l'innovation, à protéger la propriété intellectuelle, et à encourager la construction d'infrastructures dédiées à la production de matériel informatique (*hardware)*. La seconde prévoit d'augmenter les services gouvernementaux en ligne et d'améliorer l'accès à internet des citoyens.

Les résultats de ces efforts pourraient cependant être longs à émerger. Le manque d'organisation et de coordination entre les entités gouvernementales chargées de la cybersécurité, l'absence d'agence nationale de la sécurité des systèmes d'information et la collaboration encore insuffisante entre acteurs publics et privés ralentissent et limitent en effet l'efficacité des politiques lancées.

La cybersécurité en inde : une accumulation d'acteurs étatiques aux prérogatives redondantes

Au niveau gouvernemental, les politiques et structures nationales chargées de la cybersécurité sont chapeautées par quatre organes :

- Le **MeitY**, le ministère de l'Électronique et des Technologies de l'Information, dont dépend notamment le CERT-IN et le conseil d'administration en charge des certifications de qualité et de conformité[4];
- Le **ministère de l'Intérieur** qui encadre des forces de police spécialisées dans la cybercriminalité ;
- Le **ministère de la Défense** dispose lui de deux structures de recherche : la *Defence Information Assurance and Research Agency* et la *Defence Research and Development Organisation* (DRDO). Certains laboratoires de la DRDO se spécialisent sur les problématiques IT telles que la gestion de la sécurité de l'information, l'intelligence artificielle, l'extraction de données ou encore les technologies de cybersécurité[5]. La DRDO développe également des outils souverains pour le ministère de la Défense indien tels que des radios logicielles[6]. Parallèlement, chacun des trois corps d'armée, fonctionnant de manière cloisonnée, s'est doté de ses propres unités spécialisées pour ses réseaux.
- Le ***National Security Advisor***, rattaché au cabinet du Premier ministre, dirige la *National Technical Research Organisation* chargée de prendre les mesures nécessaires pour protéger les infrastructures critiques et faire face aux cyber-incidents dans les secteurs critiques[7].

Chaque ministère intervient via ses structures dédiées et espère s'illustrer dans le domaine de la cybersécurité sans coordonner ses actions avec celles des autres ministères et sans se soucier de leur éventuelle redondance. La cybercriminalité par exemple, est traitée à plusieurs niveaux. Ainsi, le ministère de l'Intérieur a pris des mesures de prévention des actes de cybercriminalité à l'encontre des femmes et des enfants (*Cyber-Crime Prevention against Women & Children* – CCPWC) tandis que le *National Cybersecurity Coordination Centre* (NCCC) du MeitY lutte quant à lui contre la cybercriminalité à travers la surveillance des flux sur les réseaux privés et publics et l'analyse des métadonnées des communications[8].

L'absence de structure nationale spécifique à la gestion du cyberespace, telle l'ANSSI* en France, permettant précisément d'orienter et de coordonner le travail des acteurs existants, explique en partie cette situation. Cette structure surplombante est pourtant réclamée aussi bien par des organes de l'État que par des sociétés privées (le *Data Security Council of India* ou la *National Association of Softwares and Services Companies*)[9].

Ce manque de coordination est enfin aggravé par le caractère embryonnaire de la collaboration public-privé. Le volet défense de la campagne « *Make in India* » qui devait faciliter l'accès des sociétés privées (nationales ou étrangères) à l'industrie de la défense, et permettre aux industries de soumettre des suggestions, pourrait cependant partiellement pallier le manque de collaboration entre les secteurs public et le privé.

Les acteurs privés de la cybersécurité indienne : vers une filière indienne de la cybersécurité

L'un des volets de la politique « Make in India » prévoit, à terme, la réduction de la dépendance indienne vis-à-vis des importations en technologies de l'information d'ici à 2025 au profit du développement de matériels et de logiciels conçus et produits en Inde pour le marché indien.

Mais la mise en œuvre de cette politique est ralentie par la structure même de l'industrie indienne essentiellement composée de petites et moyennes entreprises qui ne détiennent pas les ressources nécessaires pour attirer les employés les plus qualifiés ou mener les changements structurels nécessaires à la production *in situ* de matériels informatiques (*hardwares*).

Toutefois, l'Inde demeure un pays propice au développement de logiciels et d'applications, notamment grâce à son économie basée principalement sur les services et à une main-d'œuvre foisonnante dans le domaine des technologies de l'information. L'investissement dans les *startups* indiennes a atteint 100 millions de dollars en 2017 (contre 1 million en 2012) et a favorisé leur émergence dans le domaine. On peut ainsi citer des sociétés comme *Security Brigade*, spécialisée dans la sécurité des applications ou *Lucideus technologies* qui propose des formations, des services SOC et des tests d'intrusion et de vulnérabilité[10]. Malgré les financements reçus et l'accès à une main d'œuvre qualifiée, ces sociétés n'ont cependant pas atteint les marchés mondiaux. L'Inde compte également des SSII de rang international telles qu'*Infosys*, *Tata Consultancy Services* ou *3i Infotech.* Des pures players de la cybersécurité se distinguent enfin, tels que *Hicube,* qui vend des solutions VA/PT à plusieurs administrations de police, ou *Cyberoam* qui produit notamment des routeurs, pare-feux, UTM…[11]

Dans un contexte marqué d'une part par des cyberattaques régulières et d'autre part par l'essor des services en lignes prévu par la campagne « Digital India », la demande en services de cybersécurité croît dans tous les secteurs (gouvernements, grandes industries automobile ou IT, banques et compagnies d'assurance) et pourrait donc bénéficier aux sociétés indiennes. Deux autres initiatives récentes devraient leur permettre de

trouver de nouveaux débouchés et de diversifier leurs solutions, tout en les contraignant à plus de rigueur.[12] D'abord en 2017, la décision du MeitY d'appliquer un critère de préférence nationale dans l'acquisition de solutions logicielles et matérielles de cybersécurité par tous les ministères, conformément aux orientations de l'initiative « Make In India ». Ensuite, la publication en juillet 2018 d'une version préliminaire de la *Personal Data Protection Bill*[13] destinée à clarifier les statuts juridiques de la vie privée et de la protection des données et renforcer ainsi un cadre normatif flou et peu contraignant. Celui-ci constituait en effet un enjeu de taille pour l'Inde, principale destination de l'*outsourcing* des sociétés étrangères d'IT[14].

Perspectives

Tandis que l'absence d'agence nationale en charge de la cybersécurité freine l'exécution des politiques nationales, l'Inde ne semble pas pour le moment être en mesure de remédier à la juxtaposition d'infrastructures de cybersécurité aux activités redondantes. La filière nationale de la cybersécurité, encore en cours de constitution, est malgré tout soutenue par l'Etat indien et pourrait à terme se développer à l'international.

En matière de cyberdéfense, le ministère de la Défense entend toujours concrétiser la mise en place du *Tri-service Cyber Command*, une structure de cybersécurité interarmées évoquée depuis 2014 destinée à remédier au cloisonnement des trois corps et dont l'existence est d'autant plus nécessaire que la notion de guerre cyber figure désormais dans la version préliminaire de la *Defence Production Policy* de 2018[15].

La politique de coopérations internationales et principalement bilatérales avec des partenaires européens, américains ou asiatiques dans des domaines comme le partage de connaissances et d'expériences en matière de détection, de résolution et de prévention,[16] pourrait toutefois permettre à l'Inde de monter en compétences[17] et de développer ses capacités de cyberdéfense malgré ces limitations organisationnelles et structurelles.[18]

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[2] *Wannacry* est un rançongiciel qui tirait profit d'une faille du système d'exploitation Windows XP.

[3] http://meity.gov.in/content/icert

[4] https://www.opengovasia.com/article/indian-ministry-of-defence-plans-to-strengthen-the-countrys-cybersecurity et http://meity.gov.in/content/icert

[5] https://www.drdo.gov.in/drdo/English/index.jsp?pg=dg-med-and-cos.jsp

[6] https://www.drdo.gov.in/drdo/labs1/DEAL/English/indexnew.jsp?pg=homepage.jsp

[7] http://www.pib.nic.in/PressReleseDetail.aspx?PRID=1540827

[8] https://www.opengovasia.com/article/the-current-state-of-cyber-security-in-india et https://www.indiatoday.in/education-today/gk-current-affairs/story/nccc-cyber-india-1029203-2017-08-11

[9] https://www.dsci.in/content/gulshan-rai-becomes-first-chief-cyber-security-post-created-tackle-growing-e-threats-0

[10] https://www.securitybrigade.com/ et http://www.lucideus.com/service/

[11] http://www.hicube.in/ ; https://www.cyberoam.com/

[12] https://www.thehindubusinessline.com/info-tech/cyber-security-start-ups-attract-big-funding/article24381880.ece

[13] https://www.forbes.com/sites/sindhujabalaji/2018/08/03/india-finally-has-a-data-privacy-framework-what-does-it-mean-for-its-billion-dollar-tech-industry/#4371ba1a70fe

[14] https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-4/1151286/india; des sociétés de l'IT américaines (IBM, Dell, HP) et européennes (Capgemini) sont implantées en Inde (https://www.silicon.fr/superpuissance-outsourcing-inde-controle-56-mondial-146988.html?inf_by=57923adb2ad0a1b0274846e7).

[15] https://currentaffairs.gktoday.in/tags/defence-cyber-agency et

[16] https://www.bestcurrentaffairs.com/india-uk-mou-cyber-security/

[17]L'Inde approfondit surtout ses relations avec Israël dans le domaine de la cybersécurité notamment pour bénéficier des investissements et l'innovation israéliens https://economictimes.indiatimes.com/news/politics-and-nation/india-israel-ink-nine-pacts-on-cyber-security-other-sectors/articleshow/62507272.cms

[18] L'*Israel National Cyber Directorate* (INCD) voudrait même collaborer avec l'Inde pour l'édification de cyber-boucliers étatiques https://tech.economictimes.indiatimes.com/news/corporate/israel-looks-to-collaborate-with-india-other-countries-to-build-cyber-shields/64802121

FOCUS INNOVATION : QUARKSLAB, IDENTIFIER, EVALUER ET COMPRENDRE LES MENACES ET LES VULNERABILITES, MATERIELLES ET LOGICIELLES

Entretien avec Eric Houdet, Business Development Manager chez Quarkslab

Présentation : un modèle de développement original

- Quarkslab, créée en 2011 par Fred Raynal (ex MISC, SSTIC, Airbus, et Sogeti), est une PME d'une cinquantaine de personnes dont le siège social est situé à Paris. Les ingénieurs sont répartis sur l'ensemble du territoire national ainsi que sur divers sites en Argentine et au Japon.
- Société jusqu'à présent autofinancée donc 100% indépendante, elle compte parmi ses clients de grands acteurs privés ou publics, en France (comme le ministère des Armées) comme à l'international (notamment aux Etats-Unis).
- Laboratoire de R&D privé dédié à la Sécurité informatique, Quarkslab s'est initialement financé grâce au conseil puis a étendu ses activités à l'édition de logiciels. Elle a notamment développé une plateforme d'analyse de malware (IRMA) et une solution d'obfuscation des codes développée grâce au dispositif RAPID de la DGA (EPONA).

Une approche intégrée de la sécurité

- Convaincue qu'une bonne compréhension des attaques et des attaquants est essentielle à l'élaboration de solutions de défense, et de protection performantes et adaptées, Quarkslab a, dès ses débuts, adopté une démarche de sécurisation active et continue couvrant toute la chaîne de la sécurité.
- Ses solutions permettent ainsi d'identifier, évaluer et comprendre les menaces et les vulnérabilités tant matérielles que logicielles, et de concevoir des systèmes (architectures, codes, matériel) sécurisés.
- La rétro-ingénierie et la recherche de vulnérabilités, notamment au travers de tests de robustesse, sont au cœur de ses activités. Spécialiste de sécurité logicielle, Quarkslab travaille de plus en plus les couches matérielles et cible particulièrement les véhicules connectés et/ou autonomes. Pour ce faire, Quarkslab a même créé une *Joint Venture* au Japon avec un grand équipementier du monde automobile.

Focus : Epona, solution de protection logicielle des applications

Epona est un compileur qui intègre des solutions innovantes de protection des applications permettant de garantir l'intégrité et l'inviolabilité du code. Epona intègre ainsi des solutions d'obfuscation qui empêchent les attaquants de comprendre le fonctionnement des applications, des solutions de vérification d'intégrité qui protègent contre toute modifications du code, et des solutions d'anti de-bugging pour empêcher l'analyse dynamique du code.

Perspectives

- En septembre 2018, Quarkslab a été sélectionné par Thales pour rejoindre la saison 2 du programme cybersécurité de son incubateur au sein de Station F.
- Pendant 6 mois, Quarkslab bénéficiera des conseils et de l'expertise de coaches de Thales qui l'accompagneront dans la valorisation de ses technologies et dans la mise en place de stratégies commerciales et de marketing.
- Cette expérience permettra à Quarkslab d'accélérer son développement en France et à l'international, et d'accéder aux marchés du groupe Thales ainsi qu'à son écosystème.

ACTUALITE

Séminaire Annuel de la French American Foundation

Alors que les enjeux de cybersécurité représentent une priorité grandissante pour la France comme pour les États-Unis, la French-American Foundation organise depuis 2014 à Washington une conférence annuelle dédiée à ces questions.

Cet événement rassemble des hauts responsables des gouvernements européens et américains, ainsi que des experts et des acteurs industriels de la cybersécurité, qui sont ainsi invités à échanger et débattre sur ces questions.

Présidée par le Général Paloméros, la 5ème édition qui s'est tenue les 25 et 26 septembre 2018 a notamment accueilli le Général Olivier Bonnet de Paillerets, Commandant de la Cyberdéfense français, le Lieutenant General Vincent Steward, Adjoint au Commandant de la Cyberdéfense des États-Unis, ainsi que Walter Copan, Sous-secrétaire d'État américain au Commerce pour la technologie.

Après 4 éditions dédiées respectivement au traitement judiciaire de la cybercriminalité; la gestion des risques cyber ; la cybersécurité et la menace terroriste ; et la sécurité de l'information et les technologies émergentes, l'édition 2018 portait cette fois sur la cybersécurité et l'identité numérique.

La manifestation s'est ouverte sur une analyse de l'évolution des priorités des gouvernements français et américains en matière de cybersécurité avant de laisser place à des tables rondes qui ont abordé les nombreux défis liés aux identités numériques. Parmi les sujets traités figuraient par exemple le rôle du cloud dans un environnement transnational marqué par une grande diversité de régimes législatifs et réglementaires, la menace aux systèmes démocratiques que constituent les fausses identités, ou encore la risque représenté par les fake news et leur propagation via les médias sociaux. En conclusion, cette 5ème édition a énoncé quelques recommandations pour protéger les démocraties face à ces défis.

CALENDRIER

Université d'été d'Hexatrust

Hexatrust organise le 4 septembre prochain sa 4ème Université de la Défense. Lieu de rencontre privilégié et de networking, l'Université d'été sera l'occasion d'échanges entre experts du secteur sur les sujets suivants :

- IA & Cybersécurité : buzzword ou réalité ?
- La donnée, pourquoi et comment protéger cette ressource numérique ?
- Security by design, un nouveau standard de compétitivité.

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