OBSERVATOIRE DU MONDE CYBERNÉTIQUE

JUIN 2018

SOMMAIRE

- La réalisation de cette newsletter a été confiée à CEIS par la DGRIS dans le cadre du marché BC33- 2015.1050129916. Les opinions développées dans cette étude n'engagent que leurs auteurs et ne reflètent pas nécessairement la position du Ministère des Armées.
- Si vous souhaitez recevoir cette newsletter par email, merci de contacter **omc@ceis.eu**

ACTUALITÉ

Le Cyber Defence Pledge

La France accueillait le 15 mai dernier à l'École Militaire le premier colloque « Cyber Defence Pledge » de l'OTAN, un événement d'ampleur internationale ouvert aux 29 nations membres de l'organisation. La France devient ainsi le premier pays à organiser un colloque dans le cadre de cet accord.

Ouvert par les allocutions de Mme. Florence Parly, Ministre des Armées, et M. Jens Stoltenberg, Secrétaire général de l'OTAN, et clôturé par un discours de Mme. Claire Landais, Secrétaire générale de la Défense et de la Sécurité nationale française, l'événement a également réuni des représentants de haut niveau de l'organisation et des États Membres, et notamment le Commandant de la Cyberdéfence français, le Général de division Olivier Bonnet de Paillerets, et les directeurs des agences nationales de la cybersécurité française, tchèque et estonienne, Guillaume Poupard, Vladimir Petera et Uku Särekanno.

Le « Cyber Defence pledge »

Le « Cyber Defence Pledge » traduit l'engagement collectif des pays de l'OTAN en faveur du renforcement du dispositif de cyberdéfense de l'Alliance et de sa résilience globale. L'objectif à terme est de renforcer les liens et la coopération entre les États membres de l'OTAN en matière de défense dans le cyberespace, et de permettre une montée en capacités et en compétences des alliés en la matière.

Il prévoit notamment :

- Le développement des moyens de défense nationaux des infrastructures et des réseaux,
- La montée en capacité des États membres ;
- L'amélioration du partage de connaissances et d'informations ;
- Le renforcement des dispositifs de formation et d'entraînement en cyberdéfense

La résilience est ainsi au cœur du Cyber Defense Pledge.

ENJEUX

Cet événement a permis de présenter l'action menée par les alliés dans le cadre du « Cyber Defence Pledge », de rappeler leur engagement en faveur de la cyberdéfense, et d'insister sur le fait que la cybersécurité est aujourd'hui un défi quotidien qui ne peut être relevé que par une action continue et collective.

Le colloque a également été l'occasion pour les décideurs et experts des États membres de l'OTAN d'échanger sur ce domaine en perpétuelle évolution, et d'aborder des thématiques et préoccupations communes.

QUELQUES IDÉES CLÉS

- **Florence Parly, Ministre des Armées :** L'OTAN est et reste l'un des piliers de la défense, y compris en matière cyber, et la coopération est majeure en matière de cybersécurité, notamment entre l'OTAN et l'UE.
- **Jens Stoltenberg, Secrétaire Général de l'OTAN :** Les cyberattaques doivent être considérées comme des actes de guerres : l'arme n'est qu'une ligne de code mais elle peut provoquer des dégâts mortels.
- **Général de division Olivier Bonnet de Paillerets, Commandant de la cyberdéfense française :** Seule une compréhension collective des menaces peut permettre une réponse opérationnelle.
- **Guillaume Poupard, Directeur Général de l'ANSSI :** La sécurité n'est pas statique : Elle nécessite des systèmes raisonnablement protégés mais surtout une grande agilité et une capacité à anticiper.
- **Vladimir Petera, DG Adjoint, Agence nationale tchèque de cybersécurité (NUKIB) :** les exercices d'entraînement collectifs tels Lockshields sont indispensables pour faire émerger des besoins et appréhender les menaces actuelles.

ANALYSES

Intelligence artificielle : un « game changer » en matière de Cyberdéfense

L'Homme est incapable de répondre seul aux attaques informatiques. Tel est le constat partagé par les professionnels de la cybersécurité. Plusieurs raisons : le volume des attaques, leurs mutations permanentes, la vitesse de réaction qu'elles exigent, mais aussi le manque de spécialistes sur le marché. Déjà largement utilisée en matière de lutte anti-fraude, l'intelligence artificielle apparaît donc de plus en plus comme un « game changer » majeur en matière de cybersécurité, en particulier dans la lutte informatique défensive. Le récent rapport Villani cite d'ailleurs la défense comme l'un des 4 débouchés stratégiques en la matière. A l'inverse, la généralisation de l'intelligence artificielle, y compris dans des systèmes d'armes totalement automatisés, soulèvera demain de nombreux problèmes de cybersécurité, la technologie pouvant être utilisée à des fins malveillantes.

QUEL RÔLE POUR L'IA EN MATIÈRE DE CYBERSÉCURITÉ ?

L'Intelligence artificielle est devenue en quelques années un *buzzword* marketing chez les éditeurs de cybersécurité. Avec succès **puisqu'un tiers des entreprises disent aujourd'hui utiliser des solutions de sécurité basée sur de l'IA**[1]. Ce chiffre ne peut cependant pas masquer des réalités très diverses, certaines solutions s'appuyant davantage sur des moteurs de règles sophistiqués que sur de réelles fonctionnalités d'IA. Pour parler d'intelligence artificielle, il faut en effet qu'il y ait 1) une capacité de perception de l'environnement au moyen d'un apprentissage supervisé ou non, 2) une capacité d'analyse et de résolution de problème, 3) une capacité de proposition d'action, voire de décision autonome.

Au plan théorique, **les apports de l'IA en matière de cybersécurité sont donc nombreux, qu'il s'agisse de prévention, d'anticipation, de détection ou de réaction**. Dans la pratique, la détection de vulnérabilités ou de menaces internes ou externes apparaît aujourd'hui l'un des usages les plus matures. Et il y a urgence tant les systèmes de détection actuels basés sur des signatures montrent leurs limites : nombre élevé de faux positifs, incapacité à s'adapter aux dernières menaces, notamment aux APT, lourdeur des bases de signature, ce qui a un impact sur les performances. Différents acteurs comme iTrust[2] en France (solution Reveelium), Darktrace[3] au Royaume-Uni ou Cylance[4] (société américaine venant de s'implanter en France[5]) se sont ainsi spécialisés dans le développement de solutions à base d'intelligence artificielle pour

[1] *http://www.esg-global.com/blog/artificial-intelligence-and-cybersecurity-the-real-deal*
[2] *https://www.itrust.fr/*
[3] *https://www.darktrace.fr*
[4] *https://www.cylance.com*
[5] *http://www.globalsecuritymag.fr/Florent-Embarek-Cylance-l-IA,20180605,79022.html*

la détection d'anomalies et l'analyse comportementale. De leur côté, la plupart des éditeurs de solutions de sécurité endpoint et réseau (Symantec, Sophos, F-secure, SentinelOne, Fortinet, Palo Alto Networks...) ont intégré des briques d'intelligence artificielle plus ou moins évoluées dans leurs solutions, parfois en rachetant des petits acteurs spécialisés (comme Invicea racheté par Sophos ou RedOwl par Forcepoint en 2017).

Après la détection, la réponse à incident est aussi largement touchée par le mouvement. Il s'agit en effet de démultiplier l'efficacité des SOC et CSIRT en donnant toujours plus d'intelligence aux SIEM. Splunk[6] a ainsi annoncé il y a quelques jours le rachat de Phantom Cyber[7], un spécialiste de l'automatisation et de l'orchestration de la réponse à incident. De son côté, IBM a intégré son Watson dans Qradar et propose maintenant une « sécurité cognitive »[8] permettant d'exploiter de façon combinée données structurées (les logs par exemple) et non structurées (avis d'expert, réseaux sociaux...).

Ajoutons également à ces différents usages défensifs la possibilité d'utiliser l'IA pour l'authentification des utilisateurs à partir d'une empreinte constituée grâce à l'analyse de leur propre comportement (cf. le programme Active Authentification de la DARPA[9]).

PRINCIPAUX USAGES DE L'INTELLIGENCE ARTIFICIELLE EN CYBERSÉCURITÉ

	USAGE	DESCRIPTION	MATURITÉ
PRÉVENTION	Sécurité du code	Assistance à la programmation, correction automatique des bugs	●●○○
	Cyber-résilience	Systèmes auto-adaptatifs capables de se reconfigurer automatiquement face à des attaques	●○○○
ANTICIPATION	Cyber Threat Intelligence	Prévention des fuites de données, analyse et caractérisation des attaques passées, surveillance des attaquants potentiels	●●○○
	Cybersécurité cognitive	Agrégation et traitement d'un ensemble de données non structurées (écrits des experts, réseaux sociaux...) et structurées (logs) afin d'assister les équipes sécurité	●○○○

[6] *https://www.splunk.com/fr_fr*

[7] *https://www.phantom.us/*

[8] *https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEW03134FRFR*

[9] *https://www.darpa.mil/program/active-authentication*

DÉTECTION	Détection de vulnérabilités	Tests d'intrusion automatisés, simulation d'attaques, détection de failles dans un logiciel	●●●○
	Détection de menaces internes ou externes	Détection d'anomalies à partir d'une analyse comportementale, lutte anti-APT, analyse de logs, lutte anti-fraude	●●●○
RÉACTION	Réponse à incident	Automatisation et orchestration de la réponse à incident (analyse des incidents, application de contre-mesures, filtrage de contenus, collecte de preuves...)	●●○○
	Attribution des attaques	Identification des auteurs d'une attaque informatique	●○○○

Au-delà des couches techniques du cyberespace, l'intelligence artificielle peut enfin jouer un rôle ambivalent sur la couche sémantique puisqu'elle permet à la fois de fabriquer de façon industrielle des *fake news*, à l'image du faux discours de Barack Obama produit par l'Université de Washington [10], tout en facilitant leur détection. La DARPA vient ainsi de lancer un programme de *media forensic* permettant de certifier des informations [11].

L'intelligence artificielle va donc progressivement imprégner l'ensemble des technologies et des processus de cybersécurité. En témoigne par exemple le Cyber Grand Challenge, organisé par la DARPA lors de la DEFCON 2016, qui a vu différentes IA s'affronter pour détecter et corriger de failles de façon totalement automatisée [12].

Si l'utilisation de la technologie à des fins de cyberdéfense apparaît donc prometteuse, il faut également **en mesurer les limites, qui ne sont pas tant technologiques qu'humaines (comprendre l'IA) et psychologiques (accepter l'IA)**. Sommes-nous prêts à laisser des machines prendre certaines décisions qui peuvent être lourdes de conséquences ? Si la détection de comportements anormaux ou l'analyse de code ne paraissent pas poser de problèmes, le filtrage de contenus, le blocage d'une adresse IP et *a fortiori* l'attribution d'une attaque sont des décisions « engageantes ». De façon générale, **l'intelligence artificielle ne saurait donc remplacer l'intelligence humaine. Sa vocation est surtout de l'augmenter**. Cela suppose que la technologie ne soit pas une boîte noire : l'utilisateur doit pouvoir suivre les différentes étapes du raisonnement et comprendre la décision. C'est la condition *sine qua non* de la confiance qu'il accordera ou non au système. Le risque de voir des batailles d'IA cherchant à s'affaiblir mutuellement et à leurrer les machines adverses est en effet bien réel. Lors de la DEFCON 2017, des chercheurs ont ainsi démontré qu'il était possible d'utiliser le *framework* Open AI pour rendre des malwares totalement indétectables [13].

---

[10] *https://www.sciencesetavenir.fr/high-tech/le-vrai-obama-prononce-un-faux-discours-un-trucage-criant-de-verite_114855*

[11] *https://www.darpa.mil/program/media-forensics*

[12] *https://en.wikipedia.org/wiki/2016_Cyber_Grand_Challenge*

[13] *https://www.silicon.fr/machine-learning-creer-malwares-furtifs-181669.html/?inf_by=5a1c1c8b671db8013f8b4a8c*

QUELLE CYBERSÉCURITÉ POUR L'IA ?

La relation entre IA et cybersécurité possède donc une deuxième face, négative celle-ci, liée aux utilisations malveillantes de la technologie qui peut être victime de détournements et d'attaques. Il peut tout d'abord s'agir **d'attaques par empoisonnement** qui consistent à injecter, pendant la phase d'apprentissage, des données biaisées ou de mauvaise qualité. Tay, le *chatbot* (ou robot conversationnel) de Microsoft en a été la victime [14]... Autre méthode : les **attaques par inférence** qui consistent à pousser les IA à révéler leur fonctionnement interne (seuils, règles...) en jouant différents scénarios. Cette méthode est déjà largement utilisée par les cybercriminels pour leurrer les systèmes anti-fraude. Il est enfin possible de **leurrer les IA** en modifiant légèrement leur environnement, comme l'ont récemment démontré des chercheurs de Google en matière de reconnaissance d'image [15]. Des fragilités qui ont fait dire à Adi Shamir, co-inventeur de l'algorithme RSA qu'il ne fallait surtout pas demander à une intelligence artificielle comment sauver internet. Le risque serait en effet grand qu'elle recommande d'abord de tuer le réseau pour mieux le sauver...

Au plan militaire, ces risques sont d'autant plus inquiétants que l'IA sera demain omniprésente dans les systèmes d'armes, que certains pays imaginent en large partie autonomes dans le futur proche. Si les Etats-Unis conçoivent d'abord l'IA comme un moyen d'augmentation des performances humaines, tant sur le plan physique que cognitif, la Russie travaille ainsi à l'automatisation complète de certaines plateformes. **Objectif : robotiser 30% des équipements militaires d'ici 2025 afin d'exclure progressivement l'Homme de la zone de confrontation immédiate**. Dans cette compétition mondiale, la Chine n'est pas en reste et cherche aujourd'hui à utiliser les technologies civiles comme un levier pour ses capacités militaires avec pour ambition de parvenir au leadership mondial en 2030.

L'intelligence artificielle est donc devenue un enjeu de souveraineté majeure. Face au volontarisme de ses compétiteurs russes, américains et chinois, la France a une carte à jouer, tant au plan scientifique qu'en termes de données disponibles et de débouchés industriels. Il s'agit donc de **créer les conditions de la sécurité et de la confiance dans l'intelligence artificielle**. En premier lieu, **en investissant dans la sécurité de l'intelligence artificielle**. C'est ce que préconise le rapport Villani qui propose de confier une mission à ce sujet à l'ANSSI. En deuxième lieu, **en définissant un cadre éthique**. Comment, par exemple, concilier le droit à l'oubli et la protection des données personnelles face à des systèmes qui engloutissent et mémorisent des milliards de données ? Enfin, en troisième lieu, **en concentrant les efforts sur quelques secteurs où la France est en pointe. La cybersécurité en fait assurément partie**.

---

[14] *https://www.lemonde.fr/pixels/article/2016/03/24/a-peine-lancee-une-intelligence-artificielle-de-microsoft-derape-sur-twitter_4889661_4408996.html*

[15] *http://www.ladn.eu/tech-a-suivre/hello-open-world/des-pirates-ont-reussi-a-hacker-lia-via-les-attaques-adversarial/*

Quelle stratégie pour la France ?

A l'occasion de la conférence AI for Humanity au collège de France, le Président de la République a exposé les ambitions et la stratégie de la France en matière d'IA [16].

4 priorités ont été définies :

- Conforter l'écosystème de l'IA pour attirer les meilleurs talents ;
- Développer une politique d'ouverture des données ;
- Créer un cadre réglementaire et financier favorable à l'émergence de champions de l'IA ;
- Engager une réflexion sur la régulation et l'éthique de l'IA.

Hyperconnectivité : quelles conséquences pour les opérations militaires ?

Le concept de network-centric warfare n'est pas nouveau. Mais son application opérationnelle a pendant longtemps été bridée par les limites technologiques. Cette barrière a désormais volé en éclat : nous sommes rentrés dans l'ère de l'hyperconnectivité. Une rupture qui entraine de nombreuses conséquences sur les opérations militaires et les capacités qui permettent de les mener, en particulier en matière de cyberdéfense.

UNE CONVERGENCE DE TECHNOLOGIES ET D'USAGES

L'hyperconnectivité résulte d'une convergence de nombreux technologies et usages. Elle peut se définir ainsi : des personnes et des objets connectés en permanence, quasiment depuis partout, via des équipements facilement accessibles et interactifs,

[16] *https://www.gouvernement.fr/argumentaire/intelligence-artificielle-faire-de-la-france-un-leader*

avec pour effet une croissance exponentielle des données générées, stockées et exploitées, qu'il s'agisse d'usages privés ou professionnels.

LES ATTRIBUTS DE L'HYPERCONNECTIVITÉ

ATTRIBUTS	SOUS-JACENTS TECHNOLOGIQUES	QUELQUES TENDANCES
Le « tout » connecté [17]	Objets connectés, « wearables », machine-to-machine, IPV6	Miniaturisation et autonomie énergétique des objets
En permanence	Réseaux locaux sans fil (Wifi, Bluetooth), réseaux de télécommunication sans fil (4 ou 5G, satellite), réseaux de télécommunication fixe comme la fibre ou le VDSL, protocoles radio low power-long range (LoRa, Sigfox, LTE)	Augmentation des débits et des latences
Depuis partout		Amélioration de la connectivité, y compris dans des zones non couvertes jusque-là, arrivée prochaine de la 5G
Des équipements faciles d'accès et interactifs	Smartphones, tablettes, objets connectés	Progrès de la reconnaissance vocale, des interfaces neuronales directes (après les interfaces en ligne de commande, puis graphiques).
Une croissance exponentielle des données générées	Capteurs (GPS, corporels, image, NEMS…) [18]	Miniaturisation et amélioration des performances des capteurs (intelligence embarquée)
Des données de plus en plus enregistrées en local ou à distance	Data lakes, big data, cloud privé, public ou hybride	Croissance des capacités de stockage, généralisation du cloud computing, avènement du edge computing ?

Au plan militaire, cette hyperconnectivité permet désormais **l'interconnexion de l'ensemble des plateformes de combat** : satellites, avions, drones, véhicules, radars, soldats… Chacune est ainsi en mesure de capter, diffuser, échanger et

[17] *Cf. la notion d'Internet of Everything popularisée par Cisco pour désigner un niveau de connexion généralisé allant au-delà de l'IoT.*

[18] *Un véhicule compte aujourd'hui entre 60 et 100 capteurs. Source : http://www.servicesmobiles.fr/mwc17-les-capteurs-nerf-de-la-guerre-de-tous-les-objets-connectes-35799/*

exploiter de l'information. A l'instar du Griffon, le nouveau véhicule blindé multi-rôle (VBMR), premier élément du programme Scorpion de modernisation de l'Armée de terre, ou du système FELIN (Fantassin à équipements et liaisons intégrées). Certains systèmes d'armes deviennent ainsi de véritables **« centrales informationnelles »** comme le F35 américain, avion dit « de 5ème génération ». « *Branché sur un cloud lui fournissant en temps réel des informations multidomaines sur son environnement «ami» et «ennemi» »*, cet avion est *« une sorte d'AWACS en réduction »*, souligne Olivier Zajec [19]. Au cœur du dispositif, agissant comme un véritable « ciment » : un système d'information unifié, à l'image du Système d'information du combat (SICS) qui mettra demain en réseau tous les systèmes produisant un effet tactique sur le terrain.

QUELS DÉFIS ?

Si l'hyperconnectivité marque une véritable rupture stratégique en permettant l'avènement du combat collaboratif et le renforcement de l'approche multidomaines [20], elle soulève également de nombreux défis parmi lesquels :

- **Le défi du big data.** L'objectif est d'exploiter au mieux la masse d'information qui croit de façon exponentielle pour éviter « l'obésité informationnelle ». On estime ainsi que l'ARGUS-IS, module d'observation constitué de 368 capteurs mis au point par l'armée américaine collecte 6 millions de Go de données par jour [21], alors qu'un drone peut générer au cours d'une mission de 14 heures environ 70 000 Go de données ;

- **Le défi de la résilience.** Les systèmes doivent garantir la disponibilité des données dans des conditions parfois dégradées ou en tenant compte de contraintes d'accès aux réseaux particulières. « Les unités doivent en effet pouvoir travailler aussi bien «connectées» que «déconnectées» ou avec des niveaux de connexion (serveurs de réplication asynchrone par exemple) plus ou moins localisés. Cela doit permettre d'éviter tant les pertes de capacités opérationnelles que les dysfonctionnements liés à la latence des réseaux » [22] ;

- **Le défi du « mode dégradé ».** Celui-ci peut être imposé par l'adversaire mais aussi choisi pour créer une rupture de symétrie avec l'adversaire, ce qu'Olivier Zajec nomme la « techno-régression compétitive ». Avec l'hyperconnectivité, le risque de déni de service est en effet permanent, compte tenu de l'augmentation de la surface d'exposition au risque (objets connectés, dépendance aux liaisons de donnée pour l'accès au cloud...) et des vulnérabilités potentielles des systèmes. Le brouillage des signaux GPS est ainsi devenu monnaie courante. Un risque aggravé par les cyberattaques, voire l'utilisation demain d'armes à énergie dirigée (AED). *« Près de 70% des systèmes de combat majeurs de l'US Army dépendent de*

---

[19] *Hyperconnectivité et souveraineté : les nouveaux paradoxes opérationnels de la puissance aérienne, https://www.defense24.news/2018/02/21/hyperconnectivite-souverainete-nouveaux-paradoxes-operationnels-de-puissance-aerienne/*

[20] *Cf. Grégory Boutherin, Un nouveau phénomène conceptuel made in USA : le combat multidomaine, https://www.areion24.news/2017/01/09/nouveau-phenomene-conceptuel-made-in-usa-combat-multidomaine/*

[21] *https://leaksource.wordpress.com/2013/01/29/darpas-1-8-gigapixel-argus-is-worlds-highest-resolution-surveillance-system/*

[22] *https://ceis.eu/fr/note-strategique-emploi-du-cloud-dans-les-armees-premiere-approche-des-concepts-et-contraintes/*

signaux qui sont émis depuis l'espace », constate le colonel Richard Zellmann de l'US Army[23]. Face à des pays comme la Russie, qui a montré en Ukraine l'efficacité de ses moyens de guerre électronique, ou la Chine, pays qui développent tout deux des capacités anti-satellite, les Etats-Unis cherchent ainsi à concevoir des plateformes de combat fonctionnant sans GPS[24] ;

- **Le défi de la supériorité informationnelle.** Le leadership des armées modernes est fragilisé par la militarisation de l'information (*information weaponization*) et l'hyperconnectivité. C'est ce que constate une récente étude publiée par l'US Army War College[25] qui fait montre d'un techno-scepticisme assez inhabituel outre-Atlantique : *« l'utilisation généralisée des équipements portables capables d'enregistrer en haute définition pour une transmission immédiate du son, de l'image et du texte transforme la façon dont le monde s'informe mais également la capacité des armées et services de renseignement à opérer avec une sécurité opérationnelle minimale. En outre, les individus, les groupes et les Etats sont maintenant en mesure d'accéder à des images et à des informations sensibles de source ouverte qui étaient autrefois étroitement contrôlées par les gouvernements. En fin de compte, les chefs militaires devraient supposer que toutes les activités liées à la défense, depuis les mouvements tactiques mineurs jusqu'aux opérations militaires majeures se dérouleront désormais de façon totalement ouverte ».*

QUELLES CONSÉQUENCES AU PLAN CAPACITAIRE ?

Ces différents défis exigent une réponse capacitaire intégrant notamment les priorités suivantes :

- **L'acquisition de nouvelles capacités spatiales de télécommunication**. Avec deux objectifs, selon les députés Olivier Becht et Thomas Gassilloud[26] : au plan quantitatif, *« fournir aux armées des débits de données répondant à leurs besoins croissants »* et au plan qualitatif *« sécuriser les moyens spatiaux de captation et de transmission d'information contre les risques de captation des informations ou de compromission de leur intégrité, voire de destruction physique des satellites, qu'elle soit accidentelle, liée aux débris spatiaux, ou délibérée, dans un contexte où l'espace devient, aux termes du général Jean-Pascal Breton, « un champ de confrontation à part entière »* ;

- **Le développement d'un « Combat Cloud »** (aussi appelé « cloud tactique » ou « cloud de théâtre ») **transverse aux différents domaines**. Cette infrastructure doit répartir les données et leur traitement, et donc la puissance de calcul, entre les différents niveaux pour permettre à chaque utilisateur de fonctionner de façon autonome si nécessaire. Un chantier qui pose inévitablement la question de notre autonomie stratégique compte tenu de la très nette domination américaine et chinoise en matière de solutions technologiques mais aussi d'offres de cloud « as a service » ;

- **L'adoption d'une politique d'innovation volontariste en matière d'intelligence artificielle.** *« La défense recèle en effet une grande variété d'applications potentielles : reconnaissance automatique d'images, guerre électronique, combat*

---

[23] *https://www.todayonline.com/world/us-military-imagines-war-without-gps*

[24] *https://www.wearethemighty.com/new-artillery-destroys-without-gps*

[25] *At our owl peril : DoD Risk Assessment in a post-primacy world https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1358*

[26] *Rapport sur les enjeux de la numérisation des armées, http://www.assemblee-nationale.fr/15/rap-info/i0996.asp*

collaboratif, navigation autonome des robots, cybersécurité, maintenance prédictive, aide à la décision et au commandement », déclarait Florence Parly en mars 2018[27] ;

- Le renforcement de nos moyens d'action globaux dans le cyberespace. Il s'agit à la fois de renforcer les capacités de protection, de lutte informatique (défensive ou offensive), de renseignement « cyber », d'action informationnelle mais aussi de guerre électronique. Les opérations menées par les forces russes en Syrie ou en Ukraine mettent en effet en lumière le renouveau de la guerre électronique et le retard pris par la France[28], mais également par les Etats-Unis, dans le domaine. Ce sera le rôle du programme CUGE (capacité universelle de guerre électronique) qui se traduira en 2025 par la livraison de 3 Falcons qui remplaceront les 2 Transall Gabriel.

Une posture permanente cyber (PPC)

Le projet de Loi de programmation militaire 2019-2025 adopté par le Sénat le 29 mai 2018 inclut la création d'une posture permanente cyber (PPC) placée sous le contrôle du ComCyber pour assurer la défense des forces armées dans le cyberespace, en temps de paix comme de crise, ou de guerre.

Cette posture recouvre trois missions principales :

- *« La surveillance de l'espace numérique et la détection des atteintes affectant le ministère des Armées » ;*
- *« La capacité des forces à se déployer en sécurité au regard des menaces provenant du cyberespace, et à accomplir leur mission » ;*
- *« La réaction aux agressions informatiques ou informationnelles, y compris en prenant des mesures pour en faire cesser les effets ».*

[27] *https://www.defense.gouv.fr/actualites/economie-et-technologie/florence-parly-presente-son-plan-en-faveur-de-l-intelligence-artificielle-axe-d-innovation-majeur-du-ministere-des-armees*

[28] *Lire à ce propos l'article d'Olivier Dujardin sur le site de l'AGEAT : https://ageat.asso.fr/spip.php?article248*

FOCUS INNOVATION

Entretien avec Frédéric GUIHÉRY, Responsable des activités R&D, AMOSSYS

PRÉSENTATION

Amossys, PME rennaise créée en 2007, est une société de conseil et d'expertise en Cybersécurité reconnue (CESTI, PASSI-LPM...). Son laboratoire d'études et de R&D, qui emploie aujourd'hui une quinzaine de personnes, réalise des prestations d'expertise dans de nombreux domaines et porte la démarche d'innovation de la société, notamment en matière de lutte informatique défensive (LID) et d'analyse de vulnérabilités.

LA DÉMARCHE

La démarche d'innovation d'Amossys est avant tout collaborative et repose sur des partenariats avec des laboratoires académiques et notamment ceux de l'INRIA, centre de recherche également basé à Rennes. Cette collaboration permet d'allier les capacités de recherche fondamentale des équipes académiques, avec la visibilité sur les besoins opérationnels des utilisateurs dont disposent les équipes d'Amossys.

La démarche d'innovation d'Amossys se caractérise ensuite par une vocation duale, civile et défense. Les solutions conçues par ses équipes sont aussi bien destinées à des clients du secteur de la défense, notamment le ministère des Armées, qu'à des acteurs privés, en particulier les éditeurs de produits de sécurité.

Les projets de recherche auxquels participe la société bénéficient ainsi du soutien d'organismes publics, notamment celui de l'Agence Nationale de la Recherche et du ministère des Armées via le dispositif RAPID.

LES PROJETS EN COURS

- **Analyse et évaluation des vulnérabilités.**

L'analyse et l'évaluation des vulnérabilités constituent le cœur de métier d'Amossys. Elles peuvent être réalisées tant sur les applications et sur les équipements réseaux que sur les systèmes industriels. Elles peuvent aussi prendre la forme d'analyse de la sécurité de protocoles de communication, de la sécurité de langages, compilateurs et APIs, ou de la résistance d'application face à la rétro-ingénierie. En partenariat avec l'INRIA, Le laboratoire d'études et de R&D d'Amossys a développé plusieurs outils innovants dans ce domaine, et notamment des frameworks de rétro-conception et de fuzzing de protocoles.

Netzob, framework open source d'ingénierie inverse de protocoles de communication propriétaires

Cet outil permet de faciliter l'évaluation de modélisation de protocoles ainsi que l'analyse de la robustesse des mises en œuvre.

Il prend en charge différents types de protocoles (protocoles texte comme HTTP ou IRC, protocoles à champs fixes comme IP ou TCP, ou protocoles à champs variables comme ceux basés sur ASN.1), ce qui lui permet d'automatiser l'identification des champs sensibles d'un protocole, par exemple celui qui indique la longueur d'une charge utile. Une fois un modèle de protocole appris, le framework est capable de générer du trafic en respectant ce modèle, ce qui lui permet notamment de tester des équipements réseau.

A terme, il pourrait aussi intégrer une capacité de fuzzing de protocoles

▸ La lutte informative défensive (LID) :

Le laboratoire d'études et de R&D d'Amossys apporte également son expertise en matière de LID sur plusieurs volets : conception de systèmes d'information résilients ou de postes de travail durcis, étude sur l'embarqué sécurisé ou la sécurisation de systèmes industriels, spécification de protocoles cryptographique...Amossys a ainsi mis en place des plateformes de simulation de SI et de simulation d'attaquant.

ORECAS, solution de cartographie et topologie passive d'un SI

Cet outil innovant de cartographie et de surveillance des flux réseau se distingue par sa capacité à prendre en compte la dimension « sécurité » de la cartographie des flux réseau dans son intégralité. Les problématiques liées à la sécurité sont en effet au cœur de ce projet, et se traduit concrètement par des dispositifs dédiés, comme par exemple le couplage d'un IDS avec une cartographie. Ce dispositif, rarement déployé dans les produits de ce type, permet de réduire de façon significative les fausses alarmes remontées lors d'éventuelles attaques contre le réseau surveillé, et par conséquence d'améliorer considérablement la qualité de la surveillance du réseau.

CALENDRIER

Forum Cyberdéfense & Stratégie - Mardi 3 juillet 2018

Le Commandement de la cyberdéfense, en partenariat avec le Pôle d'Excellence Cyber, organise le 3 juillet 2018 la seconde édition du Forum Cyberdéfense & Stratégie au Cercle National des Armées sur le thème : « Quelles ruptures et quelles innovations pour la cyberdéfense ?». Intelligence artificielle et hyperconnectivité seront au centre des discussions de la journée, qui s'articuleront autour de deux tables rondes dédiées aux capacités d'action futures dans le cyberespace et aux outils et dispositifs d'innovation en cyberdéfense.

Les équipes des 8 chaires de recherche soutenues par le ministère des Armées échangeront avec ses représentants ainsi qu'avec des industriels du secteur, sur ces thématiques et des sujets d'intérêt commun.

VOS PROCHAINS ÉVÉNEMENTS

European Cyber Week

à Rennes

du 19 au 22 novembre 2018

Infos et inscriptions
www.european-cyber-week.eu
#EuroCyberWeek
@ExcellenceCyber

Journées C&ESAR 2018

à Rennes

du 19 au 21 novembre 2018

Intelligence artificielle et cybersécurité

Forum International de la Cybersécurité

à Lille

du 22 au 23 janvier 2019

www.forum-fic.com