Lettre mensuelle – Juin 2019 - disponible sur omc.ceis.eu

Table des matières

ANALYSES

1. LES ROUTES DE LA SOIE NUMERIQUES : UNE PROJECTION EXTRA TERRITORIALE DE LA CYBERDEFENSE CHINOISE ?

Lancées dès 2013 par le Président chinois XI Jinping, les (Nouvelles) Routes de la Soie[1], constituent un programme d'aménagement transfrontalier chinois financé essentiellement par la Chine et dont l'objectif officiel est de faciliter le financement d'infrastructures terrestres (routes, ponts, chemins de fer, oléoducs et centrales électriques) reliant les continents européen, africain, américain et l'Extrême-Orient. Concrètement, nombre des infrastructures réalisées ou en projet ont pour terminaison le territoire chinois.

Les Routes de la Soie numériques, quant à elles, ont été introduites deux ans plus tard, en 2015, au moment où les Routes de la Soie deviennent aussi maritimes (ports) et aériennes, voire spatiales. La « numérisation » des Routes participe de l'élargissement des domaines couverts par cette initiative. A travers les Routes de la Soie numérique, la Chine entend :

- Améliorer la coopération entre les États pour le développement de normes communes et la progression des politiques en matière de nouvelles technologies ;
- Établir une connectivité continue, de la même manière que les Routes de la Soie terrestres et maritimes entendaient créer une continuité des voies de communications ;
- Favoriser l'implantation de sociétés chinoises du numérique à l'étranger ;
- Recréer, *in fine,* une concurrence sur le marché avec les États-Unis.

Au-delà des dimensions libérales et développementaliste des Routes de la Soie numériques, il existe cependant une volonté de contrôle des infrastructures, des contenus et des données.

Les Routes de la Soie numériques, instrument de collecte des données et de contrôle des infrastructures

Les Routes de la Soie numériques englobent des projets de natures diverses, allant du e-commerce au paiement mobile en passant par les câbles sous-marins. Les projets de e-commerce, développés avec des pays tels que la Turquie à travers DHGate, une plateforme de *Business to Business* (B2B), et les projets de paiement mobile, *via* le service Alipay présent en France, constituent des mannes de *data* concernant les individus et les foyers de dépenses locaux. Les projets les plus remarquables sont le développement du système de navigation chinois BeiDou- 2 qui reposera sur 35 à 40 satellites d'ici 2020, ou encore la construction de câbles sous-marins par *Huawei Marine*.

On observe ainsi deux phénomènes :

- D'une part les Routes de la Soie numériques permettent à la Chine de déployer des vecteurs de récolte de *data* de type applications et plateformes de vente en ligne ;

[1] « 一带一路 » en chinois, signifiant « Une ceinture, une route ».

- D'autre part, les infrastructures ainsi déployées proposent une alternative aux infrastructures et aux réseaux américains (GPS – *Global Positioning System* et les câbles sous-marins Equinix).

En ce sens, la Chine propose déjà ses infrastructures réseau à l'étranger : le Pakistan, le Laos, Brunei et la Thaïlande, entre autres, sont déjà des utilisateurs du système de navigation BeiDou[2]. De même, depuis 2017, Huawei Marine construit des câbles sous-marins pour l'Indonésie (*Indonesia Global Gateway System* et les *Palapa Rings*), les Philippines (*Palawa-Iloilo Cable System*) et pour le Pakistan (*Pakistan East Africa Cable Express* et le *Silk Route Gateway SRG-1*). Un câble reliant l'Asie du sud-est à la France en passant par l'Inde, la Péninsule arabique et le canal de Suez est en outre déjà opérationnel : le Asia Africa Europe-1 – AAE-1 (2017). Le contrôle des infrastructures physiques d'Internet (câbles, antennes 5G, centrales électriques entre autres) confère à la Chine un avantage commercial et stratégique sur ses partenaires, lui permet de surveiller les données qui y circulent et, de surcroît, lui donne la faculté d'agir sur la disponibilité des réseaux.

Les Routes de la Soie numériques sont aussi pour la Chine l'occasion d'afficher sa volonté de prendre part à l'élaboration de normes internationales en matière de nouvelles technologies, car, à l'image de l'Union européenne, elle se voudrait un modèle normatif en matière de technologies de l'information. La Chine s'appuie pour cela sur l'Organisation de coopération de Shanghai (OCS) pour la rédaction de proposition de code de conduite dans le cyberespace, mais aussi sur les contrats qu'elle établit avec ses partenaires internationaux. L'exemple de la 5G est significatif puisqu'il s'est aussi agi pour Huawei d'imposer ses standards de la 5G[3] : la Chine exporte ses propres critères de sécurité des technologies de l'information, élaborés par des institutions civiles qui dépendent – entre autres institutions du Conseil des Affaires d'État – de l'Administration de certification et d'accréditation (国家认证认可监督管理委员会)[4]. En d'autres termes, les Routes de la Soie numériques sont parties prenantes dans la lutte d'influence qui oppose la Chine aux États-Unis.

La présence du Parti communiste et de l'Etat chinois au sein des sociétés chinoises du numérique

Les Routes de la Soie numériques consistent à exporter les normes, services et matériels chinois, et s'accompagnent d'une implantation de sociétés chinoises à l'étranger. Or, la majorité des sociétés chinoises comptent parmi leurs dirigeants des membres du Parti communiste ou des personnalités menant des activités politiques qui jouent le rôle de relai entre les autorités et la société.

L'exemple le plus significatif est celui de la société Huawei, dont la présidente jusqu'en 2018, SUN Yafang (孙亚芳) est une ancienne responsable du ministère de la Sécurité de l'État. Mais cette règle s'applique à d'autres sociétés. SUN Pishu (孙丕恕), le dirigeant de la société INSPUR (浪潮集团)[5], une entreprise publique chinoise de *cloud computing* et de gestion du *Big Data* présente en Mauritanie, au Mozambique, en Zambie, au Sierra Leone, en Russie, au Vietnam et en Thaïlande, est aussi secrétaire du « comité du Parti » de sa société.

[2] http://www.ecns.cn/news/cns-wire/2018-12-27/detail-ifzccnsu7721145.shtml

[3] http://www.chinadaily.com.cn/a/201905/17/WS5cdeaa09a3104842260bc56f.html

[4] Le Conseil des Affaires d'Etat est l'organe exécutif le plus important dans le système politique chinois.

[5] http://en.inspur.com

Ces comités ont pour fonction d'assurer la conformité de la société avec les directives du Comité central du Parti et des différentes institutions chargées des normes, de la surveillance des comptes etc.

Dans d'autres sociétés, l'équipe dirigeante est membre de commissions de réflexion et d'élaboration de normes pour les technologies de cybersécurité. Ainsi, le PDG de la société de cybersécurité et de cyberdéfense ANTIY (北京安天网络安全技术)[6], XIAO Xinguang (肖新光), membre du comité national de la Conférence consultative politique du peuple chinois[7], organe qui prend part à l'élaboration des politiques publiques.

Les sociétés chinoises du numériques sont, par conséquent, liées soit au Parti communiste soit à des institutions d'État, leurs projets sont probablement cohérents avec des stratégies plus larges élaborées par les dirigeants chinois. Ce dispositif est aussi, à bien des égards, un moyen pour la Chine d'avancer ses objectifs en matière de cyberdéfense.

L'inscription des Routes de la Soie numériques dans la cyberdéfense chinoise

La cybersécurité en Chine est devenue indissociable de la cyberdéfense. En effet, le président chinois, XI Jinping, a annoncé la tonalité que prendrait la cybersécurité chinoise dès 2014 en déclarant qu'il « ne peut y avoir de sécurité de l'État sans cybersécurité »[8]. Cette déclaration est cohérente avec la conception chinoise de la souveraineté dans le cyberespace, souveraineté qui se manifeste à la fois par un contrôle institutionnel et institutionnalisé des contenus et des flux, et par une certaine imperméabilité du réseau national (*Great Firewall*).

En ce sens, les sociétés de cybersécurité chinoises participent activement au contrôle des contenus sur le web continental. La stratégie d'intégration du civil et du militaire et la loi sur le renseignement de 2017 fournissent en effet un cadre juridique à la participation des sociétés (et des utilisateurs) dans les activités de renseignement. L'article 12 de la loi sur le renseignement prévoit notamment la possibilité pour les services de renseignement de demander aux individus et aux organisations de coopérer dans le cadre de missions de renseignement[9].

Les sociétés chinoises de cybersécurité mettent également leurs technologies – notamment en matière de surveillance – et leurs données, à disposition de l'Armée populaire de libération (APL) dans le cadre de la stratégie d'intégration des technologies civiles et militaires. Cette stratégie est supervisée par la Commission centrale pour le développement intégré du civil et du militaire créée en janvier 2017 et dirigée par le président chinois, XI Jinping[10]. Autrement dit, toute société chinoise localisée à l'étranger peut se voir demander, légalement, de soumettre les données de ses clients étrangers aux autorités chinoises. Dans le cadre des sociétés de cybersécurité, les données partagées pourraient n'être autres que les vulnérabilités des réseaux de leurs clients, ou encore leurs *indicators of compromise* (IOCs). Considérant que les dirigeants de ces sociétés sont liés aux autorités, nous pouvons gager qu'ils coopéreront.

---

[6] https://www.antiy.cn/About/index.html

[7] 中国人民政治协商会议

[8] http://www.cac.gov.cn/2014-02/27/c_133148354.htm

[9] http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm

[10] http://french.xinhuanet.com/2017-01/22/c_136004598.htm

Conclusion

En définitive, la stratégie numérique chinoise est un jeu délicat qui, même soutenue par un discours de non-ingérence, parvient de plus en plus difficilement à cacher les objectifs du gouvernement chinois d'intrusion dans les systèmes d'information de pays tiers. La projection des sociétés chinoises à l'étranger est, en outre, de plus en plus perçue comme une menace. Le refus de l'Australie et de la Nouvelle-Zélande d'installer la 5G de Huawei illustre ce glissement de la perception de la Chine d'investisseur bénéfique à attaquant en puissance[11].

Quoique fondées, ces inquiétudes ne devraient pas être réservées aux matériels et logiciels chinois. Rappelons en effet que tant que l'Union européenne et la France en particulier ne se seront pas dotées de champions industriels du numériques, elles continueront de dépendre de logiciels et de matériels étrangers. Dans ce contexte, la construction d'une Europe plus autonome sur les plans matériels et logiciels semble dorénavant impérative.

[11] https://www.scmp.com/week-asia/geopolitics/article/2186402/new-zealand-bans-huawei-china-has-message-new-zealand et https://www.scmp.com/economy/china-economy/article/3003715/australias-huawei-5g-ban-hedge-against-future-chinese

2. TLS 1.3 ET DNS CHIFFRE : QUELS IMPACTS POUR LE MONITORING DES RESEAUX DES ORGANISATIONS ?

Les protocoles réseau qui sous-tendent la navigation Internet évoluent. Les protocoles de communication qui étaient jusque-là dépourvus de chiffrement, en acquièrent, et la robustesse de celui-ci se renforce pour les autres. L'IETF[12] a validé l'année dernière la version 1.3 du protocole TLS, qui permet le chiffrement des données de navigation HTTPS, et son déploiement est soutenu par Google et Mozilla qui le prennent déjà en charge dans leur navigateur. D'autre part, ces mêmes acteurs soutiennent également les protocoles DNS chiffrés que sont DoT (DNS over TLS) et DoH (DNS over HTTPS).

Si le chiffrement permet généralement un renforcement de la sécurité des échanges légitimes, il va cependant compliquer la tâche de surveillance du réseau à la recherche de flux malicieux.

Le déploiement de ces protocoles n'en est encore qu'à ses balbutiements, mais il semble bien enclenché. Quels sont les apports concrets de ces nouveaux protocoles et quelles conséquences leur déploiement aurait-il pour la sécurité interne des organisations ?

Du TLS 1.2 au TLS 1.3

En mars 2018, 10 ans après la publication de TLS 1.2, l'IETF a approuvé la norme TLS 1.3. Ses principaux apports sont les suivants :

Une amélioration des performances. Le protocole TLS 1.3 ne nécessite qu'un seul aller-retour entre le client et le serveur pour établir une session sécurisée, là où la version 1.2 en nécessitait deux.

Une sécurité du chiffrement renforcée : Tous les protocoles de chiffrement obsolètes intégrés à TLS disparaissent se voient disparaître. En effet, lors de l'établissement d'une session TLS, le client et le serveur doivent commencer par s'accorder sur le protocole de chiffrement à utiliser. Il était important de faire disparaître ces protocoles, pour éviter les attaques alors courantes consistant à "convaincre" les cibles d'utiliser un protocole de chiffrement plus faible pour permettre l'écoute malveillantes d'une session TLS. Parmi les protocoles restants, tous offrent la confidentialité persistante (Forward Secrecy), ce qui signifie que la compromission de la clé privée du serveur ne compromet pas la confidentialité de l'ensemble des communications passées.

Jusqu'au protocole TLS 1.2, le plus répandu aujourd'hui, les solutions de sécurité internes aux organisations pouvaient se contenter d'une écoute passive du réseau pour surveiller le contenu des sessions TLS à destination de leurs serveurs. Il suffisait d'intégrer à la solution de sécurité la clé privée du serveur à protéger et de lui envoyer une copie du trafic réseau (mirroring). L'outil pouvait alors choisir les paquets à déchiffrer pour inspection, de façon complètement transparente pour les participants à la session TLS.

Du fait, du choix de n'intégrer dans TLS 1.3 que des protocoles de chiffrement PFS (Perfect Forward Secrecy), cette technique n'est plus applicable. Il devient nécessaire, pour inspecter les flux TLS, de placer la solution entre le client et le serveur, ce qui nécessite de déchiffrer et re-chiffrer l'ensemble de leurs échanges. Concrètement, la solution de sécurité devient un intermédiaire car elle établit deux sessions TLS : l'une avec le client, l'autre avec le serveur, ce qui n'est pas sans impact sur les performances de la session client/serveur. Et ce d'autant que cette technique doit être mise en œuvre dès l'ouverture de la session. De ce fait, il faudra

[12] (Internet Engineering Task Force – groupe de normalisation rattaché à l'Internet Society)

généralement systématiser le procédé, une opération au coût computationnel qui peut être considérable selon les cas.

Les protocoles de chiffrement DNS : DoT et DoH

Les détournements DNS massifs révélés fin 2018 ont incité l'ICANN[13] à réagir en encourageant le déploiement global du protocole DNSSEC[14]. Celui-ci permet de répondre partiellement à la problématique des détournements DNS en établissant une chaîne de confiance entre les serveurs racines DNS et l'utilisateur final. Cependant, la réalité du schéma de déploiement de DNSSEC par les opérateurs (qui sont tentés de le dénaturer afin d'éviter d'éventuels échecs de résolution), couplé à l'absence de sa prise en charge par les navigateurs, prive l'utilisateur du dernier maillon de la chaîne de confiance du DNSSEC. En outre, le protocole DNSSEC n'intègre aucune fonctionnalité de chiffrement du contenu des échanges DNS, qu'il s'agisse des requêtes ou des réponses, ce qui ouvre la porte à d'éventuelles interceptions.

Le chiffrement des requêtes et réponses DNS qu'apportent ces nouveaux protocoles séduit pour plusieurs raisons :

- Il apporte une garantie de protection de la vie privée des utilisateurs, dont les données de navigation ne sont plus accessibles aux acteurs qui contrôlent ne serait-ce qu'un seul élément réseau entre le poste client et son résolveur DNS. Notons cependant que le propriétaire du résolveur DNS (FAI, GAFAM par exemple) a toujours pour sa part accès à ces données. A ce titre, il n'est donc sans doute pas surprenant que Google et Cloudflare s'empressent d'intégrer ces nouveaux protocoles de DNS chiffrés et en fassent la promotion ;
- Il assure l'intégrité des échanges DNS entre le client et son résolveur DNS. Les données n'étant pas lisibles par un hypothétique attaquant sur le réseau, elles ne peuvent pas être modifiées de façon à tromper l'utilisateur. Le chiffrement des requêtes et réponses DNS apporte donc une sécurité renforcée de la navigation, ainsi que de tout autre type de communication par Internet faisant usage du DNS.

Historiquement, DNSCrypt est le premier protocole de DNS chiffré à avoir été développé et déployé (principalement par OpenDNS, depuis racheté par Cisco). Cependant, ce sont aujourd'hui les protocoles DoT (DNS over TLS) et DoH (DNS over HTTPS) qui ont le vent en poupe, ayant été adoptés comme standards par l'IETF et étant soutenus par des acteurs majeurs du numérique tels que Google, Mozilla et Cloudflare (Mozilla et Cloudflare ont un partenariat pour le développement de DoT).

La différence majeure entre DoT et DoH réside dans le port utilisé, et ceci intéresse directement la surveillance du réseau :

- Le DoT utilise un port réseau spécifique (le 853), ce qui facilite le monitoring légitime des organisations en interne, en permettant de distinguer le flux DNS ;
- Le DoH, comme son nom l'indique, se mêle au trafic HTTPS du port 443. Il vise spécifiquement à empêcher la surveillance du réseau, partant du principe que l'adversaire (notamment quand il s'agit

[13] Internet Corporation for Assigned Names and Numbers, autorité de régulation de l'Internet

[14] Domain Name System Security Extensions, un protocole standardisé qui permet de résoudre plusieurs problèmes de sécurité liés au protocole DNS.

d'un acteur étatique) ne pourra pas se permettre de couper le trafic HTTPS – donc Internet, et donc perdra sa capacité à tracer la navigation de l'utilisateur qui l'emploie.

Les flux DNS font partie des premiers éléments qui intéressent les équipes de sécurité dans le cadre de la surveillance réseau d'une organisation. Face à ces nouveaux protocoles, celle dernière devra intégrer des solutions de sécurité adaptées à ceux-ci. Quoiqu'il en soit, le DoH impliquera nécessairement une majeure partie du trafic HTTPS afin de pouvoir continuer à surveiller les flux DNS.

Développement de solutions alternatives de surveillance des réseaux.

Face à la démocratisation des flux chiffrés, les outils de sécurité réseau commencent à intégrer des capacités d'analyse sans déchiffrement des flux. Il va s'agir de s'intéresser aux métadonnées intra-flux comme la longueur des messages ou l'intervalle de temps entre deux paquets, mais aussi par exemple aux données contenues dans le premier paquet de chaque flux, car il contient généralement des informations non chiffrées sur le flux. Evidemment, cela restera en-deçà des capacités d'analyse disponibles avec un flux qu'il est possible de déchiffrer.

Le développement de ces capacités d'analyse des flux chiffrés est d'autant plus important que les flux chiffrés malveillants bénéficient de la démocratisation des protocoles chiffrés, qui facilitent leur camouflage aux côtés des flux légitimes.

L'arrivée des protocoles de chiffrement DNS et du TLS 1.3 ne rend pas impossible la surveillance réseau, mais nécessitera certainement une adaptation, à savoir une révision de l'architecture de sécurité et le déploiement de produits prenant en compte les évolutions des protocoles. Les améliorations apportées par ces protocoles ont en effet un coût…

FOCUS INNOVATION

HARFANG LAB, HARFANGLAB, PLATEFORME DE DETECTION ET DE NEUTRALISATION DES CYBERATTAQUES

La société

Créée en avril 2018, la société HarfangLab est composée d'une équipe de 6 experts anciens de l'ANSSI, du ministère des Armées et de grands acteurs privés de la cybersécurité spécialistes de lutte informatique.

En partenariat avec la société Gatewatcher, leur solution d'investigation numérique à distance Hurukai a remporté en 2019 le défi cyber du ministère des Armées.

La technologie

Reflétant une approche intégrée de la cybersécurité sur les terminaux et serveurs d'un parc informatique, cette solution permet de combiner des capacités de :

- Détection (Remontée automatique d'informations des terminaux) ;
- Investigation (Qualification d'un incident de sécurité) ;
- Remédiation (Ciblage et élimination d'une menace).

Cette solution, duale par nature, est utilisable à la fois par les acteurs de la défense et par les acteurs civils, notamment dans les secteurs dits critiques ou stratégiques pour les opérateurs d'importance vitale (OIV) ou les opérateurs de services essentiels (OSE). Elle est ainsi utilisée à la fois par les RSSI comme instrument de maîtrise des risques et par les SOC et CSIRT comme un outil de détection des compromissions et d'appui à l'analyse dans le cas d'un incident de sécurité.

Cet outil se positionne ainsi sur le marché des EDR (Endpoint Detection and Response) qui est en forte croissance et traditionnellement dominé par des sociétés basées aux États-Unis.

HarfangLab se distingue par une solution :

- Conçue initialement pour être déployée au sein de l'infrastructure du client, c'est-à-dire « on premise», ce qui garantit ainsi à l'utilisateur le stockage en interne de ses données plutôt qu'un stockage sur un cloud externe pouvant être hébergé à l'étranger comme c'est le cas dans la plupart des solutions EDR américaines,
- Flexible, capable de fonctionner hors ligne et à distance, ce qui constitue un véritable avantage dans certains contextes opérationnels,
- Intuitive qui permet de baisser le niveau de qualification requis pour utiliser toutes les fonctionnalités.

Hurukai se distingue aussi par plusieurs technologies et dispositifs innovants

Les innovations

1. Une solution ouverte, caractérisée par la connexion native avec les sondes de Gatewatcher, qui permet d'enrichir automatiquement les alertes de la sonde réseau par les données de télémétrie issues de l'EDR afin d'accélérer la détection et la qualification des compromissions ;

2. Une plateforme d'investigation collaborative qui permet d'associer experts confirmés et opérateurs, à la fois sur les volets « analyse » et « qualification » des alertes, mais aussi dans le cadre d'activités de cyberdéfense comme le hunting (recherche de compromission proactive). Ce dispositif permet un gain de temps et d'efficacité. Il facilite la formation et la montée en compétences des opérateurs moins expérimentés.

3. Une solution intégrée qui couvre l'ensemble de la chaîne, de la détection à la remédiation en passant par l'investigation.

- Détection : la présentation des alertes sous forme d'arbres de processus permet de visualiser simplement les alertes. Un rapprochement automatique avec une base de renseignement sur la menace (Threat Intelligence) et le modèle MITRE ATT&CK apporte de la contextualisation à ces alertes.
- Investigation : le moteur d'analyse et de collecte intègre continuellement de nouveaux éléments techniques pour détecter les nouvelles menaces et les moyens de persistance. L'interface avec des outils tiers (base de réputation de malwares, sandbox…).
- Remédiation : l'utilisateur peut déclencher des opérations active pour neutraliser des menaces sur des terminaux ciblés (isolation) ou sur des groupes (neutralisation de process en mémoire, effacement de fichiers, modification de registres…).

Perspectives

- En février 2019, HarfangLab a été choisie par le comité de sélection du Village by CA Paris pour intégrer, avec 8 autres startups son programme d'accélération de 2 ans.
- En juin 2019, La solution d'HarfangLab a été sélectionnée par le jury des Assises de la cybersécurité parmi les trois solutions les plus innovantes sur plus de 20 candidatures.

CALENDRIER

04/07/2019 : Combattantes@Numériques 2019

Dans un contexte global de pénurie des talents dans le secteur du numérique, le déficit croissant de femmes est un phénomène aggravant malgré les efforts de l'ensemble des professionnels et associations.

La pénurie de talents est déjà vécue par la plupart des entreprises et grandes organisations et devrait s'intensifier dans les années à venir. La Défense a besoin de femmes qui s'engagent pour servir dans le Numérique.

Combattantes@Numérique est une communauté de professionnelles du numérique au sein du ministère des Armées. Elle œuvre à l'attractivité des métiers du numérique pour les femmes. Ouverte à tous et toutes, elle est composée de + de 100 femmes (chiffre de mars 2019) issues des filières numériques du ministère avec une représentation homogène de profils en matière de statuts (militaires, civils), classes d'âge et grades. L'initiative a été pensée pour accompagner le lancement de la Fondation Femmes@Numérique le 27 juin 2018.

L'édition 2019 de l'événement Combattantes@Numériques aura lieu le 4 juillet prochain à l'École militaire. Événement ouvert et en symbiose avec l'écosystème extérieur de la Défense et du numérique, il s'adresse à la fois à un public interne mais aussi externe, aux juniors comme aux plus séniors, avec un objectif de 400 participants.

Cet événement permettra de découvrir des femmes et rôles modèles de toute la diversité des filières du numérique. Il s'agit de mettre en place une prise de parole forte et récurrente alliée à un fort rayonnement médiatique dans un format innovant et attractif pour créer l'impulsion et donner envie.

Au programme de la journée :

LA MATINEE :

- Témoignages et roles modèles

L'APRES-MIDI :

- Speed dating géant
- Demos ethical hacking, iaIA et algos
- Ateliers codage et développement personnel
- Espace recrutement

2 invités surprises : T2R et MINISSIA, participeront à cet événement pour un showcase et une séance de dédicaces.

ACTUALITÉ

Lancement du nouveau kit de sensibilisation aux risques numériques de Cybermalveillance.gouv.fr

ACYMA a lancé le 13 juin 2019 la nouvelle version du kit de sensibilisation aux risques numériques de Cybermalveillance.gouv.fr.

Un an après la sortie du 1er volet du kit, cette nouvelle version s'enrichit de 5 nouveaux thèmes et de 4 nouveaux formats. Fruit d'une collaboration menée depuis plusieurs mois entre institutions publiques, organismes privés et associations membres du GIP ACYMA, et avec la contribution d'utilisateurs, cet outil s'adresse à tous les publics, que ce soit dans leurs usages professionnels ou personnels et quelles que soient leurs connaissances en sécurité du numérique.

Dans un contexte de recrudescence des cyber-attaques envers les particuliers et les professionnels, le kit de sensibilisation vise à sensibiliser et à partager les bonnes pratiques dans les usages personnels et, de manière vertueuse, à améliorer les usages dans le cadre professionnel.

Le kit contient ainsi :

- Six fiches pour adopter les bonnes pratiques :
  – Les mots de passe,
  – La sécurité sur les réseaux sociaux,
  – La sécurité des appareils mobiles,
  – Les sauvegardes,
  – Les mises à jour,
  – La sécurité des usages pro-perso.

- 3 fiches pour comprendre les risques et agir :
  – Le phishing

  – Les ransomware

  – L'arnaque au faux support technique

La nouveauté de ce volet complet réside également dans l'intégration de nouveaux formats adaptés à tous les publics, et propose ainsi une diversité de contenus et de supports qui contribue à la sensibilisation du plus grand nombre et permet ainsi au dispositif de répondre à sa mission de service public.

– 8 vidéos avec mises en situation et exemples,
– 1 quiz pour tester ses connaissances,
– 1 bande dessinée sur le thème « la sécurité sur les réseaux sociaux »,
– 9 mémos sur les thèmes du kit,
– 1 synthèse des mémos au format poster (A2),
– Des autocollants déclinés de la bande dessinée pour la version papier du kit.

Diffusés sous une licence ouverte pour en permettre la plus large diffusion, adaptation et réutilisation, les contenus ont été pensés pour être utilisés directement, pour servir de support à des actions de formation ou pour être intégrés à des initiatives déjà en place ou à venir. La version complète du kit de sensibilisation aux risques numériques est téléchargeable à l'adresse : https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/

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