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

Table des matières

ANALYSES

1. LE FINANCEMENT DE L'INNOVATION EN CYBERSECURITE : LE DEFI DE LA SOUVERAINETE

Les technologies de cybersécurité ont un caractère spécifique. Leur développement requiert donc la mise en place de mécanismes de soutien à l'innovation et de financement adaptés. Plusieurs raisons à cela : la nature profondément duale de ces technologies, la dimension stratégique du domaine « cyber », les cycles de R&D relativement longs qu'elles exigent du fait des briques technologiques issues de la « deep tech » (telles l'intelligence artificielle) sous-jacentes… Parce que l'innovation technologique en cybersécurité ne saurait obéir à une logique exclusivement « top down » et être l'apanage des grands groupes et de la R&D gouvernementale, il s'agit donc de prendre en compte ces contraintes pour concilier des logiques contraires : « temps court » du marché et « temps long » de la R&D, exigences de souveraineté et perspectives de sortie pour les investisseurs, extrême rapidité du progrès technologique, évolutivité des menaces et besoin de sécurité « by design ».

1.1. ÉTAT DES LIEUX

- **Cybersécurité et deep tech**

La deep tech, qui constitue le socle technologique de nombreuses solutions de cybersécurité, jouit aujourd'hui d'une véritable popularité qui lui a permis de bénéficier de levées de fonds relativement conséquentes. Depuis 2017, la deep tech se place en effet au premier rang des investissements en Europe, avec, depuis 2015, des investissements en capital-risque augmentant 3 fois plus vite dans ce secteur que dans les start-up technologiques B2C[1]

Mais malgré l'engouement que suscite la deep tech, le financement de l'innovation en cybersécurité reste pourtant limité, d'une part par sa complexité technique qui peut décourager certains investisseurs, d'autre part par un taux de retour sur investissement inférieur à d'autres domaines technologiques. Ainsi, si la prise de conscience du risque « cyber », le développement des réglementations sur la protection des données ou des infrastructures stratégiques (RGPD, NIS, LPM…) et les nouvelles exigences en matière de souveraineté ont permis une relative accélération de l'investissement en cybersécurité depuis 2017, le niveau reste encore largement insuffisant pour répondre aux besoins des start-up qui sont 87% en France à vouloir lever des fonds[2].

- **Des technologies duales**

Force est de constater que l'innovation en cybersécurité est encore aujourd'hui en grande partie issue du secteur civil. A côté des fonds d'investissements publics, et pour bénéficier des avancées technologiques tirées par le marché civil, les opérateurs publics ont donc développé des mécanismes de financement reposant sur l'intégration des dimensions civiles et militaires. C'est par exemple le cas de la DARPA aux États-Unis, et en France, des dispositifs de financement RAPID (Régime d'Appui Pour l'Innovation Duale) et Astrid (Accompagnement Spécifique de Travaux de Recherche et d'Innovation Défense) qui ont vocation à améliorer la captation de technologies, complétés dès 2013 par « Astrid maturation » qui permet d'accompagner ces technologies un peu plus loin. Tous deux ont fait de la dimension duale des solutions candidates une condition *sine qua non* de l'octroi de financements, dans le but de permettre à la défense de se doter des technologies et solutions correspondant à ses besoins spécifiques, tout en évitant de priver les sociétés accompagnées de débouchés sur les marchés civils. Parmi les projets et sociétés de cybersécurité accompagnés par ces mécanismes, on peut par exemple citer Tetrane (détection des vulnérabilités et anticipation des attaques) ou Smartesting.

Considérant qu'elle devait permettre d'« innover plus vite »[3], cette nouvelle vision de l'innovation duale, poussée le ministère des Armées, s'est ainsi développée dans le sillage de la Loi de programmation militaire 2019-2025.

L'enjeu des solutions souveraines

A l'instar de certains secteurs spécifiques, la cybersécurité est au centre d'enjeux de souveraineté nationale et d'autonomie stratégique (localisation et hébergement des données, sécurité des OIV et des infrastructures critiques…). L'intérêt porté par la défense pour le chiffrement, la détection ou encore l'analyse prédictive en témoignent. Pour autant, toutes les solutions de cybersécurité ne sont pas destinées à devenir des outils souverains. Pour certains investisseurs comme pour les sociétés concernées, cette finalité peut même être perçue comme un obstacle qui limite la taille du marché accessible et peut compliquer leurs perspectives de sortie. D'où la nécessaire entrée en scène, aux côtés des investisseurs traditionnels du secteur, d'acteurs capables de mettre en place des mécanismes de financement adaptés aux exigences du marché de la défense.

1.2. QUELS OUTILS ?

En France

La question de la souveraineté n'est pas spécifique à la cybersécurité, comme en témoigne l'intervention de Laurent Collet-Billon, alors Délégué général pour l'armement, lorsqu'il déclarait en 2016 : *« De plus en plus de sociétés d'autres continents tentent de s'emparer de certaines de nos PME 'pépites' et nous n'avons pas d'outil pour les défendre »*[4]. Un an plus tard, la création de Definvest, fonds de capital-risque doté de 50 millions d'euros à destination des PME géré par Bpifrance pour le compte du ministère des Armées, devait

permettre de protéger ces entreprises jugées stratégiques pour l'Hexagone. Le mécanisme RAPID subventionne les innovations duales dans les premiers stades de leur développement, et les mécanismes Astrid et Astrid maturation ont vocation à les aider à traverser la « vallée de la mort » si cruciale à leur croissance. Definvest intervient de son côté en tant que co-investisseur pour accompagner le développement général ou la transmission de PME et start-up stratégiques. La DGA y apporte sa connaissance sectorielle et Bpifrance son expertise financière et sa connaissance de l'écosystème industriel.

A l'international

La France est loin d'être un cas isolé. Outre-Atlantique, les États-Unis ont depuis 1999 développé des mécanismes de financement allant dans ce sens. La société In-Q-Tel, qui permet à la CIA d'intervenir dans le financement de l'innovation, illustre cette tendance. Plus récemment, Israël s'est également saisi de la question avec le lancement de Libertad Ventures et du programme Xcelerator.

Nom	Pays	Création	Entité	Opérateur public	Secteur(s)	Sociétés soutenues
In-Q-Tel	États-Unis	1999	Société à but non lucratif	Appartient à la Central Intelligence Agency (CIA)	Entreprises jugées stratégiques pour le renseignement	In-Q-Tel est notamment connue pour ses investissements dans Google Earth, Palantir (Big data) ou Recorded Future (Machine learning), financé conjointement avec Google[1]
Definvest	France	nov-17	Fonds d'investissement	Géré par Bpifrance pour le compte du ministère des Armées	PME stratégiques pour la défense, en particulier celles ayant développé des innovations de « rupture » ou celles qui sont critiques dans la supply chain des programmes d'armement	A ce jour, le fonds est entré au capital de quatre entreprises : **Kalray** (spécialisé dans les processeurs dédiés aux nouveaux systèmes intelligents) **Fichou** (composants optiques de très haute précision) **SINTERmat** (métallurgie des poudres) **Unseenlabs** (surveillance maritime par nanosatellite)
Libertad Ventures	Israël	2017	Fonds d'innovation technologique	Appartient au Mossad	Robotique, énergie, chiffrement, web intelligence, traitement du langage naturel et analyse sémantique	Libertad Ventures ne communique pas son portefeuille mais chaque projet peut être soutenu jusqu'à 2 000 000 de Nouveau Shekel Israélien (NIS), soit 470 000 € environ
Xcelerator	Israël	2018	Programme d'accélération	Lancé par le Shabak, équivalent de la DGSI israélienne, avec TAU Ventures, fonds de capital-risque de l'Université de Tel Aviv	Start-up développant des technologies utilisant l'IA (parmi les start-up sélectionnées, toutes ne sont pas des solutions souveraines)	7 start-up sélectionnées pour le premier programme[2] : **CannyAI** (vidéos) **AutoPlay AI** (bots pour tests automatisés de produits logiciels) **XTend** (connexion entre l'œil humain et les drones) **Cloner** (réalités augmentée et virtuelle) **Talamoos** (prédiction et apprentissage automatique du comportement) **Cyabra Strategy Ltd.** (lutte contre les fake news) **Legal Automation** (analyse automatique de documents) A noter qu'elles perçoivent notamment une subvention de 50 000 $ du Shabak

Point commun à ces différentes initiatives : elles reposent sur l'interaction des gouvernements, de la communauté du capital-développement et de l'écosystème des start-ups, et entendent jouer un rôle majeur dans ce nouveau modèle de financement de l'investissement collaboratif. Par ailleurs, elles couvrent les secteurs considérés comme « stratégiques » dont la cybersécurité fait partie.

Chaque État a toutefois développé des outils de financement différents, à la mesure des caractéristiques de son marché, de ses objectifs et capacités d'investissement. La France se distingue par exemple par le fait que le développement à l'international n'est pas toujours envisagé par une start-up dans les premières phases de son existence. Et ce d'autant plus que nombre de fonds d'investissements nationaux n'ont pas la portée internationale suffisante pour les y accompagner. D'autre part, l'absence de grands éditeurs susceptibles de tirer vers le haut les start-up et de consolider progressivement le secteur, contribue à affecter le dynamisme de l'écosystème numérique français. L'approche israélienne, au contraire,

est tournée avant tout vers le marché mondial en raison d'un marché domestique trop restreint pour se suffire à lui-même. Et cela à la différence de l'approche américaine, qui repose sur un marché intérieur particulièrement vaste et des fonds d'investissement nationaux solides et dynamiques.

1.3. QUELS OBJECTIFS DE SOUVERAINETÉ POUR LES ÉTATS ?

- **Assurer son « autonomie stratégique »**

Pour assurer son « autonomie stratégique », l'État doit se doter des moyens d'assurer le développement de sa base industrielle et technologique de défense (BITD), en particulier en matière de cybersécurité. En France, si l'implication d'un opérateur public dans le financement de l'innovation n'est pas nouvelle, l'approche adoptée par Definvest se distingue en ce qu'elle combine accompagnement de l'innovation et défense de la souveraineté, et se traduit par l'entrée du fonds au capital de PME stratégiques pour la défense. In-Q-Tel fait de même aux États-Unis, en prenant des participations dans des entreprises jugées stratégiques pour le renseignement de son côté.

- **Protéger son écosystème national**

Aux côtés des autres mécanismes déjà existants, les nouveaux modes de financement concourent au développement, voire à la création, d'un écosystème de cybersécurité national. Les États entendent ainsi garder la main sur l'innovation conçue en leur sein, et consolider une véritable relation à double sens entre les pépites technologiques et les opérateurs publics : les premières y perçoivent des cas d'usage leur permettant d'améliorer et d'éprouver leurs solutions ainsi qu'une nouvelle source de financement indispensable à leur développement, les seconds y trouvent des technologies souveraines répondant à leurs besoins. Par exemple en Israël, s'il n'y a pas de prise de participation dans les entreprises financées par les opérateurs publics, le Mossad (Libertad Ventures) peut en revanche exploiter la propriété intellectuelle de la technologie financée, via une licence non commerciale et non exclusive[7].

- **Anticiper les enjeux futurs**

A mesure que les dispositifs de financement et d'accompagnement se multiplient, les États affirment ainsi leur volonté de porter l'innovation au-delà de la simple identification des entreprises ou projets innovants. En France, la politique industrielle de cybersécurité a notamment pour objectif d'investir dans des marchés d'avenir et de miser sur des briques technologiques à fort potentiel. Si l'algorithmie ou la cryptologie représentent l'excellence française en matière de cybersécurité, la France doit aussi prouver qu'elle est capable d'investir dans les technologies stratégiques de demain, au premier rang desquelles l'intelligence artificielle[8]. Sur les 250 millions d'euros par an investis par le Fonds pour l'innovation et l'industrie (FII), créé sous le modèle de la DARPA américaine[9] au profit des innovations de rupture, 150 millions d'euros serviront ainsi à financer les grands défis technologiques et sociétaux – dont les 2 premiers concernent l'IA – et 70 millions seront dédiés à l'accompagnement de sociétés de la deep tech française. Parallèlement, la « stratégie nationale de recherche en intelligence artificielle » dévoilée par le

gouvernement le 28 novembre devrait permettre d'affirmer le rôle moteur de l'Hexagone à l'échelle mondiale dans le domaine de l'intelligence artificielle, notamment grâce à la création d'une vingtaine de chaires liées à l'IA dès 2019, qui viendront s'ajouter aux 20 déjà existantes afin d'attirer les meilleurs talents étrangers tout en évitant la fuite des cerveaux nationaux[10].

[1] https://www.wavestone.com/fr/insight/deep-tech-global-investor-survey-2017/
[2] L'Observatoire FIC des start-up cyber
[3] https://www.usinenouvelle.com/editorial/le-ministere-des-armees-cree-une-agence-dediee-a-l-innovation.N667849
[4] http://www.opex360.com/2017/11/17/definvest-le-fonds-dinvestissement-de-la-defense-pour-les-entreprises-strategiques/
[5] https://www.wired.com/2010/07/exclusive-google-cia/
[6] https://www.israelvalley.com/2018/07/tel-aviv-baptise-the-xceleratorle-contre-espionnage-lance-incubateur/
[7] http://www.libertad.gov.il/eng/
[8] Le programme Man Machine Teaming, visant à intégrer l'IA dans l'avion de combat du futur, en est le parfait exemple
[9] « *A la différence que les innovations soutenues ne seront pas uniquement militaires* » (Bruno Le Maire)
[10] https://www.numerama.com/sciences/443615-voici-les-6-axes-de-la-strategie-de-recherche-en-intelligence-artificielle-pour-la-france.html

2. COMMUNICATIONS SENSIBLES : COMMENT REPONDRE AUX EXIGENCES DE SECURITE ET DE SOUVERAINETE ?

La donnée, « or noir » de l'âge numérique, est une source de richesse considérable. Sa protection et sa sécurité sont devenues un enjeu majeur pour les entreprises et les administrations qui stockent et échangent, à la fois en interne et avec leurs partenaires, des données parfois sensibles. Insuffisamment sécurisés, les communications et les échanges d'informations sont en effet autant de vecteurs privilégiés de fuites de données potentiellement stratégiques.

Dans ce cadre, la sécurité des canaux de communication, pourtant primordiale, est de fait devenue le point faible de bien des sociétés et des Etats. Les organisations qui s'appuyaient traditionnellement sur des échanges par e-mail pour leur communications, internes et externes, se tournent également de plus en plus vers les messageries instantanées, qu'il s'agisse de solutions grand-public peu sécurisées telles que WhatsApp ou Telegram, ou de solutions spécialisées non chiffrées comme Slack, à la fois pour leurs échanges internes avec leurs collaborateurs et pour leurs communications à l'extérieur avec leurs sous-traitants, clients ou partenaires.

Or ces services grands publics ne correspondent cependant pas toujours aux besoins réels des entreprises et à leurs exigences de sécurité, de confidentialité et de souveraineté. Certaines solutions se sont donc positionnées sur ce créneau, tout l'enjeu étant de trouver le bon équilibre entre sécurité et facilité d'usage et de leur permettre de se faire une place dans un marché où les effets de réseaux jouent à plein (principe du « winner takes all »).

2.1. Solutions grand public : quels sont les risques ?

L'usage de messageries électroniques grand public, pour la plupart initialement non chiffrées, dans le cadre de communications professionnelles, comporte des risques considérables et potentiellement dévastateurs pour une entreprise, surtout quand il s'agit de sujets sensibles ou confidentiels (stratégie d'une organisation, réponse à un appel d'offres, stratégie d'acquisition…). Parce qu'ils transitent en clair sur le réseau, les messages sont lisibles par le prestataire et peuvent facilement être interceptés, altérés ou simplement analysés, non seulement par le prestataire lui-même mais également par des tiers, potentiellement malveillants. Google permet ainsi toujours à ses partenaires commerciaux de scanner les messageries Gmail et de partager les données collectées[1].

Le problème se pose dans les mêmes termes pour les messageries instantanées dont l'usage s'est d'abord développé de façon exponentielle dans le domaine privé, suscitant parmi les utilisateurs des craintes quant à la protection de leurs données personnelles. C'est dans ce contexte que sont nées, puis se sont développées des solutions comme Whatsapp ou Telegram, intégrant des fonctionnalités de chiffrement « de bout en bout » pour protéger le secret des correspondances.

Ces solutions, mieux sécurisées et désormais régulièrement utilisées dans le cadre professionnel, comportent pourtant un certain nombre de risques. Facebook, qui exploite WhatsApp, accède ainsi aux métadonnées de l'application et utilise les informations de comptes des utilisateurs, y compris les numéros de téléphone. Quant à Telegram, l'application a été sommée à plusieurs reprises de fournir ses clés de chiffrement au

gouvernement russe dans le cadre de la lutte contre le terrorisme, sous peine d'amende ou de blocage, et si elle s'y est jusque-là refusée, elle n'est pas à l'abri d'autres tentatives de manipulation.[2]

2.2. Quelles alternatives sécurisées ?

De manière générale, le succès et la pérennité d'un service de messagerie dépendent :

- De son architecture technique, qui conditionne son niveau de sécurité et de souveraineté : ses choix techniques (modalités et algorithmes de chiffrement notamment…), la localisation des serveurs et du stockage des clés de chiffrement, la maîtrise et l'audit du code source...
- Du business model de l'application, fruit d'un arbitrage entre la réponse à des besoins génériques et l'adaptation à des besoins particuliers, qui lui permettra de développer son marché.

C'est en partant de ce double constat du niveau insuffisant de sécurité des messageries existantes, et de la nécessité de fédérer une communauté d'utilisateurs autour d'une solution de messagerie, que la startup londonienne New Vector a développé un nouveau serveur de communication pour messageries instantanée baptisé Matrix[3]. Ce protocole de communication qui tire les enseignements des avancées techniques de la messagerie Signal en matière de chiffrement de bout en bout[4], notamment en s'appuyant sur son « Double Ratchet Algorithm », a pour ambition de devenir le nouveau standard dans le domaine. Plusieurs applications récentes s'appuient ainsi sur Matrix comme Citadel Team[5] de Thalès, ou le projet d'application de messagerie sécurisée du gouvernement français, ou bien encore Riot[6], l'application dédiée développée par New Vector.

▶ Quelle sécurité ?

Ces applications se différencient par leurs choix en matière de sécurité mais aussi d'ergonomie, et se distinguent par l'équilibre qu'elles peuvent trouver entre le niveau de sécurité adapté aux besoins de l'organisation utilisatrice et la facilité d'usage pour leurs membres.

Au plan technique, la sécurité repose principalement sur deux éléments : le chiffrement des données, et la sécurité du code. Matrix s'appuie ainsi sur :

- Un audit de sécurité de son algorithme de chiffrement de bout en bout,[7] réalisé par NCC Group en 2016 pour détecter et corriger d'éventuelles failles de sécurité dans le code ;
- La licence libre de son code source[8] : New Vector a choisi de distribuer Matrix sous la licence Apache 2, qui permet à chacun d'utiliser, modifier, distribuer et vendre les logiciels concernés à condition de ne pas s'attribuer la paternité du code. Matrix est donc utilisable indépendamment de la solution New Vector. En cas de rachat ou de faillite de la startup, le code restera ainsi disponible pour la communauté et pourra continuer à vivre.

Le niveau de sécurité est également fonction :

- Des modalités de backup des clés de chiffrement et de l'historique des conversations. Dans l'idéal, pour une sécurité optimale, les clés de chiffrement ne devraient être stockées que sur le terminal utilisé. Ceci peut avoir pour conséquence la perte des messages en cas de perte du terminal, risque

parfois considéré comme non supportable pour une organisation dans le cadre de communications professionnelles.
- De possibilité de déployer la solution sur les serveurs internes de l'organisation concernée, afin de garantir son indépendance vis à vis d'hébergeurs tiers qui peuvent être situés à l'étranger.

▶ Quelles fonctionnalités ?

Le choix d'un service de messagerie s'appuie également sur les fonctionnalités annexes de ces solutions, fonctionnalités développées pour cibler des communautés particulières et répondre aux besoins spécifiques de l'organisation utilisatrice. On peut citer notamment :

La gestion des flottes et du parc de machines. Une gestion centralisée, comme celle choisie par Thales pour toucher les grands groupes, lui permet par exemple de désactiver un terminal perdu ou volé, de détecter les retards de mises à jour, etc. et d'ainsi optimiser l'utilisation de la messagerie. Riot, au contraire, a choisi de fonctionner de façon décentralisée sans structure dédiée à la gestion des flottes.

Les services d'assistance ou d'astreinte. La continuité des communications peut être critique dans certains secteurs, en particulier dans la défense. Dans ce cas, l'assistance du prestataire de la solution, ou même l'astreinte, peuvent être nécessaires voire indispensables.

La gestion des applications tierces et l'interopérabilité. Ces applications de messageries peuvent être couplées avec des clouds, des boîtes emails, etc., l'objectif étant de maintenir un haut niveau de sécurité tout en garantissant l'interopérabilité entre ces différentes applications.

▶ Comment développer une communauté d'utilisateurs ?

Il s'agit enfin d'offrir aux organisations déployant ce type de solutions de proposer l'expérience utilisateur la plus ergonomique, car l'enjeu est de susciter l'adhésion du plus grand nombre et de construire une communauté d'usage. Ceci passe par exemple par :

- La mise à disposition d'un annuaire interne qui permet la constitution d'une « communauté d'usage », qui s'avère être l'un des facteurs déterminants d'adoption d'une application à grand échelle ;
- La possibilité d'utiliser ce service dans des cadres privé et professionnels, ce qui facilite l'adoption d'une solution.

[1] CNN Business, Google still lets third-party apps scan your Gmail data, 20 septembre 2018. money.cnn.com
[2] Le monde informatique, La Russie exige les clés de chiffrement de Telegram, 22 mars 2018. lemondeinformatique.fr
[3] [matrix], matrix.org
[4] Signal, The double ratchet algorithme. signal.org
[5] Citadel Team, citadel.team
[6] Riot, riot.im
[7] Matrix, Matrix's 'Olm' end-to-end security assessment released, 21 novembre 2016. matrix.org
[8] Matrix, Matrix specification. matrix.org

FOCUS ENTREPRISE

SERENDPTECH : GARANTIR L'IDENTITE NUMERIQUE

Entretien avec Émilie THEBAULT, Fondatrice et CEO

▶ Présentation

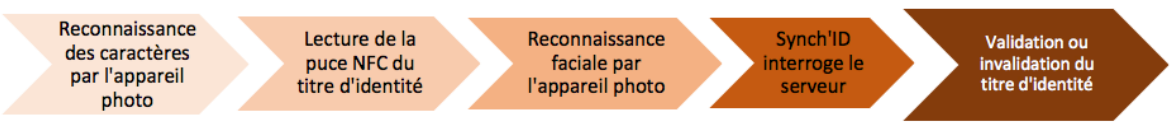
Fondée en 2016 par Emilie Thébault, SERENDPTECH est une société au croisement du KYC (Know Your Customer), de la RegTech et de la cybersécurité. La société a développé Synch'ID, un lecteur de titres d'identité portable sous forme d'application mobile. Synch'ID permet un contrôle instantané, simple et hautement sécurisé des identités, qui repose sur un logiciel capable de traiter les informations reçues et collectées en temps réel, et de les comparer à une base de données de plus d'un milliard de titres.

Pour répondre aux exigences de protection des données ainsi collectées, la solution est non seulement conforme aux exigences règlementaires en vigueur (RGPD, eIDAS, ANSSI, etc.), mais intègre aussi des outils permettant de crypter et anonymiser les données et les résultats ainsi collectées. Synch'ID propose ainsi une authentification renforcée des individus à partir d'un titre d'identité délivré par l'État et ses délégataires.

▶ L'innovation

- L'authentification par Synch'ID prend moins d'une minute depuis un smartphone (IOS ou Android) et suit les étapes suivantes :
- Reconnaissance optique des caractères : l'appareil photo scanne la pièce d'identité ;
- Vérification des informations contenues dans le titre d'identité : le NFC du téléphone lit la puce NFC du titre d'identité ;
- Reconnaissance faciale : l'appareil photo identifie le détenteur du titre d'identité. L'application Synch'ID vérifie qu'il s'agit bien d'un visage filmé en temps réel et non d'une simple photo.
- Ces étapes sont des briques modulables qu'il est possible d'ajouter ou d'enlever selon les besoins de l'utilisateur et l'usage souhaité.

Une fois les informations récoltées, Synch'ID interroge le serveur qui compare les données à sa base d'individus connus. L'application peut ainsi valider les titres authentifiés, et détecter et alerter sur les titres d'identités frauduleux.



Les usages

La solution Synch'ID permet un certain nombre d'usages intéressants pour la défense :

- **Contrôle des identités** lors du processus de recrutement, par exemple dans les centres de recrutement pour contrôler les titres d'identité des candidats ;

- **Contrôle des accès** via la carte d'identité militaire, notamment pour reconnaître les éléments contenus dans la carte CIMS ("carte d'identité professionnelle multiservices") et contrôler l'identité du personnel militaire pour l'accès aux emprises. Pour un contrôle plus encore fiable, la fonction NFC de Synch'ID peut servir à valider les documents d'identité et authentifier chaque individu accédant au lieu concerné ;

- **Contrôle des visiteurs** à l'entrée de sites militaires ou des bâtiments du ministère des Armées pour fluidifier « l'enrôlement » et le contrôle d'identité des visiteurs, et permettre ainsi un gain de temps considérable tout en assurant un contrôle plus fiable et sécurisé ;

- **Contrôle des identités en OPEX**, une fois déployée sur des smartphone mis à disposition du personnel en opérations extérieures afin de simplifier et améliorer le contrôle des identités en opérations.

ACTUALITÉS

L'APPEL DE PARIS POUR LA CONFIANCE ET LA SECURITE DANS LE CYBERESPACE

Le 12 novembre, à l'occasion du 13ème Forum de la gouvernance de l'internet (FGI) qui s'est tenu à Paris du 12 au 14 novembre 2018, La France a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace.

Contexte

Cette initiative s'inscrit dans la lignée des de la Semaine numérique de Paris, où se sont tenus, à côté du FGI, deux autres évènements majeurs liés au numérique :

- Le volet "Nouvelles technologies" du Forum de Paris sur la Paix, du 11 au 13 novembre
- Le Sommet des GovTech/GovTech Summit, consacré à la transformation numérique des États et des démocraties, le 12 novembre ;

Ces événements témoignent de la volonté de la France de se positionner comme un acteur clé de la confiance numérique et de la sécurité du cyberespace, et fédérer autour d'elle dans cette démarche une pluralité de partenaires publics et privés.

Au total, 51 États, 93 acteurs de la société civile et 218 partenaires du secteur privé ont signé l'appel dont une grande majorité d'États européens et d'acteurs américains. La Chine et la Russie, ainsi que le gouvernement fédéral américain, n'en sont en revanche pas signataires.

Objectifs

Après l'échec des travaux du Groupe d'Experts Gouvernementaux de l'ONU en 2017, cette déclaration de haut niveau en faveur de l'élaboration de principes communs de sécurisation du cyberespace doit permettre de relancer des discussions sur un code international de bonne conduite sur internet.

Par cette déclaration, les signataires prennent acte du fait que le cyberspace est le théâtre de nouveaux affrontements et nouvelles menaces tout autant que le lieu de véritables opportunités, et que la cybercriminalité et les cyber-attaques peuvent mettre en danger la vie des individus tout autant que la sécurité des infrastructures vitales et la résilience des sociétés démocratiques.

Ils s'engagent ainsi à agir de concert pour protéger les droits et la sécurité des individus sur Internet comme dans le monde physique, et œuvrer en faveur un cyberespace ouvert, sûr, stable, accessible et pacifique"

Principales dispositions et orientations

Par cette déclaration, les signataires s'engagent notamment en faveur de :

- Une meilleure coopération internationale en matière de lutte contre la cybercriminalité et les cyber attaques, en agissant de concert pour empêcher les « cyberactivités malveillantes qui causent des dommages importants, sans discernement ou systémiques »

- Une collaboration renforcée en la matière et « les pouvoirs publics, le secteur privé et la société civile en vue d'élaborer de nouvelles normes de cybersécurité permettant aux infrastructures et aux organisations d'améliorer leurs systèmes de cyberprotection »

- Un comportement responsable des États et des acteurs privés dans le cyberespace, en favorisant une large acceptation et la mise en œuvre de normes internationales de comportement responsable, ainsi que de mesures de développement de la confiance dans le cyberespace.

- La protection du modèle démocratiques contre les interférences étrangères en développant les capacités d'« empêcher des acteurs étrangers de perturber des processus électoraux ».

- Contre la pratique du hackback : en s'engageant à empêcher des acteurs privés de répliquer par une cyber-offensive à une attaque dont ils seraient victimes, pour leur propre compte ou pour celui d'autres acteurs non étatiques.

CALENDRIER

11EME FORUM INTERNATIONAL DE LA CYBERSECURITE, 22-23/01/2019

Lille Grand Palais accueillera pour sa 11ème Edition les 22 et 23 janvier 2019 le Forum International de la Cybersécurité sur le thème « Security and Privacy by design ; Europe kicks off ! ». Cette nouvelle édition mettra l'accent sur les défis opérationnels, technologiques et humains inhérents à cette nouvelle conception de la cybersécurité.

Co-organisé par la Gendarmerie Nationale et CEIS, avec le soutien de la Région Hauts-de-France, le FIC est devenu l'événement européen de référence en matière de sécurité et de confiance numérique et représente un moment privilégié de réflexion stratégique rassemblant les acteurs publics et privés du secteur. Les ministres de l'Intérieur, Christophe Castaner, des Armées, Florence Parly, et le Secrétaire d'État chargé du numérique Mounir Mahjoubi, ainsi que la Commissaire européenne à l'économie et à la société numériques Mariya Gabriel, participeront à l'événement.

Cette année encore, le ministère des Armées sera représenté sur un pavillon de 90 m2 au cœur du salon.

L'événement sera également l'occasion pour le ministère des Armées de partager son expérience et son expertise dans deux tables rondes dédiées à l'innovation en cybersécurité et aux technologies de défense active. Pour plus d'information et pour toute demande d'inscription, veuillez consulter le site du FIC2019

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