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

Table des matières

ANALYSES

1. POLITIQUE INDUSTRIELLE DE CYBERSECURITE : UN ENJEU CLE POUR LA FRANCE

La dernière décennie a vu la prise de conscience, au niveau politique, de l'importance d'assurer la sécurité de nos systèmes d'informations pour garantir la résilience de la Nation, et de la nécessité de se doter de moyens techniques, technologiques et humains, nécessaires pour répondre à des cyber-menaces de plus en plus sophistiquées.

Pourquoi une politique industrielle est-elle indispensable

A mesure que la cybersécurité s'imposait comme un enjeu vital, une myriade de petites voire très petites entreprises, bien souvent issues du monde de la recherche, ont fait leur apparition sur ce marché en pleine mutation pour proposer des produits et services de cybersécurité. Quant aux acteurs traditionnels de la sécurité et de la défense, ils n'ont pas eu d'autre choix que d'intégrer ce nouvel impératif, soit en absorbant les solutions développées par ces nouveaux acteurs, soit en développant leurs propres solutions. Le paysage industriel, ainsi que l'offre et le profil des sociétés le composant, se sont donc considérablement transformés à mesure que s'imposait ce nouvel enjeu sécuritaire. Une transformation qui s'est la plupart du temps effectuée par le seul jeu des forces du marché, sans coordination ni planification, et donc sans réelle politique industrielle.

Or malgré des besoins croissants et un marché en forte progression, force est de constater que le secteur privé n'est pas en mesure de répondre de façon autonome aux enjeux de résilience sociétale et d'autonomie stratégique que sous-tendent la cybersécurité. Les raisons en sont multiples : lourdeur des investissements en R&D nécessaires (à l'instar des autres domaines de « deep technology »), dispositifs de financement de l'innovation inadaptés, forte concurrence anglo-saxonne, marché national étriqué, fragmentation des marchés européens, écosystème industriel encore trop peu structuré etc.

La mise en place d'une véritable politique industrielle, qui peut être définie comme un « *ensemble de mesures interventionnistes des pouvoirs publics visant à développer certaines activités économiques et à promouvoir le changement structurel* »[1], est donc indispensable. Et si certains l'accuseront de fausser le marché en favorisant certaines industries au détriment d'autres et de faire le lit du protectionnisme, le principe de réalité et une vision bien comprise de nos intérêts commanderont d'y voir le meilleur moyen de « *promouvoir des secteurs qui, pour des raisons d'indépendance nationale, d'autonomie technologique, de faille de l'initiative privée, de déclin d'activités traditionnelles ou d'équilibre territorial, méritent une intervention.* »[2]

Qui doit la formuler et la mettre en œuvre ?

Toute la question est ensuite de savoir à qui revient le rôle de formuler, porter et mettre en œuvre la politique industrielle. Le secteur de la cybersécurité recouvre en effet des enjeux et des réalités très diverses qui sont traités par plusieurs agences gouvernementales, lesquelles ont bien sûr leurs propres approches, contraintes et objectifs.

- **Le ministère de l'Économie**, traditionnellement chargé d'élaborer la politique industrielle du pays ;
- **Le ministère des Armées**, responsable, au travers du Commandement de la Cyberdéfense, de la défense « cyber », et le Pôle Technique de la Direction Générale de l'Armement (DGA)[3];
- **Le ministère de l'Intérieur**, chargé notamment de la lutte contre la cybercriminalité et qui a confié à la Délégation Ministérielle aux Industries de Sécurité et de lutte contre les Cybermenaces (DMISC) des responsabilités précises en matière de politique industrielle et de R&D technologique[4];
- **L'Agence nationale de la sécurité des systèmes d'information (ANSSI)**, qui est l'autorité nationale en matière de cybersécurité, mais dont le rôle en matière de politique industrielle reste pourtant à préciser ;
- **Le Comité de la Filière Industrielle de Sécurité (COFIS),** chargé du développement de la filière.

De fait, chacune de ces entités s'est dotée de responsabilités et d'objectifs propres. En l'absence de mécanisme institutionnalisé de coopération ou de dialogue, elles peuvent toutefois s'appuyer sur des textes fondateurs qui, s'ils ne formulent pas directement une stratégie structurée, en donnent de facto les grandes orientations.

- **Le Livre Blanc de 2010,** qui fait de la sécurité et la défense des systèmes d'information une priorité stratégique pour la France.
- **La Stratégie nationale pour la sécurité du numérique de 2015**[5] dans laquelle l'État s'engage pour la sécurité du numérique, conscient qu'elle contribue à la stabilité de l'État, au développement économique et à la protection des citoyens.
- **Le Plan Cybersécurité de l'ANSSI[6] de 2015**
- **La Revue Stratégique**[7] **de 2018**, conçue comme une synthèse de la doctrine française en matière de cybersécurité, et qui émet des recommandations d'actions à mettre en œuvre tant par l'État que les entreprises, en particulier par les opérateurs d'infrastructures vitales (OIV).
- **Les travaux du COFIS** sur ce sujet, et notamment ceux qui ont été présentés à Milipol 2017 qui fixent des objectifs relatifs à l'environnement des start-up, à la sécurité de la ville intelligente, à la cybersécurité et à la sécurité de l'internet des objets, à l'Europe et à la « marque France ».

Les grands objectifs

On peut ainsi tirer de ces documents les grands axes et objectifs de la politique industrielle de cybersécurité.

- **Garantir la souveraineté nationale et l'autonomie stratégique de la France en favorisant l'émergence d'une filière française de la cybersécurité**.

Le numérique et la cybersécurité sont aujourd'hui le moteur de la filière de sécurité française, à la fois en termes de croissance économique, de création d'emploi, d'exportations… S'appuyer sur ce dynamisme pour

développer une industrie de confiance solide et sécuriser du même coup nos grands systèmes stratégiques nous permettra non seulement d'assurer notre sécurité, mais constitue également un avantage concurrentiel pour les entreprises françaises. Une industrie solide capable de rayonner à l'international est également un moyen de faire entendre notre voix et de renforcer notre position sur la scène internationale, tant au niveau industriel que politique et stratégique.

- **Contribuer au développement d'une industrie européenne en décloisonnant les marchés nationaux.**

Le constat est simple : le marché français est étriqué et atomisé. Et il en va de même dans les autres pays européens : les marchés domestiques sont trop étroits et trop peu structurés. Face aux pays européens, ce sont donc les États-Unis, dont le tissu industriel est bien plus dense et le marché interne beaucoup plus vaste que le nôtre, qui concentrent tous les champions de la cybersécurité. Il paraît donc essentiel de mettre en pratique le fameux « marché unique du numérique » et de décloisonner les marchés européens de la cybersécurité. Il s'agit là d'une ambition politique, mais aussi d'une nécessité économique.

- **Investir dans des marchés d'avenir.**

Pour développer l'offre française, il faut miser sur quelques technologies et applications. En termes de briques technologiques il faut bien sûr commencer par celles sur lesquelles la France est déjà en position de force : algorithmie, cryptologie, intelligence vidéo… Mais il faut aussi apprivoiser celles qui seront critiques demain, et en tout premier lieu l'intelligence artificielle (IA). Autre domaine clé : les technologies de simulation et de virtualisation indispensables en matière de test de sécurité et d'entrainement (cyber range) mais aussi de déception (mise en place de réseau « leurre » permettant d'attirer les attaquants sur des « pots de miel » et de mieux comprendre leurs modes opératoires). En termes d'applications, les priorités comprennent notamment la sécurisation des données, la sécurisation du poste de travail, l'automatisation de la cyberdéfense, la résilience des architectures ou bien encore les outils d'investigation forensic

Quels sont les outils de la politique industrielle ?

Ces ambitions et ces nouveaux impératifs doivent se traduire concrètement par la mise en place de différents outils à l'échelle sectorielle. Ceux-ci doivent permettre de :

- **Capter et soutenir l'innovation**

C'est de l'innovation que nait l'avantage comparatif, tant au plan opérationnel et de performance qu'au plan économique et de concurrence commerciale. Il faut donc pouvoir identifier, le plus en amont que possible, les solutions, projets et expérimentations prometteurs. Or dans le secteur numérique et dans celui de la cybersécurité où les technologies sont la plupart du temps duales, l'innovation vient très souvent du secteur civil. C'est la raison pour laquelle le ministère des Armées s'est doté de divers dispositifs pour « capter » l'innovation. C'est le cas du DGA-Lab ou de l'Innovation Défense Lab, véritables showrooms de l'innovation où des start-ups et PME présentent et démontrent des solutions répondant à des besoins exprimés au préalable. D'autres projets en cours consistent également à cartographier les capacités et foyers d'innovation en matière de cybersécurité dans une démarche de veille et d'anticipation afin de détecter les technologies les plus stratégiques.

Des mécanismes de financement et d'accompagnement de l'innovation ainsi détectée permettent ensuite aux projets sélectionnés de se développer, de gagner en maturité, et *in fine* d'atteindre la phase de commercialisation. Ces dispositifs constituent à ce titre de véritables outils de politique technologique et de gestion de l'innovation. La DGA finance ainsi des projets et start-ups innovantes, dans le cadre du Régime d'Appui pour l'Innovation Duale (RAPID) et parfois des Plans d'Études Amonts (PEA). Des structures dédiées comme la Banque Publique d'Investissement (BPI), qui joue en la matière le rôle de fonds souverain, ou le Fonds pour l'Innovation et l'Industrie, créé en janvier dernier, peuvent aussi être sollicitées, tant pour le financement que l'accompagnement.

L'investissement public en matière d'innovation doit cependant être ciblé pour éviter tout saupoudrage des efforts. Compte tenu de l'urgence de la situation et de la faiblesse de nos moyens, nous n'avons ainsi ni le temps ni les moyens de développer plusieurs champions pour chacun des segments clés du marché de la cybersécurité comme l'exigent souvent la *doxa* en matière de politique industrielle. Autre point clé : à l'instar de la DARPA américaine, savoir arrêter des projets de R&D qui n'aboutissent pas ou ne rencontrent pas le marché suffisamment rapidement.

Les financements ne peuvent toutefois pas provenir uniquement de dispositifs publics. Si les fonds d'investissements commencent à s'intéresser à la cybersécurité, à l'instar d'ACE Management, d'Axeleo Capital, de Kima Ventures ou d'Idinvest, ils sont encore trop peu nombreux et les montants investis trop faibles.

- **Mobiliser la commande publique et privée**

Pour s'imposer durablement sur les marchés et devenir les champions de demain, les pépites d'aujourd'hui doivent en effet avoir les moyens financiers de s'émanciper des aides et subventions de l'Etat pour se frotter très rapidement au « marché » grâce à la commande publique et privée, qu'il s'agisse d'achat public avant commercialisation (APAC ou *pre-commercial procurement*). Il est ainsi essentiel que les administrations et les grandes entreprises montrent l'exemple en recourant aux solutions et services des start-up et PME françaises de cybersécurité, quitte à utiliser les services de grands intégrateurs pour se « réassurer » et bénéficier d'une couverture fonctionnelle plus large.

A plus large échelle, les outils de soutien à l'export permettent également aux entreprises d'élargir leurs perspectives de marchés. On peut regretter à ce titre que les labels délivrés par l'ANSSI (certifications et qualifications) ne fassent pas encore l'objet d'une harmonisation, a minima à l'échelle régionale et européenne.

- **Structurer une filière de confiance**

Pour être compétitive et pouvoir rivaliser avec ses concurrents étrangers, la filière de cybersécurité doit se développer de façon structurée, en prenant en compte à la fois les besoins et contraintes du marché, les compétences disponibles et les insuffisances. En l'absence de politique publique dédiée, un dialogue État-entreprise comme celui porté par le COFIS permet justement de recenser les acteurs, cartographier les compétences et les lacunes, et *in fine* de proposer une vision prospective du développement de la filière.

Sur un plan plus opérationnel, l'émergence de groupements industriels et clusters comme Hexatrust ou de pôles d'excellence comme le Pôle d'Excellence Cyber, contribuent aussi à structurer et renforcer la filière, notamment parce qu'ils permettent de décloisonner les approches et de favoriser les coopérations. En rassemblant les acteurs industriels, institutionnels et académiques autour d'un projet de création d'une chaîne

de valeur confiance, ils permettent ainsi des mutualisations et émulations qui ne peuvent que bénéficier à leurs membres à titre individuel et à la filière à titre collectif.

- **Construire une industrie et un marché européen**

Le décloisonnement des marchés européens suppose la mise en place de mécanismes de coopérations formels et réguliers à tous les échelons de la chaîne de valeur et entre tous les acteurs : marchés et industries (entreprises), administrations publiques (agences nationales et gouvernementales, ministères concernés…) monde académique (universités, centres de recherche…). Il passera notamment par :

L'harmonisation des politiques nationales de qualification et certification nationales grâce à une démarche de standardisation « par le haut » sur la base des critères proposés par les pays présentant les niveaux d'exigence les plus élevés ;

Une coopération approfondie entre les agences nationales, dans la lignée de ce qui existe déjà entre la CNIL et ses homologues réunies au sein du G29, ou au niveau bilatéral entre l'ANSSI et le BSI allemand ;

Le renforcement des liens entre les grands salons professionnels, à l'instar du Forum International de la Cybersécurité (FIC) et du grand salon allemand ITSA qui ont formalisé leur coopération en juin 2018 ;

Au niveau de l'Union européenne : la multiplication des initiatives de promotion de l'innovation comme le European Public Private Partnership on Cybersecurity lancé par l'ECSO (European Cybersecurity Organisation) en 2016, et la poursuite des programmes de recherche type Horizon 2010. A ce titre, les réflexions de la Joint European Disruptive Initiative (JEDI) sur la création d'une agence européenne d'innovation sur le modèle de la DARPA américaine peuvent s'avérer déterminantes.

[1] http://www.cae-eco.fr/IMG/pdf/26.pdf

[2] Idem

[3] https://www.defense.gouv.fr/dga/la-dga2/missions/presentation-de-la-direction-generale-de-l-armement

[4] https://www.interieur.gouv.fr/Le-ministere/Organisation/Delegue-ministeriel-aux-industries-de-securite-et-a-la-lutte-contre-les-cybermenaces

[5] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

[6] https://www.ssi.gouv.fr/uploads/2015/01/Plan_cybersecurite_FR.pdf

[7] https://www.numerique.gouv.fr/files/files/revue_strategique_de_cyberdefense.pdf

2. L'UTILISATION DU SMARTPHONE EN MILIEU MILITAIRE

Le contexte

Selon le baromètre annuel du numérique publié en 2017 par l'ARCEP en collaboration avec l'Agence du Numérique, près de 73% des Français, âgés de 12 ans ou plus, sont équipés d'un smartphone[1]. La multiplication des fonctionnalités et des applications ont permis au smartphone de devenir notre « boîte à outils » du quotidien.

Omniprésent dans la société civile, le smartphone et son évolution intéresse de plus en plus les armées. Cette volonté d'intégration des technologies civiles au militaire est d'ailleurs au cœur de la récente Revue Stratégique de Défense et de Sécurité nationale, qui souhaite « *mieux préparer les prochaines générations de systèmes et d'équipements* »[2]. Pourtant, l'idée d'utiliser des smartphones en milieu militaire n'est pas nouvelle. Certaines forces armées étrangères ont ainsi développé plusieurs projets. Par exemple, en 2017, Motorola annonçait le lancement de sa première ligne de smartphones à usage strictement militaire[3], en collaboration avec le ministère de la Défense israélien. Ces téléphones portables peuvent supporter les réseaux 4G civils comme les réseaux militaires et permettre l'envoi de fichiers audio ou vidéo de manière sécurisée grâce au chiffrement.

En France, la société Atos a donné la première impulsion avec la solution Auxylium, co-développée avec la Direction Générale de l'Armement, intégrée dans un smartphone fonctionnant avec Android. Cette solution permet d'abord une communication chiffrée applicable aussi bien sur les réseaux de téléphonie mobile civils que militaires, permettant ainsi d'éviter les risques de saturation. Elle propose également une fonction de géolocalisation des différentes unités sur une cartographie. Elle a d'abord été déployée dans le cadre de l'opération Sentinelle mais a vocation à se développer plus amplement au sein des armées[4].

Avant la création de smartphones dédiés à l'usage militaire, plusieurs sociétés du secteur civil ont développé des applications mobiles. De nombreuses applications destinées aux personnels militaires sont déjà disponibles aux États-Unis, tant sous Android qu'IOS. Il s'agit plus particulièrement d'application GPS (*Tactical NAV*[5]), d'aide aux premiers secours (*Army First* Aid[6]) ou encore d'applications permettant au service support des armées de calculer les modalités logistiques pour acheminer, à une localisation donnée, une quantité précise de ressources alimentaires via l'application (*CCALC-I* par Northrop Grumman[7]).

Intégrer le smartphone sur le champ de bataille semble présenter de nombreux intérêts :

- La fonction « boite à outils » du smartphone permet de disposer de plusieurs fonctionnalités réunies sur un seul support;
- Les capteurs intégrés ainsi comme la photo et la vidéo font du smartphone un outil de renseignement efficace ;
- La rapidité et la simplicité d'utilisation.

Mais subsistent encore quelques zones d'ombre : qu'en est-il de la question de la connectivité en milieu dégradé ? Comment cloisonner l'usage professionnel de l'usage personnel du smartphone?

Les défis technologiques

Si l'utilisation du smartphone en milieu hostile constitue une opportunité réelle pour les armées en termes de baisse des coûts et de gain en agilité, son usage non-maîtrisé accroit cependant leur surface de risques. Les vulnérabilités liées aux réseaux de communication, aux systèmes hardwares employés et aux applications utilisées constituent les principales menaces pouvant mettre en péril la sécurité et la confidentialité des opérations.

Risques réseaux : la mise en place d'un réseau de défense de type LTE représente un avantage significatif pour les armées, car il permet le déploiement rapide de moyens de communication sur un théâtre d'opération tout en répondant aux impératifs de sécurité associés. Cependant, il est également susceptible de créer des vulnérabilités de taille : sensibilité particulière au brouillage, absence de protection contre la menace IEM (impulsion électromagnétique pouvant détruire des appareils électroniques et brouiller les télécommunications) et instabilité du réseau lui-même. Par ailleurs, l'utilisation de la 4G par les personnels militaires les rend également vulnérables au piratage des smartphones. En 2017, 4000 soldats de l'OTAN ont ainsi été victime d'une attaque massive russe qui, à l'aide de drones spécialisés et d'antennes portables, ont pu accéder aux appareils mobiles personnels des militaires.[8] Ce type d'opération peut révéler des informations sensibles telles que la localisation et le nombre de soldats en opération mais peut aussi être la porte ouverte à la compromission d'un réseau dans son ensemble.

Risques hardwares : En dévoilant fin 2017 son application mobile capable de transformer un smartphone Android en outil anti-surveillance, Edward Snowden a mis en évidence certaines vulnérabilités inhérentes aux smartphones. L'outil se sert en effet de tous les capteurs présents dans le smartphone, du micro à la caméra, pour identifier une potentielle menace à la vie privée, en ligne comme dans la vie physique. Ces capteurs enregistrent et transmettent donc les données personnelles de son utilisateur, et deviennent ainsi une porte d'entrée pour de potentiels hackers car ils restent facilement manipulables par des applications et aisément contrôlable à distance.[9] En ce sens, le gouvernement américain a récemment interdit l'usage des smartphones Huawei et ZTE sur les bases militaires américaines.[10]

Risques applications : Les applications représentent également une menace grandissante. En effet, les sociétés développent des applications à un rythme effréné pour répondre aux besoins commerciaux, faisant parfois abstraction des mesures de sécurité. Parmi les organisations qui développent des applications mobiles, 83% externalisent le développement et 79% intègrent des librairies tierces. Lorsque les développements externalisés ne sont pas soumis à des tests, il arrive régulièrement que les applications concernées présentent des comportements non désirés, et divulguent des données sans que le distributeur n'en soit même conscient. Les armées en ont déjà payé le prix. L'armée française a mis en garde ses soldats face à l'utilisation de l'application de fitness Strava, dont l'option de géolocalisation pouvait révéler l'emplacement d'infrastructures militaires secrètes.[11] L'armée israélienne a également été visée par une cyberattaque du Hamas utilisant des applications liées au Mondial 2018 pour pénétrer les smartphones des militaires israéliens.[12]

Quelles mesures de prévention adopter ?

Face à ce constat et les risques pesant sur l'utilisation des smartphones en milieu militaire, plusieurs mesures peuvent être prises en amont, afin de protéger au mieux ces données sensibles.

- **Sensibiliser le personnel**

Les détenteurs de smartphones sont les premiers concernés par l'utilisation qui en est faite, et par conséquent, de la sécurité des données qu'ils contiennent. A l'instar de l'armée américaine[13], l'une des premières mesures de prévention consiste à sensibiliser les personnels par l'édiction de règles de sécurité afin de cloisonner l'utilisation personnelle de l'utilisation professionnelle du smartphone. A ce titre, l'ANSSI a publié en juillet 2015 une notice technique contenant des recommandations de sécurité sur l'utilisation des smartphones[14], et notamment sur la cohabitation entre usage privé et usage professionnel : interdire l'installation automatique d'applications, désactiver l'association automatique aux points d'accès Wi-Fi, utiliser des smartphones dédiés à l'usage professionnel…

- **Renforcer la sécurité des systèmes d'exploitation et la création de solutions spécifiques**

Aujourd'hui, la question se pose essentiellement pour les deux leaders du marché européen : Android et iOS. En France, Android représente 80% de part de marchés devant iOS avec 19.5%. La diversité des menaces actuelles oblige à prendre en compte le niveau de sécurité par défaut de ces OS, mais aussi leur capacité de résilience. Après s'être arrêté sur le choix du Samsung Galaxy Note 4, le ministère de la Défense britannique a finalement annoncé l'utilisation d'iPhone 7s spécialement adaptés au secteur militaire, le Samsung Galaxy Note présentant trop de failles techniques susceptibles d'être exploitées. iOS serait donc plus sécurisé, mais ce constat reste à mettre en perspective car plus un smartphone est utilisé, plus il intéresse les cyber-attaquants et intensifie leur recherche dans l'exploitation de failles.

Au-delà d'une sécurisation des OS, la création d'applications dédiées permet également de garantir un niveau supplémentaire de protection des données contenues dans le smartphone. Afin de pouvoir traiter des informations sensibles à distance, une solution ultra sécurisée a été conçue par Thalès, l'application CITADEL. Elle contient une messagerie et une plateforme d'appel et de partage de documents, chiffrées de bout en bout. De plus, les données recueillies sont uniquement stockées en France. L'application, disponible sur Android et iOS, est aujourd'hui utilisée au plus haut niveau de l'Etat français et dans 50 pays membres de l'OTAN.

- **Développer des terminaux spécifiques**

C'est notamment la position adoptée par la Russie. Précédemment, la solution utilisée par l'armée russe consistait en l'emploi de deux cartes SIM distinctes : l'une servant à connecter l'utilisateur au réseau classique, et la seconde permettant de chiffrer les informations sur les lignes de communications. Cependant, le support et les composants fabriqués à l'étranger pouvaient poser de véritables problèmes de sécurité pour les informations contenues. Le ministère de la défense a alors développé son propre portable à usage exclusivement militaire : l'Atlas M-663S, strictement conçu en Russie, composé de sa propre méthode de chiffrement, OS et logiciels. Cependant une fabrication entièrement souveraine reste relativement complexe à mettre en place. Vérifier et tester les composants fabriqués à l'étranger permet déjà de prévenir le risque de cyberattaques.

Les besoins en sécurité ne cessent d'augmenter au rythme des évolutions technologiques. De plus, la tendance grandissante à l'hyperconnectivité rendrait difficile la maîtrise d'un réseau ultra sécurisé par les opérateurs civils. L'une des solutions serait d'envisager la création d'un réseau LTE de sécurité de niveau européen. Il permettrait d'avoir un réseau commun sécurisé mais aussi de rallier les États membres à un projet fédérateur, dans la continuité d'une Europe de la Défense.

[1] https://www.arcep.fr/uploads/tx_gspublication/barometre_du_numerique-2017-271117.pdf, page8

[2] Revue stratégique de défense et de sécurité nationale (2017), page 71, paragraphe 232

[3]https://www.israelvalley.com/2018/07/cisrael-smartphone-militaire-youtube-de-tsahal

[4]https://www.defense.gouv.fr/terre/actu-terre/auxylium-battlefield-jusqu-au-combattant-debarque

[5] http://soldiersystems.net/tag/tactical-nav/

[6] http://doubledogstudios.com/apps/armyfirstaid/

[7] http://www.globenewswire.com/newsarchive/noc/press/pages/news_releases.html?d=10006268

[8] https://siecledigital.fr/2017/10/05/russie-pirate-smartphones-soldats-otan/

[9] http://www.lefigaro.fr/secteur/high-tech/2018/01/03/32001-20180103ARTFIG00119-haven-l-appli-de-snowden-pour-transformer-son-smartphone-en-outil-de-surveillance.php

[10] https://www.zdnet.fr/actualites/les-smartphones-huawei-et-zte-bannis-des-bases-militaires-us-39867816.htm

[11] https://www.numerama.com/politique/325474-strava-ce-que-preconise-larmee-francaise-sur-la-geolocalisation.html

[12] http://www.lalibre.be/economie/digital/des-logiciels-espions-dans-les-smartphones-de-l-armee-israelienne-5b3df09e5532692547e790f6

[13] http://archive.defense.gov/news/newsarticle.aspx?id=14689

[14] https://www.ssi.gouv.fr/uploads/2013/05/NP_Ordiphones_NoteTech_v1.2.pdf

FOCUS INNOVATION

ENTRETIEN AVEC CHARLES THOORIS, CHIEF SALES OFFICER, DIRECTOR SECURE-IC

Secure-IC, spin-off de l'université Télécom ParisTech co-fondée en 2010 par Hassan Triqui et Philippe Nguyen, est spécialisée dans la sécurité des systèmes électroniques embarqués (téléphones portables, passeports électroniques, cartes bancaires, électronique automobile…). Ses produits sont aujourd'hui plébiscités par des fabricants de composants et de téléphones mobiles, des concepteurs de carte à puce, ou encore des agences de sécurité étatiques.

Le modèle

Le succès de Secure IC repose sur trois axes de développement :

- **La R&D**

Née d'un essaimage de la recherche publique, et plus précisément des travaux de recherches menés à l'Institut Mines-Telecom (alors Télécom ParisTech), Secure-IC reste très attachée à sa forte culture scientifique et continue à investir massivement dans la recherche et le développement. A côté de son équipe composée en grande majorité d'ingénieurs (presque 99%), elle poursuit également une activité de recherche académique avec les 4 à 5 doctorants qu'elle héberge chaque année. Elle entretient également ses liens avec l'Institut Mines-Telecom, dont 3 chercheurs jouent le rôle de conseillers scientifiques de la société. Secure-IC a aussi rédigé plus de 200 publications avec ses partenaires académiques.

- **L'innovation**

Cet investissement continu et significatif en R&D sous-tend la stratégie d'innovation permanente de la société. Pour Secure-IC, c'est le caractère innovant d'un produit qui fait sa force. Convaincue qu'exploiter l'innovation pour réinvestir dans la R&D permet de concevoir de nouveaux produits, Secure IC a déposé 120 brevets dans près de 30 familles et 15 marques et a conclu un partenariat stratégique avec France Brevet qui lui permet de profiter d'un accompagnement dédié.

- ***International by design.***

L'internationalisation est au cœur du développement de la PME bretonne. Installée en Asie depuis sa création en 2010, Secure-IC réalise aujourd'hui 75 % de son chiffre d'affaires à l'étranger. Si elle emploie une quarantaine de personnes à son siège à Rennes, elle détient également des bureaux et des équipes à Paris, Singapour et Tokyo.

Des technologies innovantes

La société dispose de deux unités opérationnelles : l'une fournit des sous-systèmes électroniques qui protègent les puces sur lesquelles ils sont intégrés ; l'autre est dédiée à l'étude des attaques et à la conception de solutions de détection et d'analyse des vulnérabilités.

Parmi les produits et solutions conçus par ces équipes, deux en particulier présentent un caractère particulièrement innovant.

- Cyber Escort Unit

Cette solution permet de faire le lien entre la sécurité du logiciel et celle du matériel (la sécurité embarquée). Elle permet ainsi de détecter en temps réel des attaques "zero day" dans le code. Cette solution unique sur le marché constitue le fondement de cybersécurité assisté par le matériel.

- Smart Monitor

Ce superviseur sur puce assisté par l'intelligence artificielle apporte une dimension d'intelligence collective et de cohérence entre les IP, tant analogiques que numériques, et les autres lanceurs d'alertes et signaux faibles, tant logiciels que matériels. Il assure la détection, l'analyse et le diagnostic des incidents de sécurité, et fluidifie ainsi la prise de décision. Cette solution permet ainsi de prendre l'avantage sur les attaquants et enrichit les process d'intelligence économique en offrant la possibilité de pouvoir remonter des informations sur le cycle de vie du système.

ACTUALITE

Publication du rapport d'information sur la cyberdéfense

L'Assemblée Nationale a publié le 9 juillet 2018, en conclusion des travaux de la mission d'information sur la cyberdéfense, son rapport d'information sur la cyberdéfense présenté par M. Bastien LACHAUD, député de la 6ème circonscription de Seine-Saint-Denis, et MME Alexandra VALETTA-ARDISSON, députée de la 4ème circonscription des Alpes Maritimes.

Dans la lignée de la Revue stratégique de cyberdéfense publiée par le Secrétariat général de la défense et de la sécurité nationale le 12 février 2018, ce rapport pose quelques pistes de réflexions et recommandations en matière de défense cyber. Il préconise notamment de :

- Élaborer d'une loi « cyber » ;
- Recouvrer la souveraineté numérique de la France, sur le plan national et européen ;
- Renforcer la résilience des acteurs nationaux (autorités publiques, acteurs économiques, collectivités territoriales, citoyens…) ;
- Consolider une base industrielle et technologique de défense cyber ;
- Ajuster la « ressource humaine cyber » via la sensibilisation, la formation, notamment au sein des structures dédiées du ministère des Armées ;
- Assurer les conditions de la cybersécurité collective en développant les régulations internationales, les standards et les certifications, et les dispositifs de coopération internationale.

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.

https://www.hexatrust.com/ueht2018/

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