# CYBERSÉCURITÉ INTELLIGENTE : comment mutualiser pour ne plus subir ?

**Lors des Assises de la Sécurité, en octobre à Monaco, Guillaume Poupard (92), DG de l'ANSSI, a proposé d'"anticiper pour ne plus subir et de trouver des solutions par une approche collective". *Deux experts d'IMS Networks, Philippe Lepain, Directeur de la technologie, et Roberto Pasqua, Docteur en informatique,* nous expliquent comment la mutualisation consolidera la cybersécurité par l'intelligence artificielle.**

La sophistication et l'ampleur des attaques sur les systèmes d'information les rendent de plus en plus destructrices. La cybersécurité constitue un enjeu économique majeur par la nécessité absolue de protéger les données, capital informationnel des entreprises. Une course s'est engagée contre pirates et rançonneurs qui ont une longueur d'avance dans cette guerre.

Si la sauvegarde du cyberespace est l'affaire des États et des organisations intergouvernementales régulatrices (UE, OCDE), elle est aussi celle des entreprises, petites et grandes, et des utilisateurs par ailleurs consommateurs, mais pas encore suffisamment conscients de leur vulnérabilité. Dans les entreprises, cette prise de conscience doit s'étendre au-delà des DSI et RSSI, pour toucher l'ensemble des décideurs et des collaborateurs. À l'analyse des risques doivent correspondre méthodes, outils et formation.

**Gestion des talents et développement des compétences**

Face à ces menaces capitales, et aux risques qu'elles créent, les mondes étatique et entrepreneurial n'ont pas progressé à la même vitesse que celui des agresseurs en termes de compétences : le manque de clairvoyance a atténué la demande de talents formés pour résister aux attaques et les contrer. Le rapport Gartner sur la sécurité de l'information estime la croissance globale annualisée de ce marché à 8,5 % de 2017 à 2022. Cette étude prévoit les plus fortes accélérations en matière de *Security as a Service*. Ce marché favorable est en pleine croissance. Mais, selon Le Monde, 350 000 postes en cybersécurité manqueraient en Europe d'ici à 2022. Cette raréfaction des compétences s'observe déjà en France, avec 1 200 postes non pourvus sur 6 000 en 2017. Il manque des opérateurs dans les *security operation centers* (SOC), alors que les menaces augmentent tout autant que les masses de données à traiter. On tente de combler cette lacune avec de l'intelligence artificielle (IA), mais les attaquants, de leur côté, investissent aussi dans ce domaine. On comprend alors l'impératif des méthodes IA dans les SOC, mais les *data scientists* y sont trop souvent absents.

**La souveraineté française et européenne en matière de cyberintelligence**

Récemment, le Groupement des industries de défense et de sécurité terrestre et aéroterrestre (GICAT) a proposé la création d'une réponse technologique souveraine en matière de surveillance numérique (Cluster Data Intelligence). Une grappe d'entreprises mutualisera les savoir-faire de grands groupes industriels, de PME et de start-ups.

IMS Networks partage la volonté de l'ANSSI, du GICAT et de la Commission européenne de fédérer des partenaires publics et privés pour répondre aux enjeux de la cybersécurité et mettre en valeur le potentiel technologique qui émerge de ses rapprochements. Par ailleurs, la recommandation de créer des pôles de recherche 3IA, issue du rapport Villani sur la stratégie nationale de recherche en IA, vise à enrayer le retard français en la matière. Il a généré le lancement de quatre pôles d'excellence au sein desquels nous voyons des collaborations possibles, et notamment dans notre région d'origine, à Toulouse, avec le projet ANITI dédié à la recherche sur l'IA hybride, plus fiable, mixant différentes méthodes et technologies. Par notre taille, nous savons qu'il est vain de combattre seul face au cyber-ouragan annoncé dans le rapport de l'Institut Montaigne sur les cybermenaces (2018). Cependant, nous avons d'ores et déjà lancé un axe de recherche et développement en matière d'apprentissage automatique pour la cybersécurité.

**Vers une communauté ouverte, multidisciplinaire, transparente et innovante**

Nous pensons que le GICAT et les pôles 3IA ne pourront pas, à eux seuls, relever le défi de la cybercriminalité. Au travers d'une plateforme ouverte, nous voulons agréger l'intelligence d'acteurs divers comme les entreprises, les laboratoires de recherche, les communautés et les particuliers, y compris les *white hats* vertueux.

> **"Au travers d'une plateforme ouverte, nous voulons agréger l'intelligence d'acteurs divers."**

À la nécessaire diversité de ces acteurs s'ajoute celle des données multisectorielles qui alimenteront la plateforme au fur et à mesure de son développement. Au-delà de l'intérêt de créer cette richesse tout en testant les méthodes de détection sur tel ou tel corpus, nous construirons une base de connaissance partagée


Centre opérationnel du réseau et de la sécurité NSOC d'IMS Networks à Castres.

et largement distribuée, incluant à la fois les données sources et une grande variété de modèles d'attaque. Ceci permettra de contribuer aux efforts de normalisation et de proposer des standards d'échange de ces flux.

La plateforme reposera sur un troisième pilier fondateur : un vaste choix de méthodes de détection. Elles relèvent en général du monde de l'IA puisqu'elles viennent sinon remplacer, au moins épauler l'opérateur humain.

En cybersécurité, bien des hypothèses restent à tester. L'apprentissage supervisé est trop coûteux en temps d'indexation des corpus malveillants et bénins, et l'approche non supervisée, plus facile à mettre en œuvre, génère trop de faux positifs. Les méthodes qui utilisent les réseaux neuronaux ont produit encore moins de résultats probants pour la détection d'attaques. La plateforme proposera de tester les résultats les plus prometteurs en recherche, par exemple l'apprentissage actif.

**"Nous savons qu'il est vain de combattre seul face au cyber-ouragan."**

À Monaco, Guillaume Poupard a rappelé que "l'approche par l'open source est essentielle, et passe par l'implication de chacun, y compris par les plus petits acteurs". Nous pensons que seul le modèle du logiciel libre peut permettre la mise en œuvre de cette vision. Il faut ouvrir les boîtes noires présentées aux clients comme des logiciels *magiques* et éclairer leurs contenus. Si on n'applique pas les principes de l'open source, elles resteront fermées. Publier et donner les résultats en toute transparence n'est pas toujours naturel, mais les gains potentiels sont réels en matière d'offre de services sur le marché de la cybersécurité. Notre proposition intègre le fait que les décideurs ne peuvent opérer des choix sans comprendre les résultats des logiciels de détection d'attaque. La plateforme proposera de nouveaux types d'applicatifs permettant de tester, d'évaluer et de comparer les résultats des méthodes de détection de manière pragmatique.

Il faut centrer notre approche sur les usages, comme le fait Anaël Beaugnon dans sa récente thèse (*Apprentissage supervisé et systèmes de détection : une approche de bout en bout impliquant les experts en sécurité*).

Dans le domaine de la cybersécurité, aucun système actuel ne propose d'outils pour comprendre et caractériser les résultats des moteurs d'IA, pas plus que d'interfaces ergonomiques réellement adaptées. L'espace de représentation des flux malveillants n'est, à ce sujet, pas encore assez défini. Qui plus est, comme la guerre attaquants/défenseurs risque d'employer les mêmes armes en IA, on ne pourra pas se passer de l'arbitrage humain.

La plateforme reposera sur la diversité des acteurs, des données et des méthodes de détection, dans une approche multisectorielle, transversale et transparente. Elle n'atteindra pas nos objectifs sans innovation en matière d'outils pédagogiques et ergonomiques, condition pour qu'elle soit attractive, aussi, en termes de talents à susciter. Elle aura la mission de réduire la fracture numérique pouvant naître de l'application inappropriée de l'IA au domaine de la cybersécurité.

Par cette approche adaptative, itérative, réactive et transparente, notre projet est de mutualiser pour ne plus subir.

## EN BREF

*IMS Networks est une société française qui gère des infrastructures numériques critiques depuis vingt ans. Sa filiale, Cyblex Technologies, développe des activités de R&D dans le domaine de l'intelligence artificielle qu'elle associe à des plateformes technologiques spécialisées dans la cyberdéfense.*