Lettre mensuelle – **Mai 2021 – Disponible sur omc.ceis.eu**

Table des matières

ANALYSES.....

1) Union européenne et OTAN : les piliers de la cyberdéfense européenne 1

2) Quelle régulation pour l'industrie d'armement cyber ? 7

FOCUS INNOVATION .....

Freemindtronic : Une barrière physique pour reprendre le contrôle de ses données 12

CALENDRIER .....

Quels défis pour la cyberdéfense de demain ? (06, 07 et 08 juillet 2021) 14

ACTUALITÉ.....

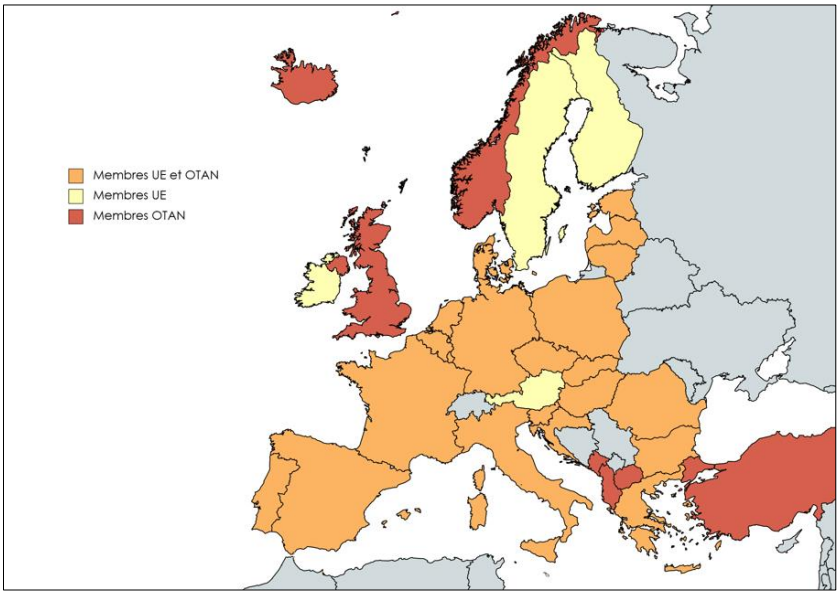
Point d'étape sur la feuille de route de l'IA de défense 15

ANALYSES (1/2)

Union européenne et OTAN : les piliers de la cyberdéfense européenne

Deux visions de la sécurité européenne se distinguent. Si certains États souhaitent pérenniser les garanties de la présence américaine sur le continent (pays baltes, Pologne…), d'autres, tels que la France et l'Allemagne, souhaitent y développer un cadre de sécurité collective plus autonome. Ces approches influent sur la défense de l'Europe, et plus précisément sur l'Union européenne (UE) et l'Organisation du traité de l'Atlantique nord (OTAN) qui en sont les acteurs incontournables.

En matière de cyberdéfense, ces deux organisations ont progressivement adapté leurs institutions pour appréhender le risque cyber grandissant. L'UE et l'OTAN ont instauré une politique s'appuyant tant sur des décisions et des textes réglementaires, que sur la création d'agences spécialisées. Elles partagent des objectifs similaires visant, d'une part, à renforcer la sécurité de leurs réseaux et de leurs systèmes d'information (SI), et d'autre part, à renforcer les capacités des pays qui les composent[1]. Sur ce dernier point, l'OTAN est particulièrement impliquée dans le développement des cyber-capacités militaires des Alliés, contribuant *de facto* à la résilience de certains États-membres de l'UE et à la sécurité de cette dernière.



Pays-membres de l'UE et/ou de l'OTAN (Source : CEIS/Avisa Partners)

Par leur vingt et un membres en commun, l'UE et l'OTAN ont une zone d'action analogue, qui peut conduire à des chevauchements voire à des doublons d'activités. D'autant que les deux institutions ne se sont pas coordonnées dans le développement de leurs cyberdéfenses, domaine dans lequel elles communiquent par ailleurs peu et plus encore en ce qui concerne la sphère militaire. Pour autant, des éléments de subsidiarité ou de complémentarité existent bel et bien entre ces organisations. Le contexte international offre alors des opportunités de les rationaliser et de les mettre en avant au profit d'une cyberdéfense européenne plus forte.

[1] Vincent Joubert, Jean-Loup Samaan, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », *Hérodote*, n° 152-153, 2014, pp. 261-275.

L'ère Trump posait en effet des incertitudes quant à l'engagement américain en Europe, interrogeant la pérennité de l'OTAN, mais l'administration Biden a depuis confirmé le « retour des puissances » (*great-power competition*) et son intérêt pour le partenariat transatlantique. Si sa politique étrangère peut remettre en cause le projet d'une défense européenne forte, elle peut aussi inciter l'Europe à exister davantage dans cette compétition entre grandes puissances en tant que bloc politique d'États, plutôt que sous la seule forme d'une alliance militaire. Le Brexit constitue un autre facteur en faveur de l'Europe de la défense. Alors que le Royaume-Uni en freinait le développement, son retrait de l'Union ouvre la voie à une sécurité commune plus ambitieuse. Enfin, l'instabilité aux portes de l'UE, hors zone d'intérêt direct de l'OTAN, avec le Sahel notamment, mobilise les forces armées de ses membres et contribue à leur interopérabilité dans le cadre d'opérations et de missions militaires communes[2].

Comment ce nouvel environnement stratégique pour l'Europe se traduit-il dans le cyberespace ? Alors que l'UE et l'OTAN peuvent s'enrichir mutuellement sur de nombreux points, en quoi sont-elles complémentaires dans le cadre de la cyberdéfense européenne ?

1. Un développement en « miroir » des entités cyber européennes et otaniennes

L'UE et l'OTAN développent leurs propres architectures de cyberdéfense militaire. Celles-ci sous-tendent le partage d'informations et de bonnes pratiques, aussi bien entre leurs membres respectifs qu'avec les États partenaires de ces organisations. Ces architectures se déclinent en organes de gouvernance et en entités dédiées à des missions de cyberdéfense. Pour l'UE, certaines des plus actives d'entre elles relèvent de la coopération structurée permanente (CSP ou PESCO en anglais), cadre découlant de la politique de sécurité et défense commune (PSDC) permettant à un groupe d'États-membres de prendre des engagements mutuels en matière de dépenses, de programmes d'armement et de capacités opérationnelles.

Les principales structures de cyberdéfense sont présentées ci-dessous. Le tableau *infra* vise à montrer que les deux organisations sont dotées de sorte à pouvoir couvrir le spectre des cyber-opérations, et non à mettre sur le même plan leurs entités dont les mandats et les périmètres sont distincts.

Entités de cyberdéfense militaire de l'UE et de l'OTAN (liste non-exhaustive)

Union européenne	OTAN
Centre d'alerte et de réaction aux attaques informatiques	
CERT-EU	NATO Cyber Security Centre (NCSC) – ex-NCRIC
Le CERT-EU et le NCSC, outre le traitement et le signalement des incidents de sécurité des réseaux et des SI, partagent des bonnes pratiques visant à réduire le risque cyber et ses conséquences. Si le CERT-EU se limite aux institutions, agences et organes de l'UE, le NCSC/NCRIC est compétent pour une partie des infrastructures de l'OTAN.	
Protection des systèmes d'information et de communication (SIC)	
EU Agency for Cybersecurity (ENISA)	NATO Communications and Information Agency (NCIA)
Ces agences sont chargées de la gouvernance et de la sécurité des SIC de leurs organisations respectives, ainsi que du partage à cet égard de bonnes pratiques. Leur périmètre diffère néanmoins : l'ENISA intervient auprès des autorités nationales et des institutions européennes (civiles), alors que le NCIA agit pour les états-majors et armées de l'OTAN.	

[2] EUFOR Althea (Bosnie-Herzégovine), EUNAVFOR Atalanta et EUTM Somalia (Somalie), EUTM Mali, EUTM RCA (République centrafricaine), EUNAVFOR Med IRINI (Méditerranée).

Union européenne	OTAN
***Command-and-control* (C2) des opérations militaires**	
Cyber and Information Domain Coordination Center (CSP/CIDCC)	Cyber Operations Centre (CYoC)
Alors que l'OTAN dispose sur le plan opérationnel d'un centre C2 pour les cyber-opérations (CYoC), l'UE n'a pas d'entité spécifiquement dédiée. Son projet allemand CSP/CIDCC constitue néanmoins l'embryon d'un centre de coordination multinationale en matière cyber et d'information, comptant quatre participants (France, Allemagne, Hongrie et Pays-Bas).	
Alerte et réponse à incident	
Cyber Rapid Reaction Team (CSP/CRRT)	Cyber Rapid Reaction Team (NATO/CRRT)
Ces deux équipes de réaction rapide ont des périmètres d'actions très différents. Si le NATO/CRRT peut agir au profit des trente-six Alliés, le projet lituanien CSP/CRRT n'a pour le moment pas les bases juridiques pour intervenir au-delà de ses six seuls États-membres participants (Croatie, Estonie, Lituanie, Pays-Bas, Pologne et Roumanie).	
Formation et entraînement	
European Security and Defence College (CESD)	NATO Defence College (NDC)
Ces deux institutions d'enseignement dispensent des sessions de formations sur la cyberdéfense et les problématiques attenantes (risque cyber, protection des infrastructures critiques, etc.). Si le NDC s'adresse exclusivement à des officiers supérieurs de pays-membres l'OTAN, le CESD a une approche plus globale en s'adressant aussi à des diplomates.	
Agence européenne de défense (AED)	Cooperative Cyber Defence Center of Excellence (CCDCOE)
Visant à combler les lacunes au sens large en matière de formation et de capacités opérationnelles des ministères européens de la Défense, l'AED organise des exercices cyber tels que Cyber Phalanx, MIC[3] et CYBRID. Le CCDCOE a été créé *ad hoc* pour soutenir l'OTAN et les Alliés dans le domaine de la cyberdéfense. Le centre pourvoit des formations et des exercices pour les militaires et les décideurs (Cyber Coalition, Locked Shields, Crossed Swords…).	

Du fait de leurs histoires et de leurs natures respectives, la cyberdéfense militaire est aujourd'hui moins institutionnalisée à l'UE qu'à l'OTAN. L'Alliance – dont l'essence même tient à la défense et à la cyberdéfense *de facto* de ses membres – a des moyens financiers surclassant ceux de l'Union sur le plan militaire, et donc dispose de plus d'entités *ad hoc* matures telles que le CYoC et le CCDCOE. L'OTAN pèse ainsi davantage sur le développement des capacités de cyberdéfense militaire de ses nations membres que l'UE. Bruxelles cultive en effet une approche plus globale de la défense cyber dont la dimension militaire n'est qu'un volet : cela est perceptible dans la participation aux projets CSP qui s'effectue finalement au gré des États-membres.

L'UE, qui aspire néanmoins à agir de façon autonome et collective dans le cadre de cyber-opérations militaires[4], possède tous les instruments pour organiser, équiper, entraîner ses États-membres. Outre l'AED, les projets CSP/CIDCC et CSP/CRTT forment des cadres permettant aux Européens de contribuer de façon décisive aux efforts communs, à la condition d'être élargis à plus de participants. Cette notion de « solidarité européenne » est par ailleurs prévue par l'art. 42.7 du traité de l'UE[5], la clause de défense mutuelle, qui stipule que les États-membres peuvent se solliciter en cas de cyberattaque majeure contre l'un d'entre eux. Les modalités de sa mise en œuvre telles que les délais et le type d'assistance restent toutefois à déterminer.

[3] EU MilCERT Interoperability Conference.
[4] Vision partagée, action commune : Une Europe plus forte, Union européenne, Juin 2016, p. 16 (lien).
[5] Article 42, Traité sur l'Union européenne, *EUR-Lex* [en ligne], 9 mai 2008.

Cette disposition européenne complète ainsi l'art. 5 du traité otanien sur la sécurité collective. Les membres de l'UE et de l'OTAN peuvent alors invoquer ces deux textes en cas de cyberattaque d'envergure en Europe.

2. Une cyberdéfense européenne à rationaliser selon une approche globale

2.1. Face aux menaces des stratégies en « zone grise » …

Les relations entre l'UE et l'OTAN se sont structurées au début des années 2000. Lors du sommet de Varsovie en 2016, les deux organisations ont signé une déclaration conjointe définissant leur coopération et leurs préoccupations. Les questions d'intérêt commun sont désormais traitées à l'occasion d'un dialogue stratégique de haut niveau, qui porte aujourd'hui sur, outre le risque cyber et les menaces hybrides, la pandémie de Covid-19, la Chine, le Moyen-Orient, l'Afghanistan, les Balkans occidentaux et la Russie.

L'UE voit ses flancs Est et Nord sous pression. Depuis la crise en Ukraine en 2014, Bruxelles veille à se coordonner avec l'OTAN sur les dossiers relatifs à la Russie[6]. Sa recherche de complémentarité présente toutefois des limites du fait d'une fragmentation de ses États-membres sur la question. L'Autriche – qui ne fait pas partie de l'Alliance – est par exemple traditionnellement favorable à plus de souplesse vis-à-vis de Moscou, alors que les États baltes s'inscrivent sur une ligne « atlantiste » plus dure, en raison des tensions récurrentes le long de leurs frontières avec la Russie[7]. Pour cette dernière, l'élargissement à ses portes de l'UE et de l'OTAN, que le Kremlin associe à une forme de pression militaire et informationnelle[8], légitime le renforcement à la fois de son arsenal cyber et de ses campagnes de manipulations de l'information en Europe.

L'Europe se confronte ainsi à des compétiteurs recourant à des stratégies hybrides dans lesquelles le cyber occupe une place grandissante. Celles-ci visent à « *obtenir des gains en orchestrant les effets* [d'actions] *diplomatiques, informationnelles, militaires, économiques et juridiques, selon une dynamique d'ensemble ambiguë et souvent difficile à déceler ou à dénoncer*[9] ». Leur généralisation nécessite de pouvoir anticiper, détecter, comprendre, caractériser et, le cas échéant, attribuer les actions adverses, ce qui permet *a minima* d'en limiter les effets et de reprendre l'initiative dans l'intention de décourager. Les travaux de la « Boussole stratégique », lancés par la présidence allemande du Conseil de l'UE en 2020, permettront à cet égard de faire converger les Européens autour d'intérêts communs et d'une analyse de la menace partagée.

Face au recours croissant à des actions en « zone grise », investir le cyberespace devient essentiel à la liberté d'action européenne. Si l'OTAN a rapidement reconnu ce milieu comme un « domaine opérationnel », l'UE accroît ses efforts pour mieux appréhender les enjeux de sécurité dans ce nouvel espace de compétition[10], comme en témoigne les efforts de certains États-membres – dont la France et le Portugal – pour rédiger des doctrines consacrées et conduire des réflexions autour des espaces communs/stratégiques contestés.

La définition d'une posture et d'une riposte potentielle de l'UE implique dès lors la coordination étroite de ses outils diplomatiques, juridiques, économiques et informationnels, ainsi que de ses moyens militaires nationaux de renseignement et d'action, y compris de lutte informatique. Sur ce dernier point, les réflexions en cours quant à l'introduction d'une potentielle réponse cyber militaire aux agressions adverses ont pour le moment lieu dans le cadre des missions et des opérations de la PSDC, qui se situent principalement hors zone UE.

---

[6] *Les relations OTAN-UE*, Fiche d'information, Division Diplomatie Publique, OTAN, Mars 2021, p. 2.
[7] *Actualisation stratégique*, Ministère des Armées, Février 2021, p. 11.
[8] Fédération de Russie, *Stratégie de sécurité nationale*, 31 décembre 2015, point 12.
[9] *Op. cit. Actualisation stratégique*, 2021, p. 39.
[10] *Ibid*, p. 29.

Celles-ci sont en l'état alimentées par les travaux de synthèse du Centre de situation et du renseignement de l'UE et par le souhait à Bruxelles de rendre la clause de défense mutuelle (art. 42.7 du TUE) plus opérationnelle.

2.2. … assurer un continuum entre les volets militaire et civil de la cyberdéfense

L'UE favorise, pour rappel, une approche globale de la cyberdéfense dont la dimension militaire n'est qu'un volet. Si elle s'est organisée de sorte à pouvoir agir sur tout le spectre des cyber-opérations militaires, ses efforts les plus significatifs ces dernières années sont ceux ayant conduit à un meilleur encadrement du cyberespace, à la fois en termes de normes et de diplomatie. Parmi ces réalisations, la directive NIS, le RGPD, le règlement eIDAS, le Cybersecurity Act, la boîte à outils cyber-diplomatiques et les réseaux de coopération entre ses États-membres (CSIRTs Network, CyCLONe et NIS Cooperation Group principalement) sont autant d'initiatives dans lesquelles la France a par ailleurs joué un rôle majeur.

L'UE doit capitaliser sur sa puissance normative et diplomatique pour enrichir mutuellement les dimensions civile et militaire de sa cyberdéfense. Dans le contexte d'un « retour des puissances » et de recours grandissant à des stratégies hybrides, sa défense cyber ne peut se limiter à des réponses strictement capacitaires ou opérationnelles. Elle doit contribuer plus généralement à la sécurité internationale par la promotion de mesures de confiance, en participant aux discussions sur l'applicabilité du droit international au cyberespace et en accélérant les synergies avec le secteur privé. L'aspect dual du cyberespace implique en effet que les réglementations civiles soient parfois prescriptrices pour les applications militaires[11]. Le développement d'un tissu industriel à partir d'un système de confiance, au travers de la densification de l'arsenal réglementaire civil, bénéficierait alors directement à la résilience de tous les SI de l'UE et de ses États-membres, permettant de surcroît de meilleures planification et conduite des opérations.

À l'inverse de l'OTAN, dont les engagements de défense découlent d'un consensus souvent difficile à obtenir, en raison de la diversité politique des Alliés (et de la cadence imposée par les États-Unis), l'UE est une organisation aux compétences supranationales, mais aussi intergouvernementales en matière de défense, dont relève *a fortiori* la cyberdéfense[12]. Bruxelles est ainsi en mesure d'influer directement sur les orientations, les dispositifs et les dépenses des États-membres. Ces derniers ont dès lors un champ d'action plus large que les Alliés pour développer la cyberdéfense européenne. L'OTAN et l'UE affichent ainsi une complémentarité vis-à-vis de l'Europe de la défense : si la première peut lui faire bénéficier de son expertise militaire, la seconde est en mesure d'apporter une haute valeur ajoutée en faisant interagir les sphères militaire et civile.

En outre, la stratégie américaine du *burden sharing* peut profiter à terme au développement de la base industrielle et technologique de défense européenne (BITDE). Pour alléger son implication financière dans la sécurité collective de l'OTAN, les États-Unis demandent en effet aux Alliés de consacrer au moins 2% de leurs PIB à leurs propres dépenses militaires. Dans ce cadre, ces financements sont susceptibles de bénéficier à la R&D de défense européenne en général, ainsi qu'aux cyber-capacités des vingt et un membres à la fois de l'OTAN et de l'UE. Pour autant, seuls sept d'entre eux[13] atteignent actuellement ce niveau[14].

[11] Morgan Jouy, « Une cyberdéfense collective en Europe ? », Note de recherche, n°83, IRSEM, 2017 (lien).
[12] Jaap de Hoop Scheffer, Strengthening the EU's Cyber Defence Capabilities, CEPS, 2018 (lien).
[13] France, Estonie, Grèce, Lettonie, Lituanie, Pologne et Roumanie.
[14] *Defence Expenditure of NATO Countries (2013-2020)*, Public Diplomacy Division, NATO, 21 October 2020.

3. Une coopération de cyberdéfense encourageante mais encore insuffisante

En 2018, l'UE et l'OTAN ont signé une autre déclaration conjointe visant à institutionnaliser des consultations politiques relatives à la sécurité en Europe et dans son voisinage. Si ces deux organisations font preuve de convergence dans leurs intérêts stratégiques, il convient de rappeler qu'elles poursuivent leurs propres agendas : l'Union vise à « *promouvoir la paix, ses valeurs et le bien-être de ses peuples* » au travers d'un espace et d'un marché intérieur communs, alors que l'Alliance existe pour assurer la sécurité collective de ses membres. Leur coopération doit alors être appréhendée à la lumière de la défense de ces objectifs distincts.

Ces institutions organisent, à intervalle régulier, des visites croisées de haut niveau avec notamment le Secrétaire général de l'OTAN qui prend fréquemment la parole devant le Conseil européen, et le Haut représentant de l'UE pour les affaires étrangères et la politique de sécurité qui participe aux réunions en format « 2+2 » de l'Alliance. Ces événements constituent autant d'occasions de traiter des questions d'intérêt commun (cf. 2.1.) et de faire le point sur leur coopération. À l'échelon stratégique, les directeurs généraux des états-majors de l'UE (EMUE) et de l'OTAN (IMS) se rencontrent aussi chaque année. Dans le domaine de la cyberdéfense, si la dernière session en mars 2021 n'a pas été particulièrement significative[15], celle de 2019 a mis en exergue le besoin de renforcer l'interopérabilité des SIC et de faciliter l'échange de données classifiées.

À des niveaux plus opérationnels, le CERT-EU et le NCSC/NCIRC (cf. 1) ont conclu en 2016 un arrangement technique relatif au partage d'informations. Celui-ci prévoit la tenue d'ateliers relatifs à l'analyse des menaces. Ce cadre a permis de développer une relation soutenue entre les experts techniques de part et d'autre, produisant ainsi des résultats tangibles, notamment lors des attaques par rançongiciels de 2017 (WannaCry et NotPetya). L'OTAN, par le biais du NCSC/NCIRC, a en effet pu envoyer un message d'alerte à l'UE et lui partager des données cruciales[16]. En 2016, l'UE et l'OTAN ont institué les Parallel and Coordinated Exercises (PACE), qui consistent en l'organisation croisée chaque année d'un exercice évaluant l'efficacité de l'UE et de l'OTAN en cas de cyberattaque, ainsi que d'améliorer la synchronisation de leurs activités de réponse aux crises.

Si l'UE et l'OTAN cultivent un bon niveau de coopération stratégique, au regard de leur convergence de vues sur des sujets d'intérêt commun et des visites régulières de haut niveau, celle-ci se heurte parfois à la réticence de certaines nations membres à partager leurs informations avec d'autres (entre Chypre et la Turquie par exemple). Ces tensions internationales tendent en effet à resurgir et à avoir un impact sur le plan opérationnel. De plus, la coopération n'est éprouvée qu'à l'occasion d'exercices, et non en conditions réelles. Le théâtre le plus opportun à cet effet serait le plus vraisemblablement la Méditerranée où les deux organisations sont actives.

Conclusion : l'UE et l'OTAN sont complémentaires et non redondantes

D'autres pistes pour consolider la cyberdéfense militaire de l'Europe existent, à commencer par un effort de cohérence et un *leadership* de poids à l'UE, plutôt que l'ajout de nouvelles entités. Cette exigence implique dès lors une volonté politique forte. En 2022, la France assurera la présidence du Conseil de l'UE (PFUE), qui est une occasion unique de renforcer sa force de proposition à l'OTAN et à l'UE, dont elle est respectivement un pilier et un membre fondateur. Elle est ainsi légitime pour améliorer les synergies entre ces organisations.

[15] « Le directeur général de l'État-major militaire international de l'OTAN et son homologue de l'État-major de l'Union européenne font le point sur la coopération actuelle », *OTAN* [en ligne], 16 mars 2021.
[16] « NATO-EU Relations », *Factsheet*, NATO, Février 2019, p. 2.

Pour la cyberdéfense militaire, la feuille de route de la PFUE peut prendre en compte les objectifs suivants :

1. Au niveau politique, veiller à la complémentarité avec les autres États-membres, particulièrement la Slovénie qui précédera la France à la tête du Conseil de l'UE, mais aussi la République tchèque et la Suède qui la suivront. Le développement de la cyberdéfense militaire ne peut se limiter à un seul mandat et implique une coordination globale et dans la durée. La France doit initier – si ce n'est poursuivre – une dynamique en sa faveur.
2. Renforcer la coopération stratégique entre les autorités de cyberdéfense militaire des États membres, notamment grâce à la création d'un forum des *Cyber Commanders*, en complément de la traditionnelle « CIS&CD Conference » du Service européen pour l'action extérieure (UE/SEAE).
3. Initier et soutenir la création d'un réseau européen de CERT militaires pour développer l'interopérabilité des États-membres. Ce projet, identifié dès 2014 mais délaissé depuis, est une opportunité de réunir des ressources nationales au profit d'une coopération fructueuse d'un point de vue national mais aussi de l'UE.

ANALYSES (2/2)

QUELLE RÉGULATION POUR L'INDUSTRIE D'ARMEMENT CYBER ?

Le développement du numérique dans nos sociétés et la concrétisation du cyberespace en tant que théâtre d'affrontements a fait émerger une industrie de l'armement cyber. Un véritable écosystème privé s'est constitué pour répondre aux besoins des États qui souhaitent aller au-delà de leurs capacités propres de recherche et développement pour mener des opérations dans le cyberespace.

Parmi ces acteurs privés : les courtiers en vulnérabilités dites *zero-day*. Ces failles consistent en des vulnérabilités informatiques n'ayant fait l'objet ni de publication ni de correctif connu. Un chercheur les identifiant peut alors les vendre avec les *exploits*[17] associés à un courtier pour en tirer les meilleurs bénéfices, plutôt que d'en faire part, pour sa correction, à l'éditeur du logiciel ou au fabricant du matériel concernés. Ces courtiers revendent ensuite ce type de vulnérabilités soit à des États, soit à des entreprises privées de vente d'accès ou AaaS (*Access-as-a-Service*), qui fournissent notamment les forces de l'ordre. Les acquéreurs des *exploits* les intègrent alors à leurs produits clé en main d'interception des communications et de compromission de systèmes informatiques (ordinateurs et *smartphones*).

La nature privée de cet écosystème n'est cependant pas sans contrepartie. Elle implique un risque de prolifération dont les conséquences néfastes sont de plus en plus visibles, et pourraient justifier un encadrement plus strict de la part des autorités publiques et de la communauté internationale.

1. Une prolifération protéiforme des cyber-armes aux risques multiples

1.1. Écosystème privé de l'armement : une attractivité qui augmente le risque de fuite de cerveau

Pour les experts, l'industrie de l'armement cyber offre des rémunérations supérieures à celles des entreprises de cybersécurité défensives, des éditeurs de logiciels et surtout des entités étatiques. Il existe donc un risque fort pour les États de voir leurs meilleurs éléments rejoindre la sphère privée, et ce parfois pour une entreprise

[17] Un exploit est un élément de programme permettant l'exploitation d'une faille de sécurité informatique.

étrangère. Pour les nations concernées, cette fuite de cerveau représente non seulement une perte de capacités sous la forme de ressources humaines, mais également un gain potentiel de capacités par un État tiers non souhaité. À titre d'exemple, l'entreprise émirienne DarkMatter, dont la création a bénéficié de la participation active de la CIA, a depuis recruté plusieurs anciens membres des renseignement américains, ce qui embarrasse l'agence aujourd'hui[18].

1.2. Des « dépôts » d'armes cyber très convoités

Les industriels de l'armement cyber constituent une cible de choix aussi bien pour des États tiers que pour des organisations cybercriminelles classiques. Outre la valeur pécuniaire des *exploits* qu'elles possèdent, la valeur métier associée est évidente pour les groupes en capacité de les attaquer : ils sont une source d'outils que les pirates pourront réutiliser pour leurs propres opérations. Le piratage en juillet 2015 de l'entreprise italienne Hacking Team a par exemple donné lieu à la mise en ligne « publique » d'une grande partie de ses données, parmi lesquelles plusieurs kits d'exploitation de vulnérabilités zero-day. Leurs outils offensifs ont depuis été utilisés par des cartels mexicains contre des journalistes ou encore par des groupes APT affiliés à la Russie et à la Chine. Ce piratage a par ailleurs suscité la publication du premier *exploit* connu de micrologiciels UEFI[19], offrant aux logiciels malveillants (*malwares*) correspondants une capacité de persistance et de furtivité particulièrement importante.

1.3. Une prolifération d'apparence légitime

Les entreprises proposant des capacités offensives cyber ont généralement un large panel de clients. Elles fournissent soit leur pays d'origine, soit les pays alliés et amis de celui-ci. Cette tendance est poussée par deux facteurs : les États dont relèvent ces entreprises peuvent encourager ces exportations car ils souhaitent favoriser leur développement commercial, gage de pérennité de leur savoir-faire. En second lieu, il peut également être dans leurs intérêts de venir en aide à leurs alliés en leur fournissant de telles capacités. Ceci concerne notamment les produits clés en main de surveillance et d'interception des communications. Cette largesse dans les exportations est néanmoins susceptible de se retourner contre :

- L'image du pays exportateur, qui peut être écornée par l'usage avéré de ces outils à l'encontre d'opposants politiques et d'activistes, et plus encore lorsque ceux-ci militent pour les droits de l'homme. On peut à ce titre citer l'utilisation alléguée d'outils de surveillance de l'entreprise israélienne NSO Group par les services saoudiens à l'encontre du journaliste Jamal Khashoggi en amont de son assassinat ;
- Les intérêts des entreprises du pays exportateur, qui peuvent être compromis lorsqu'ils entrent en concurrence avec ceux des pays importateurs. Ces derniers, nécessairement soucieux de soutenir leurs propres entreprises, peuvent utiliser cet outillage cyber à l'encontre des entreprises exportatrices.

[18] https://www.nytimes.com/2021/01/26/us/politics/intelligence-officers-foreign-governments.html

[19] L'UEFI (Unified Extensible Firmware Interface) est un micrologiciel permettant l'amorçage du système d'exploitation. Sa compromission permet au malware de persister de cacher des processus au système d'exploitation et de persister malgré la réinstallation de ce dernier.
https://www.trendmicro.com/en_us/research/15/g/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems.html

2. Un encadrement des actions de cet écosystème privé est-il possible ?

2.1. Le rétropédalage de l'arrangement de Wassenaar

L'arrangement de Wassenaar est un régime multilatéral de contrôle des exportations visant à coordonner les politiques d'exportation d'armements conventionnels et de technologies à usage dual. Entré en vigueur dans sa version initiale en 1996, le traité n'a pas de valeur juridiquement contraignante. Il incite ses signataires à intégrer à leur législation nationale ses principes, et à respecter l'obligation de notifier les membres des échanges de biens ou de matériaux sensibles figurant sur une liste dédiée. Il a fait l'objet de révisions en 2012-2013, intégrant divers biens et technologies duales pouvant servir au fonctionnement de « logiciels d'intrusion », alors que ceux-ci ne sont pas intégrés en tant que tels à cette liste.

Le périmètre de la liste prévue par l'arrangement de Wassenaar a suscité l'inquiétudes du monde de la cybersécurité, qui craignait de voir des outils et des activités à vocation défensive sévèrement encadrés par ce traité. Ce choix d'un périmètre très large, dont les intentions étaient certainement louables, a effectivement eu des effets pervers, comme en témoigne par exemple l'annulation de la Zero Day Initiative en 2015.

Cette organisation, qui vise à acheter des vulnérabilités non pas pour les revendre à des tiers, mais au contraire pour les communiquer aux éditeurs en vue de correction[20], a dû annuler en 2015 une compétition de hacking sous la forme de bug-bounty, qui réunissait physiquement les participants à Tokyo, de peur qu'elle ne soit accusée de retourner aux États-Unis avec des vulnérabilités découvertes au Japon. La Zero Day Initiative a finalement considéré que le transport de ces failles informatiques pouvait être constitutif d'une violation de l'arrangement de Wassenaar.

On notera également que l'entreprise française Vupen, fournisseur d'*exploits* pour des agences de renseignement occidentales, qui s'est expatriée aux États-Unis en 2015 et opère aujourd'hui la plateforme Zerodium, courtier de vulnérabilités zero-day de premier ordre.

De même, c'est à la même période qu'a été fondée aux Émirats arabes unis l'entreprise DarkMatter, aujourd'hui l'un des principaux fournisseurs AaaS, avec la volonté de contourner les limitations liées à l'arrangement de Wassenaar. Son objectif est de développer des outils localement avec des spécialistes recrutés partout dans le monde, plutôt que d'en acheter à des entreprises étrangères. Quitte à ce que ces experts puissent un jour être amenés à pirater leurs propres compatriotes[21].

Pour corriger ces effets de bord, l'arrangement de Wassenaar a assoupli en 2017 le régime de contrôle des exportations des biens et technologies impliqués dans les logiciels d'intrusion, à l'initiative des États soucieux de soutenir leurs écosystèmes nationaux privés. Le nouveau périmètre correspond cette fois à une définition davantage portée sur la finalité, qui permet d'exclure les outils et activités visant à protéger les systèmes d'information.

2.2. Des projets d'acteurs privés et de la société civile aux effets limités

Certains acteurs de la société civile et de la sphère privée s'opposent fermement à la monté en puissance d'une industrie de l'armement cyber. Sur le plan opérationnel d'abord. Outre la Zero Day Initiative, on peut citer l'équipe Project Zero de Google, dont l'objectif est de rechercher des vulnérabilités zero-day, à la fois dans les produits de l'entreprise, mais également dans ceux d'autres sociétés et dans les logiciels open-

[20] La Zero Day Initiative appartient aujourd'hui à Trend Micro, et fournit aux clients de l'éditeur des contre-mesures dans l'attente de mise à disposition de mise à jour corrective par l'éditeur.

[21] https://www.reuters.com/investigates/special-report/usa-spying-raven/

source. Cette équipe de chercheurs partage ses découvertes aux éditeurs sans contrepartie financière. Ces initiatives vont directement à l'encontre des intérêts de l'industrie des capacités offensives cyber.

En juillet 2019, la fondation Mozilla puis l'entreprise Google ont refusé d'approuver DarkMatter en tant qu'autorité de certification[6], afin d'empêcher la société émirienne de fournir des certificats TLS à des acteurs malveillants et ainsi faciliter leurs actions offensives. Ces certificats TLS visent, pour rappel, à garantir aux utilisateurs que le site Internet sur lequel ils naviguent soit bien légitime. En conséquence, les certificats TLS émis par DarkMatter ne sont pas valides au sein des navigateurs Chrome et Firefox.

Sur le plan judiciaire, plusieurs fournisseurs AaaS font l'objet à travers le monde de poursuites, comme le montre la liste régulièrement mise à jour du centre de recherche canadien The Citizen Lab[22]. À cet égard, la société israélienne NSO Group est particulièrement visée, étant poursuivie par plusieurs entreprises majeures du numérique. En octobre 2019, WhatsApp a ainsi déposé une plainte à son encontre, en demandant à la justice américaine une injonction permanente destinée à empêcher tout piratage par NSO des systèmes de l'entreprise (la violation des comptes d'utilisateurs du service étant par extension une compromission du service en lui-même). En décembre 2020, Google, Microsoft, Cisco, VMware et l'Internet Association ont rejoint l'action en justice intentée par WhatsApp.

En mai de la même année, déjà, Amnesty International avait soutenu une action judiciaire portée par des citoyens israéliens qui demandait à retirer à NSO Group toute licence d'exportation, du fait de son usage par des clients étrangers à l'encontre de défenseurs des droits de l'homme (une demande par ailleurs rejetée par un tribunal de Tel-Aviv en juillet 2020[23]).

2.3. Les propositions du Cyber Statecraft Initiative pour une stratégie anti-prolifération de l'OTAN

Le Cyber Statecraft Initiative, projet du Scowcroft Center for Strategy and Security de l'influent think-tank Atlantic Council, a formulé en mars 2021 un certain nombre de propositions visant à limiter la prolifération cyber dues à cet écosystème privé[24]. Celles-ci sont regroupées en trois catégories :

- « Comprendre et nouer des partenariats » : aucun État n'est en mesure par lui-même d'influencer significativement le marché. Le rapport plaide pour une meilleure prise en compte du sujet dans toutes les enceintes multilatérales pertinentes, notamment à travers le GGE (Group of Governmental Experts) et l'OEWG (Open-Ended Working Group) des Nations Unies.

- « Façonner » : restreindre et influencer le comportement des acteurs du marché, qu'ils soient fournisseurs ou clients. Cela passe notamment par la création de listes noires pour les entreprises ayant vendu des capacités à des entités considérées comme préoccupantes. Ces listes auraient vocation à interdire de se fournir auprès de ces vendeurs, mais également à limiter les ventes d'armement et autres formes d'assistance aux États qui se fournissent auprès de ces vendeurs. Notons que ceci rejoint la nouvelle version du régime de contrôle des exportations des biens à double usage[25] adopté par l'Union européenne en mars 2021. Ce nouveau régime prévoit notamment un renforcement du contrôle des exportations pour les technologies de cyber-surveillance lorsque l'autorité nationale compétente considère qu'elles sont

22 https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/

23 https://www.amnesty.org/en/latest/news/2020/07/israel-court-notorious-spyware-firm-nso/

24 Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf (atlanticcouncil.org)

25 https://www.europarl.europa.eu/doceo/document/TA-9-2021-0101_FR.html

potentiellement destinées à une utilisation impliquant des violations graves des droits de l'homme ou du droit humanitaire international.

- « Limiter » : D'abord, agir sur le cœur de métier des AaaS par la divulgation des vulnérabilités dont l'exploitation par les fournisseurs sur liste noire est connue. Le rapport suggère de réduire par exemple le délai de divulgation des vulnérabilités zero-day correspondantes, et d'augmenter les capacités des organisations gouvernementales en charge d'exposer les outils, tactiques et procédures des opérations cyber de ces fournisseurs sur liste noire. Sur la question de la divulgation, le rapport du Cyber Statecraft Initiative vise donc un périmètre réduit de vulnérabilité, là où d'autres organisations suggèrent d'encourager des programmes de divulgation coordonnée des vulnérabilité[26].

  Ensuite, créer des restrictions post-emplois pour les agents publics spécialisés dans l'armement et la conduite d'opérations offensives cyber. En d'autres termes, il pourrait leur être imposé d'informer leur agence d'origine jusqu'à 10 ans après leur départ d'un poste sensible. Cela pourrait également se traduire par des actions légales à l'encontre des fournisseurs AaaS et de leurs sous-traitants, afin d'apposer un coût financier et d'image aux ventes et opérations jugées problématiques.

  Enfin, les auteurs suggèrent d'encourager les vendeurs de solutions de sécurité offensives à intégrer des limitations techniques à leurs produits, notamment concernant leur périmètre d'applicabilité géographique.

Dans l'alignement de la position américaine, le rapport du Cyber Statecraft Initiative ne propose – ni ne mentionne – de développer le principe de cyber diligence. Celui-ci voudrait que la responsabilité d'un État puisse être engagée par un État tiers pour les activités offensives menées par des acteurs privés sur son territoire[27].

L'encadrement de l'industrie cyber offensive, pour lequel il ne peut y avoir de solution miracle, est particulièrement difficile à appréhender. À l'instar des propositions du Cyber Statecraft Initiative, il est nécessaire pour les États de multiplier les actions contribuant à limiter les effets délétères de cette industrie, dont aucun pays ne souhaite se passer. En effet, un État qui limiterait ses achats auprès de cette dernière serait désavantagé vis-à-vis de ses adversaires, aussi bien dans ses capacités offensives que défensives. Pour tenir compte de la réalité de la course à l'armement cyber, il apparaît donc souhaitable afin de limiter la prolifération, tout en restant de la course, de concevoir une stratégie commune de régulation avec un nombre restreint de partenaires.

[26] Voir le rapport de l'OCDE « Encouraging Vulnerability Treatment » (Février 2021).
[27] Voir les travaux de Karine Bannelier-Christakis, créatrice du concept de cyber-diligence.

FOCUS INNOVATION

Freemindtronic : Une barrière physique pour permettre aux utilisateurs de reprendre le contrôle de leurs données

Entretien avec Jacques Gascuel (co-fondateur).

Présentation

Jacques Gascuel a créé l'entreprise Freemindtronic en 2010. Précédemment à la tête d'une entreprise d'informatique en milieu rural, ce diplômé en électrotechnique et en droit, spécialiste de la maintenance industrielle, a mesuré l'impact du piratage informatique suite à la compromission des systèmes de l'un de ses clients éleveurs, qui a grandement affecté la production de ce dernier. Jacques Gascuel, après la résolution de cet incident, s'est tourné vers la sûreté et la sécurité cyber en fondant Freemindtronic (« la liberté de créer en électronique »). La société, d'abord basée dans le Comminges, s'est implantée en Andorre à partir de 2016.

Freemindtronic assure la maîtrise intégrale de ses innovations technologiques – donc de la phase de conception à l'industrialisation des solutions – et ne sous-traite ainsi aucune étape du cycle de développement. Considérant le « tout numérique » comme une menace, l'entreprise est guidée dans ses activités par deux objectifs : mettre l'humain au cœur de la sécurité et préserver au maximum l'anonymat des utilisateurs.

Solution

Toutes les solutions de Freemindtronic ont en dénominateur commun un nom commençant par « Evi » (du mot anglais « evidence ») avec entre autres EviKey, EviDisk, EviLock, EviToken et EviCard. Un tel choix fait référence aux preuves juridique et matérielle produites par une boîte noire infalsifiable, invention brevetée de Jacques Gascuel sur la sûreté des appareils électriques avec traçabilité. La dernière solution « EviCypher », fruit de quatre années de R&D, est prête depuis mars 2021 et vise à redonner aux utilisateurs la maîtrise de leurs données en général, ainsi qu'à lutter contre la cybercriminalité et l'espionnage des entreprises en particulier.

EviCypher est une solution sans contact de chiffrement de bout-en-bout depuis un dispositif NFC[28] (Near-field communication). Elle repose sur une application et un dispositif physique NFC sous forme de carte. Cette dernière est capable de gérer et de stocker aussi bien des mots de passes « compliqués », que des algorithmes de chiffrement symétrique (jusqu'à deux cents clés AES 256) et asymétrique (quatre clés RSA 2048 ou deux clés RSA 4096). Cette carte « *greentech* » a été conçue à partir de matériaux durables (fibre de verre sans halogène et n'émettant ni gaz toxique ni résidu dangereux), qui lui assurent une durée de vie de plus d'une quarantaine d'années et un fonctionnement en environnements extrêmes. Dénuée de batterie, elle

[28] La technologie NFC est connue pour être utilisée dans le cadre des paiements sans contact et des cartes de transport.

récupère de l'énergie via le signal NFC émis par un terminal NFC (*energy harvesting*). Ce dispositif, qui ne s'active qu'à la demande, est par défaut un produit passif dit « air gap », qui consiste à isoler physiquement de tout réseau le système à sécuriser.

L'application permet de son côté de paramétrer les méthodes de chiffrement de la carte EviCypher et d'y associer jusqu'à douze « critères de confiance » (dont la géolocalisation, mot de passe, empreinte digitale, codes EAN et QR…). Ces derniers, qui devront être respectés par tout utilisateur désireux de déchiffrer le message, permettent alors de bloquer toutes tentatives d'accès frauduleux en cas de vol de la carte entre autres.

Le chiffrement d'un contenu s'effectue ainsi en passant la carte EviCypher au niveau du récepteur NFC d'un terminal doté de l'application (ordinateur, *smartphone* NFC Android, etc.). Le destinataire, à la réception du message, doit répéter le geste afin que sa carte procède au déchiffrement. Il doit se trouver physiquement dans la zone géographique prédéfinie (rayon au choix de 1 à 2 500 km²) et valider les critères de confiance établis par l'émetteur. En d'autres termes, ce système, qui n'est connecté ni à un serveur ni à une base de données, chiffre un contenu avant même sa diffusion en ligne ou son stockage sur les serveurs d'une messagerie. Dans ce dernier cas, les chiffrement AES256 et RSA 2048 ou 4096 sont suffisamment robustes contre les tentatives tierces de déchiffrement.

Applications

EviCypher se veut être une solution intraçable qui préserve l'anonymat de ses utilisateurs. Destinée à la base à des services critiques de l'État (gouvernement, armées, ambassades, etc.) et à des entreprises sensibles, la solution a finalement été déclinée dans une version « grand public », suite aux récentes cyberattaques contre des hôpitaux au début de l'année. Ces différentes intrusions ont en effet convaincu Freemindtronic de profiter de la sortie de son outil EviCypher pour sensibiliser sur le besoin crucial de protéger les données.

EviCypher réduit en tout lieu la surface d'exposition aux attaques et s'applique à de nombreuses situations :

- La solution permet de contrer les tentatives d'espionnage et d'usurpation d'identité reposant sur des attaques par *ransomware* ou *phishing* visant à obtenir des données confidentielles (attaque au président). Cela est rendu possible par le système d'authentification fondé sur de multiples critères de confiance ;
- Dans le domaine militaire, EviCypher peut établir, via son critère de confiance de géolocalisation, une communication sécurisée entre le commandement en France et le théâtre d'opérations à l'étranger ;
- Cette technologie, embarquant un gestionnaire automatisé de flotte intelligent, constitue aussi un moyen pour les RSSI de gérer à la fois les multi-postes et les terminaux à antenne NFC servant d'interface.

Pour aller plus loin, Freemindtronic prévoit, outre la création d'une extension pour applications afin d'être plus « volatile » vis-à-vis de son application *ad hoc*, d'intégrer la gestion d'autres systèmes de chiffrement. Parmi lesquels, Open PGP, clés ECC, SSH et AWS. Les utilisateurs seront également en mesure de sélectionner le type de chiffrement en fonction de leurs usages. À ce jour, la nouvelle extension pour la solution Thunderbird a été développée pour chiffrer en AES256 les boîtes de messagerie utilisant notamment le protocole IMAP.

Actualité

Après avoir recruté un directeur R&D, Freemindtronic, qui s'appuie depuis sa création sur un personnel de cinq profils techniques (ingénieurs en cybersécurité, électronique, intelligence artificielle, systèmes embarqués, expert forensic), initie aujourd'hui une phase de recrutement qui confirme sa montée en puissance.

L'entreprise a par ailleurs reçu plusieurs distinctions grâce à EviCypher. Elle a notamment décroché en mars 2021 la médaille d'or de la catégorie C du Salon international des inventions de Genève[29]. Freemindtronic a plus récemment remporté au mois de mai trois prix lors de la dernière édition des Global InfoSec Awards, dans les catégories « sécurité cryptographique », « gestion des secrets » et « Hardware Password Manager ».

CALENDRIER

Quels défis pour la cyberdéfense de demain ? (06, 07 et 08 juillet 2021)

Organisé par CEIS/Avisa Partners au profit du Commandement de la cyberdéfense du ministère des Armées, le prochain forum « Cyberdéfense & Stratégie » se tiendra les 6, 7 et 8 juillet. Il aura pour thème « Quels défis pour la cyberdéfense de demain ? » et se déclinera en trois webinars indépendants de deux heures :

Atelier 1 – Mardi 6 juillet de 09h00 à 11h00
Le défi humain : quel modèle pour l'armée de cyber-combattants ?

Le constat n'est pas nouveau : depuis plusieurs années, la filière cybersécurité fait face à une pénurie de ressources et de talents, avec environ 5 000 postes à pourvoir en France dans ce secteur en 2021. La cyberdéfense n'échappe pas à cette situation : les Armées font face dans le cyberespace à des menaces toujours plus nombreuses et plus diverses qui nécessitent de nouvelles compétences. Mais comment déterminer quels profils permettront de répondre à ces nouvelles menaces ? Entre offres de formation insuffisantes et manque de vocations, où et comment recruter ces profils ? Comment valoriser la filière et les métiers de la cyberdéfense ? Comment les rendre plus attractifs et plus accessibles ? Et une fois recrutés, comment fidéliser les cyber-combattants et mettre en place des parcours et des méthodes de formation permettant de continuer à faire évoluer leurs compétences pour répondre à des besoins changeants ? Comment obtenir ces cyber-combattants opérant dans un cyberespace toujours plus conflictuel ?

Atelier 2 – Mercredi 7 juillet de 09h00 à 11h00
Le défi capacitaire : quels enjeux et perspectives ?

Opérant dans un cyberespace et un environnement informationnel en constante et rapide évolution, marqués par une numérisation tous azimuts, les Armées voient leurs missions évoluer et doivent adapter en conséquence les moyens humains et techniques nécessaires pour les remplir. Ces changements technologiques remettent en cause certains dispositifs de défense existants et font naître de nouveaux besoins capacitaires, mais représentent aussi de véritables opportunités. Comment anticiper ces évolutions afin de s'y préparer ? À quoi ressemblera le cyberespace dans lequel opèreront les armées en 2035 ? La transformation numérique aura-t-elle été au rendez-vous ? Quels nouveaux besoins techniques et capacitaires aura-t-elle faite naître ? Et quels sont les « *game changers* » technologiques qui permettront alors aux Armées de

[29] Catégorie regroupant les innovations informatique, logicielle, électronique, électricité ou méthodes de communication.

conserver la supériorité opérationnelle dans le cyberespace ? Quelles sont les innovations dans lesquelles elles doivent, dès aujourd'hui, investir pour en garder la maîtrise ?

Atelier 3 – Jeudi 8 juillet de 09h00 à 11h00
Le défi industriel : comment structurer un écosystème performant ?

Les dernières crises cyber ont montré qu'elles pouvaient avoir des effets systémiques, potentiellement susceptibles de mettre en cause la résilience même de la Nation. Cette menace grandissante rappelle l'urgence de se doter de moyens fiables et d'outils souverains pour y répondre, et ce en facilitant la montée en puissance des acteurs nationaux et européens du numérique et de la cybersécurité. Cette démarche nécessite d'abord d'identifier les briques technologiques sur lesquelles doivent se concentrer les efforts, puis de soutenir et d'accompagner l'innovation, de fédérer des acteurs de natures différentes (privés, publics, académiques et recherche, société civile) et d'animer cet écosystème en facilitant entre eux les synergies. Les initiatives en ce sens se multiplient, tant dans la sphère civile (mission d'information « Bâtir et promouvoir une souveraineté numérique nationale et européenne » de l'Assemblée nationale, Accélération de la stratégie nationale de cybersécurité, Campus Cyber), que de la défense (Cyberdéfense Factory de Rennes…). Quelles perspectives pour ces initiatives ? Quelle politique industrielle pour la cyberdéfense ?

La liste des intervenants sera disponible dans les prochains jours.

ACTUALITÉ

Point d'étape sur la feuille de route de l'IA de défense

La ministre des Armées s'est rendue le 21 mai à la base aérienne 110 de Creil. Cette visite fût l'occasion de dresser un premier bilan quant à l'avancement de la feuille de route, initiée en 2019, visant à placer l'intelligence artificielle (IA) au service de la défense. Pour rappel, cette stratégie poursuit un objectif ambitieux : garantir le plus haut niveau de protection des Français demain en développant une IA militaire de confiance, fiable, performante et robuste, dans tous les segments de la défense.

Dans son discours, Florence Parly a commencé par relever le caractère « redoutable » de l'IA : sa capacité à s'immiscer dans tous les systèmes d'armes permet de mobiliser ces derniers avec cent fois plus d'efficacité, en plus d'en décupler la force de frappe. L'IA, lorsqu'elle sera maîtrisée dans le cadre des programmes entre autres Scorpion ou SCAF (système de combat aérien du futur), sous-tendra dès lors le combat collaboratif, qui consiste à coordonner l'emploi des systèmes, tout en optimisant leur déploiement sur une zone définie.

La ministre a par ailleurs rappelé que l'IA ne contribuait pas seulement aux opérations militaires, puisqu'elle bénéficie aussi aux métiers administratifs du ministère, tels que les finances et les ressources humaines.

Suite au lancement de sa stratégie il y a deux ans, le ministère des Armées s'est doté d'un écosystème dédié à l'IA de défense, qui comprend des acteurs académiques et institutionnels, ainsi que des PME. Il a également publié plusieurs guides de recommandations pour la spécification et la qualification des systèmes intégrant de l'IA, dont un à destination des industriels.

L'un des défis majeurs concerne le recrutement : depuis 2019, le ministère des Armées a embauché soixante-treize jeunes spécialistes en IA, un nombre qui sera porté à deux cents d'ici 2023. Florence Parly a souligné

à cet égard le rôle de la loi de programmation militaire, qui consacre plus d'un demi-milliard d'euros au développement de l'IA sur la période 2019-2025, avec une moyenne de 100 millions d'euros par an.

Sur le traitement massif des données, associé au « nouveau nerf de la guerre », la ministre des Armées a évoqué le programme national Artémis, solution souveraine adaptée aux besoins de la défense. Ce projet, qui réunira puissance de calcul, sécurité et modularité, offrira la « boîte à outils » indispensable à une partie des développements à base d'IA des armées. Après des premiers résultats encourageants sur plusieurs applications (suivi de la santé des militaires, gestion de parcs de matériels militaires, surveillance maritime…), le programme Artémis s'apprête à entrer en phrase d'industrialisation.

Enfin, Florence Parly a rappelé l'opposition de la France aux « robots-tueurs », dans le cadre des systèmes d'armes létaux autonomes (SALA). La ministre a assuré que la France continuera de porter la voix, sur ce sujet, du ministère des Armées au sein de la Convention sur certaines armes classiques (CCAC) à Genève.

Pour consulter le discours de la ministre des Armées, cliquez ici.

La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose des 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 les organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

À ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique (OMC)**, qui s'inscrit dans le contrat-cadre n°2018-02. 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 | 75015 Paris

CEIS
Tour Montparnasse | 33 avenue du Maine | 75015 Paris
E-mail : omc@ceis.eu