Enjeux numériques

Cybersécurité : sommes-nous prêts ?

N°32 - DÉCEMBRE 2025

Notre site

les Annales des mines Depuis 1794

Publiées avec le soutien de l'Institut Mines-Télécom

les Annales des mines
Depuis 1794

ENJEUX NUMÉRIQUES

ISSN 2781-1263 (en ligne)
ISSN 2607-9984 (imprimé)
Série trimestrielle - N°32 - Décembre 2025

Rédaction

Conseil général de l'Économie
Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique
120, rue de Bercy
Télédoc 797
75572 Paris Cedex 12
Tél. : 01 53 18 52 68
http://www.annales-des-mines.org

Grégoire Postel-Vinay
Directeur de la publication et Rédacteur en chef

Alexia Kappelmann
Secrétaire générale

Daniel Boula
Secrétaire général adjoint

Magali Gimon
Assistante de rédaction et Maquettiste

Nuria Gorris
Webmestre et Maquettiste

Publication

Photos de couverture
Le Tricheur à l'as de carreau, Photo © RMN-Grand Palais (musée du Louvre) / Adrien Didierjean

Iconographie
Daniel Boula

Mise en page
Magali Gimon

Impression
Dupliprint Mayenne

Cybersécurité : sommes-nous prêts ?

La stratégie française – Les enjeux RH

La stratégie européenne – Impact sur les organisations

Ce numéro a été coordonné par
Éric FREYSSINET

Préface - Un collectif prêt à rehausser massivement les digues de cyberprotection de la Nation

Par Vincent STRUBEL
Directeur général de l'ANSSI

Le 18 septembre 2025, plus de 1 000 organisations ont participé à un exercice de crise d'origine cyber d'une ampleur inédite sur l'ensemble du territoire national, dans 13 régions de l'Hexagone et 7 territoires d'Outre-mer, sur 8 fuseaux horaires. Intitulé REMPAR25 et organisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) avec le soutien d'une soixantaine de partenaires publics et privés, il a non seulement permis d'éprouver les capacités de réponse des organisations face aux attaques informatiques, mais a aussi constitué un test grandeur nature du dispositif national de cybersécurité. Pari réussi.

Cet exercice de crise s'inscrit dans la continuité d'autres exercices organisés ces dernières années (REMPAR22, préparation aux Jeux Olympiques et Paralympiques de Paris 2024). Ces programmes visent à préparer la Nation face à une menace cyber qui ne cesse de se durcir, dans un contexte géopolitique conflictuel. Alors que la chaîne de valeur du numérique est de plus en plus complexe à sécuriser, les attaquants sont désormais capables de conduire des attaques massives, dans des fenêtres de temps toujours plus réduites. Ils sont aussi de plus en plus désinhibés, passant d'une logique d'espionnage ciblé à des démarches de déstabilisation et de sabotage, parfois à grande échelle. Leurs motivations peuvent également converger, entre acteurs étatiques, cybercriminels et « hacktivistes », ce qui pourrait conduire à des attaques d'ampleur.

Sommes-nous prêts à faire face à cette menace ? C'est l'objectif des travaux engagés depuis la Revue stratégique de cyberdéfense de 2018 et confortés par l'actualisation de la Revue nationale stratégique en 2025 et la stratégie nationale de cybersécurité. L'objectif ? Bâtir une résilience cyber de premier rang. La France en a les moyens.

De nouvelles formes d'action publique ont été mises en place ces dernières années pour augmenter la cybersécurité des organisations et des territoires. Elles ont permis d'aller un cran plus loin vers cette résilience. Parmi elles, on peut citer les parcours de cybersécurité déployés dans le cadre du plan France Relance[1] ou les exercices de crise massifiés à l'instar de REMPAR25. Ces actions ont aussi reposé sur le travail en réseau d'un écosystème de cybersécurité qui s'est progressivement étoffé aux côtés des services de l'État : les centres de réponse à incident cyber (CSIRT pour *Computer Security Incident Response Team*) sectoriels et territoriaux, l'InterCERT France[2], le groupement d'intérêt public Action contre la Cybermalveillance (ACYMA) qui porte la plateforme 17Cyber[3], les campus cyber, les prestataires de services et offreurs de produits de cybersécurité notamment. Au-delà de ces acteurs en première ligne, ce sont aussi des acteurs « généra-

[1] Parcours de Cybersécurité | ANSSI, https://cyber.gouv.fr/parcours-de-cybersecurite

[2] Première communauté de centres de réponse à incident cyber en France.

[3] 17Cyber - Mon assistance en ligne | Site officiel, https://17cyber.gouv.fr/

listes » qui se sont saisis de ces enjeux, à l'instar des organisations professionnelles et des collectivités territoriales.

En parallèle de ce développement, la réglementation s'est renforcée et vise à mobiliser les utilisateurs et les fournisseurs de services et de produits numériques autour de cette cause commune. L'Union européenne constitue en cela un levier important pour notre résilience collective. La France s'est fortement impliquée ces dernières années au niveau européen, pour soutenir une élévation générale du niveau de sécurité des États membres. La directive « sécurité des réseaux et de l'information », dite « NIS2 », qui impose des mesures de sécurité à plusieurs milliers d'organisations, et le règlement sur la résilience cyber (*Cyber Resilience Act*, CRA), qui imposera bientôt des règles d'hygiène numérique aux fournisseurs de produits intégrant du numérique, offrent l'opportunité de changer d'échelle en matière de cybersécurité. Le règlement sur la cybersécurité (*Cyber Security Act*, CSA), qui pose les fondements de la certification européenne en matière de cybersécurité, complète ce triptyque européen. Sa révision en cours fait l'objet d'une attention forte de la France, notamment pour se prémunir des risques liés aux lois extraterritoriales. Au-delà de la réglementation, d'autres démarches s'imposent aux acteurs pour se protéger face à de nouvelles menaces, à l'instar de l'ordinateur quantique et des travaux engagés pour conduire fournisseurs et utilisateurs de produits de cryptographie vers la cryptographie post-quantique.

Cette approche complète de la cybersécurité ne peut réussir sans une gouvernance solide et une synergie renforcée entre les services de l'État, les collectivités territoriales, les entreprises, les acteurs de la recherche et de la société civile. Cette intégration plus forte est désormais engagée dans la lignée de la Revue nationale stratégique 2025 et de la stratégie nationale de cybersécurité.

Introduction

Par Éric FREYSSINET
Officier général de gendarmerie

Notre série *Enjeux numériques* des *Annales des Mines* s'est déjà penchée plusieurs fois sur les enjeux de cybersécurité. Nous y avons démontré que la cybercriminalité est devenue une activité globalisée et industrialisée, portée avant tout par des motivations économiques. Ainsi, face à des menaces en constante évolution, la cybersécurité doit être pensée comme un enjeu stratégique mêlant gouvernance, souveraineté numérique, régulation et compétences. Nos auteurs ont également insisté sur l'importance de la formation et de la culture du risque pour renforcer la résilience collective.

En 2025, nous avons choisi de faire un point d'étape : sommes-nous prêts pour les enjeux de cybersécurité d'aujourd'hui et des cinq prochaines années à l'échelle nationale et européenne ?

La réponse courte est oui, parce que beaucoup d'efforts ont été entrepris au cours des dernières années, mais nous verrons que bien évidemment l'effort doit être poursuivi. Il est vrai que la France est souvent à l'avant-poste des initiatives qui garantissent une meilleure cybersécurité collective, mais c'est à l'échelle européenne que cela prend du sens. En effet, dans un marché commun garantissant la libre circulation des biens et services, mais aussi des personnes, dans un espace où entreprises, collectivités et particuliers sont de plus en plus dépendants de leurs partenaires, fournisseurs ou interlocuteurs dans l'espace numérique, il est indispensable que tous avancent avec les mêmes exigences.

Une première dimension est donc l'analyse de l'état de la menace. Son état actuel est décrit dans la première partie, et complété par une seconde dimension, à savoir notre capacité d'anticipation. Nous n'attendons plus passivement que les difficultés surviennent, et un vrai effort de veille est réalisé dans de nombreux métiers. Dans ce numéro, nous vous proposons de faire le point sur les enjeux du moment en matière de cybercriminalité, mais aussi sur des enjeux techniques tels que ceux liés aux crypto-actifs, à l'intelligence artificielle et à son impact sur la cybersécurité, ou encore sur l'impact de l'informatique quantique sur la sécurité des algorithmes de chiffrement.

Au-delà des évolutions technologiques, c'est la question des dépendances, illustrée dans ce numéro par celles liées aux logiciels, qui est au cœur de la menace contemporaine en cybersécurité, cause d'incidents répétés et qui démontre la nécessité de prendre en compte non seulement la sécurité de nos outils et installations propres mais aussi celle de nos partenaires. Enfin, nous avons tenu à porter notre regard sur l'impact subi par les victimes.

Tout cela nous a amenés à nous pencher ensuite dans une seconde partie sur la façon dont les organisations s'adaptent en termes de gouvernance. Le message principal est peut-être que l'on est passé de la sécurité informatique perçue comme un problème technique, à une approche plus globale, intégrée à la prise en compte dynamique des risques, et à l'intégration progressive du pilotage de la cybersécurité dans les préoccupations des dirigeantes et dirigeants. Bien entendu, tout le monde n'avance pas encore à la même vitesse, mais les évolutions organisationnelles sont fortes en particulier au sein de l'État et des grandes entreprises. La priorité des années à venir est clairement du côté des petites entreprises, des entreprises de taille intermédiaire et des collectivités locales.

Cette vision est accompagnée dans une troisième partie par une adaptation de la réponse française, avec une ambition nouvelle dans la stratégie nationale de cybersécurité qui

aura peut-être été publiée d'ici à la parution de ce numéro. Un des angles forts des débats autour de cette stratégie – qu'on retrouve dans le projet de loi sur la résilience actuellement débattu au Parlement – est celui des ressources humaines, en particulier sous l'angle de la formation. Les articles de la troisième partie vous proposent un panorama des approches tant du point de vue des employeurs que de ceux qui pensent les formations.

Enfin, la dernière partie se penche sur les ambitions européennes, jusque dans les territoires, là où l'application des réglementations européennes telles que NIS2 aura un impact, notamment du point de vue de l'offre de cybersécurité pour accompagner entreprises, collectivités et particuliers.

Cette vision globalement positive ne doit pas nous empêcher d'avoir un regard critique et de regarder de l'avant, y compris à l'échelle européenne. D'abord parce que la menace est globale et en perpétuelle évolution, et surtout peut-être que la menace nous concerne dorénavant tous, en tant que cible, mais aussi en tant qu'acteurs d'une cybersécurité collective.

C'est donc peut-être sous l'angle de la solidarité qu'il faut aborder aujourd'hui ces enjeux et nous avons essayé de l'approcher très concrètement dans un article consacré à la sécurisation des organisations humanitaires. Au-delà, cette solidarité va trouver à s'exprimer dans tous les écosystèmes, dans tous les territoires, ou entre générations.

Au nom du comité éditorial de la revue *Enjeux numériques*, je tiens à remercier l'ensemble des auteurs de ce numéro qui se sont impliqués pour partager leur expérience et souhaite qu'il contribue à la résilience collective.

Évolution des menaces de cybersécurité en 2025

Par le Général Éric FREYSSINET
Conseiller sénior cybersécurité & cybercriminalité
au commandement du ministère de l'Intérieur dans le cyberespace

À l'heure où les cyberattaques s'intensifient et se diversifient, les frontières entre criminalité, espionnage et conflit se brouillent. Les acteurs malveillants disposent de moyens sans précédent et exploitent autant les dépendances technologiques que les failles humaines et organisationnelles. Face à cette complexité croissante, États et entreprises doivent renforcer leur résilience collective, anticiper les ruptures technologiques et consolider la coopération internationale en matière de cybersécurité.

Les menaces auxquelles doivent faire face les acteurs de la cybersécurité sont évidemment en perpétuelle évolution. Les acteurs malveillants s'adaptent aux évolutions des technologies, à l'arrivée de nouveaux produits et services. Leurs approches et méthodes deviennent de plus en plus complexes, s'adaptant aux défenses mises en place et cherchant toujours de nouvelles stratégies, tout en bénéficiant de ressources sans cesse accrues.

En 2025, l'un des éléments clés de cette évolution est la confirmation d'une interpénétration de plus en plus forte entre les acteurs étatiques, les organisations criminelles et, parfois, des entreprises qui peuvent être les fournisseurs des premiers, ou les vitrines, voire les façades des seconds.

Le second élément qui caractérise l'adaptation des méthodes des attaquants est l'augmentation des scénarios mettant en cause ce qu'on appelle traditionnellement la chaîne d'approvisionnement ou encore les chaînes de dépendance : approvisionnement en matériel, logiciels et lors des développements logiciels, mais aussi interdépendances *via* les infrastructures et autres interfaces informatiques que l'on partage avec ses partenaires, fournisseurs ou plus largement l'écosystème dans lequel chaque personne ou organisation évolue.

Ces deux premiers aspects ont d'ailleurs pour conséquence de plus grands risques de retombées lors des conflits militaires qui s'accompagnent de plus en plus souvent d'une dimension numérique.

Le troisième élément est celui des évolutions technologiques actuelles ou à venir qui font évoluer la surface d'attaque ou la puissance potentielle de ces attaques. Nous citerons évidemment l'adoption croissante de l'intelligence artificielle, mais aussi les perspectives offertes par l'informatique quantique, sans oublier de regarder au-delà.

Pour certains encore, le risque posé par les évolutions juridiques est parfois considéré comme une menace. Nous verrons pourquoi cela devrait plutôt être pensé comme un cadre favorisant une meilleure sécurité collective. Mais c'est surtout l'instabilité du contexte juridique au plan international auquel il semble que nous devions être attentifs dans les années à venir.

La montée en puissance des acteurs de la menace

Les frontières entre acteurs étatiques, groupes criminels et entreprises (cybercriminelles-écrans) se sont estompées. Les premiers utilisent de plus en plus des intermédiaires non étatiques pour mener des opérations à faible coût politique ; les seconds bénéficient d'un accès à des outils et savoir-faire issus du renseignement militaire ; les troisièmes servent souvent de façades légales pour masquer des activités illicites.

Les États ont fait du cyberespace un champ d'action stratégique à part entière. Les doctrines militaires intègrent désormais des capacités offensives : sabotage d'infrastructures critiques, désinformation de masse, espionnage économique. Les exemples sont nombreux dans le conflit qui oppose la Russie à l'Ukraine, depuis les attaques ciblant les communications satellitaires au début de l'offensive en février 2022 jusqu'à des offensives numériques contre des opérateurs d'importance vitale, tel que l'opérateur de télécommunications ukrainien Kyivstar en décembre 2023[1].

De leur côté, l'écosystème cybercriminel a adopté une structure quasi-industrielle. Cette professionnalisation se traduit par la prolifération de modèles *"as-a-service"* : rançongiciels, *infostealers*, hameçonnage ou *botnets* disponibles à la location. Ces écosystèmes segmentés rendent l'attribution complexe : un même outil peut être employé par des dizaines de groupes distincts, tandis que les partenariats, comme les infrastructures d'hébergement, évoluent en permanence.

Les entreprises-écrans jouent enfin un rôle croissant. Elles servent de véhicules financiers, d'intermédiaires techniques ou de couvertures pour des opérations de renseignement ou des services cybercriminels. Cette hybridation brouille les pistes et complexifie la réponse juridique comme diplomatique.

Cette dynamique traduit l'émergence d'un véritable marché mondial de la cybercriminalité, avec ses prestataires spécialisés, ses places d'échange et ses mécanismes de réputation. Les outils, les accès et les données s'y négocient comme des biens marchands, tandis que les alliances entre groupes se forment et se défont au gré des opportunités. Le continuum créé sur certains territoires avec les acteurs étatiques rend d'autant plus cruciale la nécessité d'une posture renforcée face à ces menaces et d'une coordination étroite entre les acteurs judiciaires, diplomatiques, du renseignement et militaires.

Cette montée en puissance s'appuie aussi sur un environnement numérique de plus en plus interdépendant, où chaque maillon devient une cible potentielle.

Des chaînes de dépendance devenues cibles stratégiques

Les attaques dites de la chaîne d'approvisionnement (*supply chain*) se sont imposées comme l'un des modes d'action privilégiés des attaquants. Elles ne se limitent plus à la compromission d'une mise à jour logicielle ; elles exploitent désormais l'ensemble des interdépendances technologiques et organisationnelles.

Le matériel représente un premier vecteur de vulnérabilité. La fabrication mondialisée de composants électroniques rend la traçabilité complexe : une altération minime dans la chaîne de production peut compromettre des milliers de systèmes. Au-delà, les vulné-

[1] Attaques contre Kyivstar attribuée au mode opératoire russe Sandwork, https://www.wired.com/story/ukraine-kyivstar-solntsepek-sandworm-gru/

rabilités affectant des équipements rarement mis à jour mais connectés au réseau des entreprises – comme les caméras de surveillance IP ou les routeurs *wifi* – sont désormais largement documentées.

Le logiciel concentre lui aussi une part majeure du risque. L'économie numérique repose sur des dépendances *open source* souvent maintenues par une poignée de bénévoles. L'affaire Log4Shell[2], révélée en 2021, a illustré la portée mondiale d'une faille dans une bibliothèque omniprésente.

Les infrastructures *cloud* et les opérateurs de télécommunications constituent un autre niveau critique. Leur compromission permet d'accéder à des milliers d'organisations clientes. L'attaque de 2020 contre SolarWinds[3], éditeur d'un logiciel de supervision largement utilisé dans la gestion de ces infrastructures, a démontré la puissance de ce type de vecteur.

Enfin, les prestataires et partenaires deviennent des cibles privilégiées. L'externalisation généralisée fait de chaque sous-traitant un maillon potentiel. Une intrusion dans une société de maintenance ou de conseil peut ouvrir la porte à l'ensemble de ses clients. L'attaque qui a paralysé, en septembre 2025, plusieurs aéroports européens *via* le fournisseur Collins Aerospace rappelle avec force qu'un seul maillon vulnérable peut désorganiser un secteur entier.

Face à cela, la cartographie des dépendances et la contractualisation de la sécurité sont devenues essentielles. Les grandes entreprises adoptent des approches de cyber-résilience systémique, intégrant leurs fournisseurs dans des programmes d'audit, de supervision et de partage d'indicateurs de compromission. La cybersécurité ne peut plus être pensée comme un périmètre défensif : elle est devenue une écologie de relations.

Ces interdépendances ne sont pas les seules à amplifier le risque : les technologies émergentes redessinent elles aussi le champ de la menace.

Technologies émergentes : opportunités et nouvelles vulnérabilités

Les innovations technologiques redessinent la surface d'attaque autant qu'elles offrent de nouveaux leviers de défense.

L'intelligence artificielle est au cœur de cette mutation. Les attaquants l'utilisent pour automatiser la génération d'*e-mails* d'hameçonnage, créer des contenus falsifiés ou optimiser la recherche de vulnérabilités. Des outils de génération de *malwares* à base de modèles de langage circulent déjà sur le *dark web* et des LLMs grand public sont parfois détournés à cette fin[4]. En miroir, les défenseurs mobilisent l'IA pour la détection comportementale, la corrélation d'événements et la réponse automatisée.

L'informatique quantique constitue une menace encore théorique, mais suffisamment sérieuse pour que les autorités s'y préparent dès aujourd'hui. Un ordinateur quantique suffisamment puissant pourrait, à terme, casser les systèmes de chiffrement actuels – ceux qui protègent nos échanges, nos données et nos infrastructures numériques. En Europe, la transition vers des solutions dites « post-quantiques » fait déjà l'objet d'une

[2] https://fr.wikipedia.org/wiki/Log4Shell

[3] https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[4] https://abnormal.ai/blog/what-happened-to-wormgpt-cybercriminal-tools

coordination, y compris pour anticiper les scénarios où des données chiffrées aujourd'hui pourraient être déchiffrées plus tard. Cette démarche vise à accompagner les entreprises et les administrations dans le choix et le déploiement de nouveaux algorithmes adaptés à ces évolutions.

Les objets connectés et la 5G constituent une autre zone de fragilité. L'explosion du nombre de capteurs, de dispositifs médicaux et de véhicules connectés multiplie les points d'entrée. Or, la sécurité n'a pas toujours été intégrée dès la conception ; beaucoup d'équipements sont difficilement corrigeables ou dépourvus de mécanismes d'authentification robustes.

On pourrait explorer d'autres domaines émergents :

- la *blockchain* (la technologie inventée avec le *bitcoin*), dont les *smart contracts* mal codés peuvent être exploités ;
- les interfaces cerveau-machine, posant des questions inédites de confidentialité ;
- les systèmes autonomes dans le transport ou l'énergie, où la cybersécurité devient un enjeu vital.

Le véritable défi n'est plus seulement technique : il est organisationnel et culturel. Concevoir la sécurité dès la phase de développement, assurer une gouvernance adaptée et anticiper les usages détournés exigent un changement profond de mentalité.

Le droit entre incertitudes et leviers de cybersécurité

La maturité des pratiques dépend autant de l'évolution des technologies que de celle des règles qui les encadrent. Le droit devient ainsi un pilier essentiel de la résilience numérique et un levier de convergence entre États et entreprises. Mais, la dimension juridique joue un rôle ambivalent : contrainte pour certains, moteur de progrès pour d'autres.

En Europe, les textes NIS2 et DORA renforcent les obligations de gouvernance et de notification d'incidents. Ils visent à homogénéiser les pratiques de sécurité au sein des États membres et à accroître la transparence. Cette normalisation progressive crée un socle commun, mais elle suppose des moyens humains et financiers conséquents pour les entreprises ou collectivités locales qui n'étaient jusque-là pas concernées par ce type de réglementations.

À l'échelle mondiale, la situation reste éclatée. Les législations nationales divergent, les procédures d'entraide judiciaire demeurent lentes, et les conflits de souveraineté compliquent l'attribution des attaques. Les cybercriminels exploitent ces zones grises : il leur suffit de s'abriter derrière une frontière numérique pour échapper à toute poursuite.

Toutefois, depuis une dizaine d'années, la mondialisation du déploiement de la convention du Conseil de l'Europe sur la cybercriminalité, l'harmonisation des législations nationales en Europe ou encore la création du centre européen EC3 à Europol ont permis de gros progrès dans cette coopération.

Mais surtout, considérer le droit comme une menace serait une erreur. Il constitue au contraire un levier de résilience collective : il favorise la responsabilisation, la remontée d'information et la mutualisation des moyens. Le défi des prochaines années sera d'articuler ces cadres juridiques avec les impératifs techniques, dans une logique de gouvernance globale du cyberespace.

Conclusion

La cybersécurité en 2025 ne peut plus se réduire à une problématique technologique. Elle reflète l'interaction d'acteurs aux logiques multiples, d'écosystèmes interdépendants et de cadres normatifs encore instables. Les menaces évoluent plus vite que les réponses, mais la coopération reste possible.

Pour affronter cette recomposition permanente, les organisations doivent adopter une vision systémique : comprendre leurs dépendances, anticiper les ruptures technologiques, investir dans la formation et participer activement aux réseaux de partage d'information.

La cybersécurité n'a plus rien d'un domaine purement technique : elle est devenue un enjeu de gouvernance, de souveraineté et de confiance. Seule une approche collective, fondée sur la transparence et la coopération, permettra d'affronter les crises à venir.

Voler, négocier et répéter : les menaces convergentes de la cybercriminalité et du crime organisé en 2025

Par Edvardas ŠILERIS
Chef de département du Centre européen
de lutte contre la Cybercriminalité d'Europol

Oubliez les pirates solitaires. La cybercriminalité d'aujourd'hui est une industrie planétaire, structurée, rapide et redoutablement efficace. *Phishing* dopé à l'IA, effondrement de la cryptographie sous l'effet du quantique, *deep fakes* ultra-réalistes, contenus pédopornographiques générés par IA – le cybercrime ne connaît plus de limites. Tout peut s'acheter : accès à vos systèmes, données personnelles, services criminels « clés en main » *via* Telegram ou le *dark web*.

Pendant que les lois patinent, les cybercriminels innovent. Ce n'est pas de la science-fiction, c'est notre présent. Découvrez dans cette analyse percutante d'Europol comment le crime organisé, les États hostiles et les nouvelles technologies redéfinissent la menace.

Si l'on considère la cybercriminalité en 2025, on constate que le paysage criminel est d'abord numérique et que les frontières entre les menaces en ligne et hors ligne sont de plus en plus floues. La cybercriminalité n'est pas seulement arrivée à maturité, elle est devenue indissociable des structures plus larges de la criminalité organisée classique, des acteurs étatiques et de l'économie numérique légitime.

Selon l'évaluation annuelle de la menace que représente la criminalité organisée sur Internet (IOCTA) 2025, réalisée par Europol en consultation avec les États membres de l'UE, des pays tiers et des parties privées, la cybercriminalité est entrée dans une nouvelle ère dans laquelle les données sont l'actif déterminant – volées, militarisées et transformées en marchandises à une échelle sans précédent[1]. Le paysage cybercriminel est dominé par le commerce, l'exploitation et l'abus d'informations numériques. Du vol d'informations d'identification aux données générées par IA, le phénomène évolue rapidement, sous l'effet de l'innovation technologique, de l'évolution de la dynamique du marché et de la convergence croissante des agendas criminels et géopolitiques.

Les données comme cible et monnaie

En 2025, les données sont le moteur de la cybercriminalité. Elles sont à la fois l'actif le plus précieux et la cible principale des activités criminelles. L'extraction, la monétisation et la distribution des données sont à l'origine d'un large éventail d'infractions facilitées par internet, notamment l'usurpation d'identité, le *phishing*, les rançongiciels, la fraude

[1] https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

financière et les attaques ciblées contre les infrastructures. La valeur des données – personnelles, financières, d'entreprise – réside dans leur polyvalence. Une fois volées, elles peuvent être revendues, utilisées à des fins d'ingénierie sociale ou exploitées pour obtenir un accès plus approfondi à un système de traitement automatisé de données.

Les cybercriminels ont industrialisé le vol et la revente d'informations numériques, les traitant comme des marchandises *via* des marchés souterrains bien structurés. Les courtiers en accès initial (Initial Access Brokers - IAB) et les courtiers en données (Data Brokers) sont des acteurs clés de cet écosystème, offrant un accès personnalisé à des réseaux compromis et à des ensembles de données. Leurs services sont à la base d'une grande partie de l'économie de la cybercriminalité, alimentant des marchés à forte demande qui s'étendent sur le *dark web*, des canaux chiffrés et des places de marché sur invitation seulement.

Le déploiement généralisé de logiciels malveillants voleurs d'informations, souvent diffusés par le biais de campagnes de *phishing*, de fausses applications ou de sites *web* compromis, alimente ce commerce. Ces logiciels malveillants sont conçus pour recueillir discrètement des données sensibles sur les systèmes infectés. Les informations volées sont ensuite traitées et vendues ou échangées sur des marchés illicites. La marchandisation des informations d'identification, des fragments d'identité et des jetons d'accès reflète une économie cybercriminelle évolutive, agile et de plus en plus précise dans son ciblage.

Crime en tant que service et spécialisation

La structure de la cybercriminalité est devenue de plus en plus modulaire, avec une spécialisation claire des rôles et une division du travail. Le crime en tant que service (CaaS) est devenu la norme dans l'ensemble de l'écosystème. Les acteurs n'ont plus besoin de compétences techniques avancées pour se livrer aux activités cybercriminelles à fort impact. Au lieu de cela, ils peuvent acheter l'accès, les outils et même un service après-vente auprès de fournisseurs de services criminels.

Des plateformes entières sont apparues pour faciliter ces opérations, des services tels que l'obfuscation avancée, l'hébergement à l'épreuve des balles et les canaux de communication cryptés. Le résultat est une infrastructure cybercriminelle qui reflète une industrie multinationale décentralisée, avec des chaînes d'approvisionnement, des affiliés et même des évaluations par les utilisateurs.

Au cœur de cet écosystème se trouvent les IAB et les courtiers en données, dont les services jouent un rôle fondamental dans la réalisation de diverses formes des activités cybercriminelles. Ces courtiers opèrent sur des forums ou *via* des plateformes de messagerie chiffrées (telles que Telegram), offrant une série d'outils et de données puissants.

Ils offrent des options de ciblage fine, c'est-à-dire la possibilité de filtrer et de segmenter des individus ou des groupes sur la base de caractéristiques très spécifiques. Il peut s'agir de données démographiques (âge, sexe, localisation), de modèles comportementaux (habitudes de consommation, historique de navigation, activité sur les réseaux sociaux), voire d'informations plus sensibles telles que l'appartenance politique, l'état de santé ou le score de solvabilité. Ce ciblage précis permet aux acteurs de la menace d'adapter les campagnes de *phishing*, les escroqueries et autres attaques reposant sur l'ingénierie sociale afin d'augmenter leurs chances de succès.

En outre, ces courtiers proposent également des services groupés, c'est-à-dire qu'au lieu d'offrir uniquement des données brutes, ils regroupent plusieurs services. Une offre groupée typique peut comprendre l'accès à des listes d'adresses électroniques vérifiées, des modèles d'hameçonnage, des outils d'automatisation pour la diffusion (par exemple,

des robots spammeurs), des informations d'identification volées et même une infrastructure telle qu'un hébergement *bullet proof* ou des proxys rotatifs. Ces offres groupées sont conçues pour abaisser la barrière d'entrée des criminels ayant moins de connaissances techniques, en leur permettant de lancer des cyberattaques coordonnées et d'apparence professionnelle avec un minimum d'efforts.

Par essence, les courtiers en données servent de guichet unique aux cybercriminels, en monétisant les données personnelles et en rendant les campagnes d'attaques sophistiquées plus faciles, moins coûteuses et plus efficaces.

Ingénierie sociale avancée et armement de l'IA

La dernière évaluation de la menace de la criminalité grave et organisée (EU-SOCTA) d'Europol constate que l'IA et d'autres nouvelles technologies telles que la *blockchain* ou l'informatique quantique vont accélérer la criminalité grave et organisée de manière rapide et significative. Elles constituent un catalyseur pour toutes sortes de crimes et renforcent l'efficacité des opérations criminelles en amplifiant leur vitesse, leur portée et leur sophistication[2]. L'une des évolutions les plus préoccupantes est la montée de la cybercriminalité assistée par l'IA, en particulier dans le domaine de l'ingénierie sociale. L'utilisation de l'intelligence artificielle générative – comme les grands modèles de langage (LLM) – a considérablement amélioré la qualité, l'ampleur et l'efficacité des attaques par hameçonnage et usurpation d'identité. Des messages sur mesure peuvent être produits en masse avec un minimum d'erreurs linguistiques, ce qui les rend beaucoup plus convaincants que les escroqueries traditionnelles.

Les technologies de clonage vocal et de vidéo (*deep fake*) sont également utilisées pour usurper l'identité des individus avec une précision alarmante. Ces contenus générés par IA permettent aux fraudeurs de se faire passer pour des cadres en entreprises, des parents ou des personnalités publiques avec une authenticité convaincante. La confiance psychologique exploitée par ces simulacres aggrave la menace, car les victimes baissent souvent leurs gardes face à des voix ou des visages familiers.

Les kits d'hameçonnage dotés de capacités d'IA affichent désormais des taux de clics plusieurs fois supérieurs à ceux des campagnes élaborées manuellement. La combinaison de l'automatisation et de la manipulation psychologique permet aux cybercriminels de tromper même des utilisateurs expérimentés, ce qui pousse les organisations à améliorer leur formation et leurs capacités de détection des menaces.

En matière d'IA, il semble que nous ne soyons plus qu'à un pas d'une nouvelle frontière : la criminalité assistée par l'IA et exécutée avec un minimum de supervision humaine. Au-delà des courriels de *phishing* et des *deep fakes*, les criminels commencent à exploiter l'IA générative pour concevoir, exécuter et monétiser des attaques de manière autonome. Ce changement marque l'évolution de la « criminalité en tant que service » vers « l'IA en tant que service », où des modèles sophistiqués peuvent être loués à la demande. À mesure que ces outils deviennent plus accessibles, le paysage des menaces pourrait se transformer en un écosystème criminel semi-autonome, où l'intention est programmée et l'exécution entièrement confiée à des algorithmes.

[2] https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

Le facteur quantique : effondrement cryptographique ou course aux armements numériques ?

Mais l'IA n'est pas la seule avancée technologique qui pose des défis croissants dans la lutte contre la cybercriminalité. L'informatique quantique, qui n'en est encore qu'à ses débuts, représente une menace systémique qui plane. Une fois viable, elle fera voler en éclats les normes cryptographiques existantes, rendant le chiffrement d'aujourd'hui obsolète.

Les cybercriminels, les acteurs étatiques et les groupes criminels organisés investissent déjà dans des attaques de type « récolter maintenant, déchiffrer plus tard », en interceptant et en stockant des données chiffrées en prévision des futures capacités quantiques. La valeur des données sensibles se prolonge dans l'avenir, en particulier pour la propriété intellectuelle, les renseignements et les infrastructures stratégiques à long terme.

Cela rend plus urgentes les initiatives en matière de cryptographie post-quantique, mais augmente également les enjeux de la cyber-stabilité internationale. Si les capacités quantiques émergent de manière asymétrique – contrôlées par des États voyous ou vendues sur le marché noir – nous pourrions assister à un effondrement soudain et catastrophique de la confiance numérique dans les systèmes critiques.

Afin de relever les défis croissants liés aux progrès de la cryptographie grâce à l'informatique quantique, le Quantum Safe Financial Forum (QSFF) d'Europol a lancé un appel à l'action aux institutions financières et aux décideurs politiques, les exhortant à donner la priorité à la transition vers une cryptographie sécurisée par l'informatique quantique dès le mois de février 2025[3].

Prolifération des logiciels malveillants et exploitation de la chaîne d'approvisionnement

L'une des cibles les plus prometteuses en 2025 est le ciblage des chaînes d'approvisionnement en logiciels et des environnements de développement. Les criminels exploitent les dépôts de paquets par le biais d'une technique appelée *slopsquatting*, qui consiste à télécharger des bibliothèques malveillantes dont les noms diffèrent subtilement des paquets légitimes et populaires, généralement en raison d'erreurs typographiques, d'incohérences de formatage ou de caractères invisibles. Le *slopsquatting* vise les conventions de dénomination « négligées » que les développeurs peuvent utiliser lors de l'automatisation de la construction ou de la résolution des dépendances. Ces variations passent souvent inaperçues. Cette tactique exploite à la fois la confiance que les développeurs accordent aux référentiels publics et les flux de travail centrés sur l'automatisation du développement logiciel moderne, ce qui permet aux attaquants d'injecter des portes dérobées, des outils d'exfiltration de données ou d'autres formes de logiciels malveillants dans des systèmes qui ne se doutent de rien. Les attaques de la chaîne d'approvisionnement sont également très efficaces, car elles permettent d'injecter des logiciels malveillants dans des composants logiciels largement utilisés qui sont intégrés à leur insu dans des milliers d'applications en aval. Une fois intégrées dans une version de confiance, ces bibliothèques compromises peuvent s'implanter durablement dans les environnements cibles ou exfiltrer silencieusement des données sensibles sans déclencher de détection immédiate. L'opacité, la complexité et l'interdépendance des écosystèmes de développe-

[3] https://www.europol.europa.eu/publications-events/publications/quantum-safe-financial-forum-call-to-action

ment modernes rendent ces attaques particulièrement efficaces. Les outils automatisés et les gestionnaires de paquets tirent régulièrement des dépendances et des mises à jour de dépôts publics sans vérification manuelle, ce qui crée un environnement où des composants malveillants peuvent être introduits et propagés à grande échelle. En outre, en raison du volume considérable de dépendances imbriquées et de relations indirectes entre les paquets, les paquets malveillants peuvent rester profondément ancrés et ne pas être détectés pendant de longues périodes, et ne sont parfois découverts qu'après que des dommages importants ont été causés.

Fragmentation et évasion du marché

En réponse aux actions des forces de l'ordre et au démantèlement des places de marché, le milieu criminel clandestin est devenu plus fragmenté et plus agile. Les forums et les marchés de données migrent fréquemment d'une plateforme à l'autre, adoptant souvent des technologies plus sécurisées pour échapper à la détection. Les criminels utilisent également de plus en plus d'applications de messagerie chiffrées, tel que Telegram, non seulement pour des communications privées, mais aussi comme plateformes pour mener des activités illégales. Nombre de ces applications intègrent désormais des fonctions telles que des chats de groupe, des canaux et même des outils de type *marketplace*, qui permettent aux utilisateurs d'annoncer et de vendre des données volées, des outils de piratage informatique, des produits stupéfiants ou d'autres biens et services illicites. Ces applications concurrencent les forums traditionnels basés sur le *web*, qui sont plus faciles à surveiller et à supprimer pour les forces de l'ordre, en offrant davantage d'anonymat, de sécurité et de mobilité, ce qui les rend idéales pour mener des opérations criminelles avec moins de risque d'être détecté.

Néanmoins, Europol reste bien entendu déterminé à s'attaquer aux places de marché en ligne illégitimes qui facilitent toutes sortes de crimes en ligne. En mai dernier, une opération policière mondiale coordonnée par Europol a porté un coup sévère à la criminalité clandestine, avec 270 arrestations de vendeurs et d'acheteurs du *dark web* dans dix pays. Connue sous le nom d'opération RapTor, cette opération internationale a permis de démanteler des réseaux de trafic de drogue, d'armes et de produits de contrefaçon, envoyant ainsi un signal clair aux criminels qui se cachent derrière l'illusion de l'anonymat[4].

La réputation du marché reste un élément clé, les vendeurs et les acheteurs s'évaluant les uns les autres pour établir une confiance, ce qui renforce encore la professionnalisation de la cybercriminalité.

Hybridation de la cybercriminalité et de la criminalité organisée

On constate également une convergence croissante entre les groupes criminels organisés traditionnels et les acteurs de la cybercriminalité. Les organisations criminelles intègrent de plus en plus les capacités numériques dans leurs opérations, utilisant les nouvelles technologies pour blanchir de l'argent, intimider leurs rivaux ou coordonner leur logistique.

Cette convergence est également évidente dans l'externalisation des opérations numériques à des entrepreneurs criminels par l'intermédiaire des opérateurs CaaS. Les acteurs malveillants affiliés à des États tirent parti de l'écosystème du cybercriminel à des fins

[4] https://www.europol.europa.eu/media-press/newsroom/news/270-arrested-in-global-dark-web-crackdown-targeting-online-drug-and-criminal-networks

d'espionnage, de sabotage ou de désinformation, brouillant ainsi la frontière entre les activités criminelles et les agressions géopolitiques. Ce lien complique l'attribution des acteurs cybercriminels et élargit le paysage des risques au-delà des cibles commerciales et civiles pour inclure les infrastructures critiques et les institutions démocratiques.

Ces menaces hybrides se caractérisent par des attaques multi-vectorielles à fort impact qui combinent le vol de données, la coercition physique, la désinformation et l'atteinte à la réputation. Elles sont conçues non seulement pour le gain financier, mais aussi pour déstabiliser et intimider, souvent au service d'objectifs politiques ou économiques plus larges.

Exploitation des mineurs et contenus d'abus sexuels d'enfants générés par IA

Une autre tendance très inquiétante est l'utilisation de plus en plus importante de contenus ayant trait à la violence sexuelle sur mineurs, générés à l'aide d'outils basés sur l'intelligence artificielle. Ce contenu peut être produit sans victimes physiques, mais il est souvent distribué avec du matériel réel, ce qui rend la détection et l'intervention plus difficiles.

Au début de l'année 2025, Europol a apporté son soutien à la toute première opération mondiale visant le matériel d'abus sexuel d'enfants généré par l'intelligence artificielle (CSAM). Les autorités de 19 pays ont procédé à des arrestations et à des perquisitions coordonnées au cours desquelles 25 personnes ont été arrêtées et 273 suspects ont été identifiés. Le principal suspect, un ressortissant danois, dirigeait une plateforme en ligne où il distribuait le matériel généré par l'IA qu'il produisait. Après un paiement symbolique en ligne, des utilisateurs du monde entier ont pu obtenir un mot de passe leur permettant d'accéder à la plateforme et de regarder des enfants se faire abuser. L'opération « Cumberland » est l'une des premières interventions internationales contre le matériel d'abus sexuel d'enfants généré par l'IA, ce qui complique singulièrement la tâche des enquêteurs, notamment en raison de l'absence de législation nationale concernant ces crimes[5].

L'utilisation de modèles génératifs pour créer des images d'abus réalistes a explosé ces derniers mois, en partie parce qu'elle permet aux délinquants de contourner certaines définitions légales du matériel d'abus sexuel sur mineurs. Les canaux chiffrés et anonymes facilitent encore la prolifération de ce type de matériel, tout en limitant la capacité des autorités à identifier et à arrêter les délinquants. Le volume et la portée de ces réseaux augmentent, ce qui pose des problèmes éthiques, juridiques et techniques urgents aux services répressifs et à la société dans son ensemble.

Dans ce contexte, les États membres de l'UE discutent actuellement d'un règlement commun proposé par la Commission européenne pour faire face à cette nouvelle situation et protéger les enfants contre les abus et l'exploitation sexuels[6].

Criminalité financière et blanchiment d'argent par crypto-monnaie

Les crypto-monnaies et les technologies *blockchain* restent au cœur des opérations financières des réseaux cybercriminels. Les crypto-monnaies sont utilisées pour le paiement

[5] https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0209

de rançons, le blanchiment de fonds volés et la facilitation de transactions anonymes à travers les frontières internationales. La sophistication croissante des outils de finance décentralisée (DeFi) a permis aux criminels de contourner entièrement les systèmes de surveillance financier traditionnels.

Les services de mixage, d'échange y compris entre *blockchains* permettent d'obscurcir encore davantage l'origine des fonds illicites. Malgré une pression réglementaire croissante, nombre de ces services continuent d'opérer dans des juridictions permissives ou non réglementées. L'utilisation de cryptoactifs confidentiels et d'échanges de crypto-monnaies de pair à pair s'est également développée, offrant des couches supplémentaires d'anonymat.

Les actifs numériques sont désormais utilisés pour stocker et blanchir les produits du crime, mais aussi comme méthode de paiement au sein même de l'écosystème cybercriminel. Les affiliés, développeurs, courtiers et facilitateurs de rançongiciels effectuent souvent des transactions en crypto-monnaies, en utilisant des outils automatisés ou des intermédiaires tiers qui retiennent les paiements jusqu'à ce que les deux parties remplissent les conditions convenues – ce qui leur permet d'établir une confiance mutuelle et de faire des affaires sans jamais révéler leur véritable identité.

Complexité juridique et paralysie de l'application de la loi

Malgré les progrès réalisés, nos cadres juridiques restent mal adaptés à la nature et à la versatilité de la cybercriminalité. La plupart des instruments de coopération internationale ont été conçus pour lutter contre la criminalité traditionnelle, où les dossiers transfrontaliers sont rares et non la norme. En matière de cybercriminalité, plus de 90 % des affaires sont intrinsèquement internationales, mais les procédures d'entraide judiciaire sont encore lentes, fragmentées et réactives.

Les conflits juridictionnels, les modèles d'extradition vieillissants et les règles d'accès aux données fragmentées paralysent les efforts des services d'enquêtes. Dans le même temps, les criminels opèrent en temps réel, déploient des infrastructures sur plusieurs continents et utilisent des plateformes décentralisées à l'abri de toute action légale.

Le fossé entre la théorie juridique et la réalité opérationnelle s'élargit et pourrait devenir insurmontable s'il n'est pas comblé de manière radicale. Des efforts tels que le règlement de l'UE sur la preuve électronique et des instruments internationaux tels que le deuxième protocole additionnel à la Convention de Budapest sont des étapes cruciales, mais pas suffisantes.

Le chemin à suivre

À l'heure actuelle, la cybercriminalité n'est pas simplement un ensemble d'infractions numériques déconnectées les unes des autres. Il s'agit d'une économie criminelle sophistiquée, fondée sur les données et utilisant de plus en plus l'IA, qui est en train de remodeler le paysage mondial des menaces. La convergence des progrès technologiques, du développement des marchés clandestins et du lien entre le crime et l'État crée de nouvelles vulnérabilités à tous les niveaux de l'écosystème numérique.

Pour comprendre et atténuer ces menaces, il faut changer la façon dont les institutions, les gouvernements et les particuliers envisagent la cybersécurité. En 2025, le champ de bataille ne se limite plus aux codes informatiques et aux pare-feux : il est psychologique, géopolitique et systémique. Au cœur de ce champ de bataille se trouvent les données : la monnaie de l'économie souterraine moderne.

La menace dans le champ des cryptoactifs

Par Karolina GORNA
Doctorante en Sécurité Logicielle à Ledger et Télécom Paris

Issue de la promesse d'un échange de valeur décentralisé, la technologie *blockchain* a engendré un écosystème de cryptoactifs dont l'adoption croissante s'accompagne de risques cyber d'une nature et d'une complexité nouvelles. Le présent exposé se propose de cartographier ces risques, depuis le paradigme de l'autodétention qui charge l'individu d'une responsabilité sécuritaire, jusqu'aux vulnérabilités critiques de la pile applicative (contrats intelligents, langages, oracles). L'analyse s'étend aux dépendances des infrastructures Web3, aux paradoxes de la finance décentralisée, et aux enjeux de souveraineté soulevés par la confrontation entre monnaies numériques étatiques (MNBC) et *stablecoins* privés.

Introduction et définitions

Les origines conceptuelles de la *blockchain* remontent à plus de 30 ans. En 1991, Stuart Haber et W. Scott Stornetta, deux cryptographes et informaticiens américains chez Bell Communications Research (Bellcore), publient l'article fondateur "How to Time-Stamp a Digital Document" [1]. Ils y décrivent un système d'horodatage numérique infalsifiable basé sur une chaîne de hachages cryptographiques, considéré aujourd'hui comme l'ancêtre direct de la *blockchain*.

Une *blockchain* est une base de données cryptographiques, stockée sur un réseau décentralisé d'ordinateurs, sur laquelle il est possible de lire et d'écrire des données, mais pas de les modifier ni de les supprimer. Chaque *blockchain* est régie par un consensus définissant les règles d'existence et de fonctionnement de celle-ci. Les mainteneurs de la *blockchain*, qui contribuent à l'écriture dans sa base de données et au maintien de son intégrité, se voient récompensés par l'attribution de jetons numériques, appelés "coins" en anglais. Le *bitcoin* est ainsi le *coin* de la *blockchain* Bitcoin, et l'éther celui de la *blockchain* Ethereum, par exemple. Parmi ces jetons, certains, dont les *bitcoins*, sont programmés pour être générés en quantité limitée dans le temps, ce qui leur procure de la rareté, et donc une forme de valeur. Cette valeur est aussi le résultat de l'énergie électrique et du temps passé par les mainteneurs du réseau pour le sécuriser. Ces *coins* peuvent être ensuite vendus sur des plateformes d'échanges agissant comme des bourses numériques, soit utilisés pour construire des produits dérivés comme des jetons fongibles suivant le standard ERC20 (à penser comme les tickets restaurants, construits sur des monnaies FIAT comme l'euro). Des jetons non fongibles, appelés "NFT" en anglais, peuvent également être construits sur ces *blockchains* afin de soit apporter de la propriété intellectuelle numérique à des fichiers informatiques (art digital, objet en 3D, etc.), soit numériser des objets existants dans le monde réel pour subdiviser leurs nombres de détenteurs (art physique, immobilier, etc.). Tous ces *coins* et leurs dérivés sont qualifiés de cryptoactifs. Des débats persistent jusqu'à aujourd'hui pour savoir si certains de ces *coins* ou jetons fongibles peuvent être considérés comme des cryptomonnaies. Cet exposé vise à identifier les risques de cybersécurité liés à l'adoption croissante des cryptoactifs dans notre société.

Le paradigme de l'autodétention : entre souveraineté et responsabilité individuelle

La possession de cryptoactifs repose sur le principe fondamental d'autodétention (ou "self-custody" en anglais), qui requiert la maîtrise d'une clé cryptographique privée. Cette suite de caractères alphanumériques est le seul élément qui confère à son détenteur la propriété et le contrôle irrévocable de ses actifs sur une *blockchain*. De cette clé privée, qui doit demeurer secrète, sont générées par dérivation une ou plusieurs clés publiques et adresses, destinées à être partagées pour recevoir des fonds.

La sécurisation de la clé privée est assurée par des portefeuilles numériques, qui se déclinent en deux catégories principales. D'une part, les portefeuilles logiciels, souvent intégrés à des extensions de navigateur, permettent à l'utilisateur d'accéder à sa clé privée et de signer (au sens cryptographique) des transactions par le biais d'un mot de passe. Leur connectivité constante à Internet offre une grande commodité d'utilisation, mais les expose de manière inhérente aux cyberattaques en ligne. D'autre part, les portefeuilles matériels sont des dispositifs physiques conçus pour stocker la clé privée dans un composant sécurisé et isolé. N'étant connectés à Internet que ponctuellement pour signer une transaction, ils réduisent considérablement le vecteur d'attaque en ligne. L'enjeu majeur de conception pour ce type de matériel concerne la robustesse de son architecture : la compromission physique de l'appareil ne doit pas permettre l'extraction de la clé privée par un attaquant.

Ce modèle d'autodétention de valeur constitue une rupture par rapport aux systèmes centralisés traditionnels, où les instruments d'identité (passeport) ou de paiement (carte bancaire) demeurent la propriété des entités émettrices que sont l'État ou la banque. Ce paradigme opère un transfert de responsabilité majeur vers l'individu, qui devient le seul garant de la sécurité de ses actifs, tout en lui octroyant une souveraineté et une liberté d'usage inédites.

Pour certains utilisateurs, la contrainte de l'autodétention justifie le recours à des plateformes d'échange centralisées. Cette délégation de conservation transforme leurs actifs en une simple créance sur l'opérateur, créant un risque de contrepartie significatif. La faillite de la plateforme d'échange FTX en novembre 2022 a mis en évidence ce péril, lorsque les dépôts des clients sont devenus inaccessibles, intégrés à la masse des actifs de l'entreprise en liquidation.

D'un modèle d'échange d'information à un modèle d'échange de valeur

Les *blockchains* utilisent l'infrastructure internet (TCP/IP) pour faire communiquer leurs nœuds *via* des protocoles pair-à-pair (P2P) dédiés. Les utilisateurs peuvent interagir avec ces réseaux soit directement *via* ces protocoles natifs, soit indirectement par l'intermédiaire d'interfaces *web* (HTTPS/JSON-RPC) fournies par des services tiers ou des nœuds exposant une API. Cette hybridation entre services *web* traditionnels et interactions *blockchain* constitue le fondement du Web3.

Bien que l'architecture *blockchain* permette de se passer de confiance envers les nœuds tiers *via* la vérification cryptographique, les coûts de déploiement et de maintenance d'un nœud complet poussent les utilisateurs vers des fournisseurs centralisés. Cette centralisation *de facto* réintroduit des points de défaillance au sein d'écosystèmes conçus pour être décentralisés.

Parallèlement se développent des services de pseudonymisation ("exemple.eth") qui substituent aux longues adresses hexadécimales des identifiants aisément mémorisables. Ces dispositifs, bien que pratiques, réduisent l'anonymat et exposent davantage les utilisateurs aux tentatives de fraudes ciblées.

La complexité de la sécurité applicative et infrastructurelle

Démocratisés par le lancement d'Ethereum en 2015, les contrats intelligents ("smart contracts") sont des programmes autonomes gérant des cryptoactifs sur une *blockchain*. Toute vulnérabilité qui s'y trouve peut causer des pertes financières directes et irréversibles. La source de ces failles peut venir de l'ensemble de la pile d'exécution : les nouveaux langages (Solidity, Cairo, Noir, etc.), leurs compilateurs et les machines virtuelles introduisent chacun des classes de bogues qui leur sont propres. Face à cette complexité, un écosystème de cybersécurité s'est structuré, s'appuyant sur des audits de code menés par des entreprises expertes et sur des programmes de "bug bounty".

Cependant, les risques dépassent le seul code applicatif : la sécurité de la chaîne d'approvisionnement logicielle est un enjeu majeur. S'ajoute à cela la complexité opérationnelle des mises à niveau de protocole (les "hard forks"), qui doivent être déployées sur la *blockchain* active sans l'interrompre, au risque de fragmenter la chaîne ou paralyser l'écosystème.

Entre dynamiques spéculatives et logiques communautaires

L'avènement des contrats intelligents a engendré une prolifération de jetons fongibles, dont certains, appelés "memecoins", dépourvus d'utilité fonctionnelle, tirent leur valeur de dynamiques spéculatives et communautaires. Leur facilité de déploiement favorise les manipulations de marché, notamment les stratégies de "pump and dump" où des acteurs influents gonflent artificiellement les cours avant de liquider leurs positions.

Parallèlement, la méthode de "l'airdrop" permet à des développeurs de distribuer gratuitement des jetons aux premiers utilisateurs de leurs *blockchains* ou projets, favorisant ainsi la décentralisation du contrôle protocolaire. Cette pratique légitime est cependant détournée par des acteurs malveillants qui disséminent des jetons liés à des contrats frauduleux, l'interaction avec ces derniers pouvant déclencher le vol des actifs détenus dans les portefeuilles des victimes.

La promesse illusoire des *blockchains* privées comme garantie de sécurité

Désireuses de s'approprier les promesses de la *blockchain* en matière de sécurité et d'immuabilité, certaines entreprises ont développé des infrastructures qualifiées de « *blockchains* privées ». Ce terme est cependant souvent fallacieux ; celui de « registres distribués » lui est préférable. En effet, si ces systèmes sont bien distribués (ressources réparties sur plusieurs nœuds), ils ne sont pas décentralisés, car leur gouvernance demeure sous le contrôle d'une seule entité ou d'un *consortium* restreint.

Cette centralisation du contrôle constitue un point de défaillance unique : la corruption de l'entité dirigeante compromet l'intégrité de l'ensemble du registre, annulant la garantie de sécurité prétendue. L'appellation "blockchain" est alors fréquemment instrumentalisée comme un argument *marketing*, d'autant que le caractère propriétaire et secret de leur code source empêche toute garantie contre d'éventuelles vulnérabilités.

Les Monnaies numériques de banque centrale en réponse à *bitcoin* et aux cryptoactifs

En réponse à l'adoption croissante des cryptoactifs, illustrée en France par une détention estimée à près de 10 % de la population en 2025 [2], les banques centrales explorent quant à elles la création de Monnaies numériques de banque centrale (MNBC). Elles se déclinent en MNBC de gros ("wholesale") pour les transactions interbancaires, et en MNBC de détail ("retail") pour le public. Cette dernière variante se distingue fondamentalement de la monnaie dématérialisée actuelle en constituant une dette directe de la banque centrale envers le citoyen, un changement d'architecture qui soulève d'importants enjeux de gouvernance et de confidentialité des données. Alors que le support technologique d'un potentiel euro numérique reste débattu en Europe, la Chine expérimente déjà son yuan numérique (e-CNY) [3], un système centralisé qui ne partage pas les propriétés de résistance à la censure des cryptoactifs décentralisés comme le *bitcoin*.

Les *stablecoins* et le nouveau "soft power" américain

Au-delà des projets étatiques de MNBC, l'un des cas d'usage les plus matures de la technologie *blockchain* se situe dans le secteur des paiements. C'est dans ce cadre que se sont développés les *stablecoins* : des cryptoactifs adossés à une monnaie fiduciaire qui, en étant majoritairement gagés sur le dollar américain, étendent *de facto* l'hégémonie monétaire des États-Unis à l'écosystème numérique.

Face à cette domination, la position marginale des *stablecoins* en euro (moins de 1 % du marché en août 2025 [4]) constitue un enjeu de souveraineté pour l'Union européenne, que la régulation MiCA vise à résoudre en structurant un marché continental sécurisé afin de renforcer son autonomie stratégique.

Architecture et enjeux de la finance décentralisée (DeFi)

Les *stablecoins* constituent le principal instrument d'échange au sein d'un écosystème financier alternatif en plein essor : la finance décentralisée (DeFi). Celle-ci vise à recréer les services financiers traditionnels, comme le prêt ou l'échange, *via* des protocoles autonomes sur *blockchain* qui remplacent les intermédiaires classiques par des contrats intelligents. Cette architecture soulève cependant des défis critiques. D'une part, l'absence d'entité centrale rend la responsabilité juridique floue en cas de faille ou de pertes. D'autre part, l'écosystème dépend de manière vitale des oracles pour importer les données du monde réel (prix des actifs, etc.). La manipulation ou la défaillance de ces oracles représente un risque systémique majeur, pouvant déclencher des pertes en cascade.

Les cryptoactifs et la cybercriminalité

La nature publique des *blockchains* confère aux cryptoactifs une traçabilité inhérente, qui contraste avec l'anonymat des espèces monétaires. Cette propriété fondamentale permet une quantification précise des flux financiers, comme l'illustrent les analyses de la société Chainalysis [5].

Leurs rapports indiquent que l'activité illicite représente une fraction minoritaire de l'écosystème (0,14 % du volume total en 2024). L'évolution des pratiques criminelles, notam-

ment la migration vers les *stablecoins* qui constituent 63 % des flux illicites, suggère une priorisation de l'efficacité transactionnelle sur la recherche d'anonymat. En conséquence, cette traçabilité impacte différemment les modèles criminels : tandis que les volumes des marchés du *darknet* diminuent, en partie sous l'effet des actions répressives, la menace posée par les rançongiciels demeure significative.

La recherche fondamentale à l'épreuve du Web3

L'écosystème Web3 accélère la recherche cryptographique fondamentale. Les exigences de scalabilité et de sécurité stimulent le développement des preuves à divulgation nulle (ZKP) et des méthodes de vérification formelle. La recherche d'anonymat favorise parallèlement des technologies comme le chiffrement homomorphe (FHE), et pose des défis réglementaires liés aux mélangeurs de transactions ou aux monnaies anonymes. Ces innovations, tributaires d'une validation temporelle, font du Web3 un laboratoire où convergent recherches théoriques et applications financières immédiates.

Conclusion

L'écosystème des cryptoactifs est défini par des compromis structurels qui rendent le risque cyber systémique. Chaque aspect de cet univers, de la souveraineté individuelle (indissociable d'une responsabilité sécuritaire absolue) à l'innovation technique (génératrice de nouvelles vulnérabilités), l'expose à des menaces inédites. La nature ouverte des protocoles favorise simultanément la collaboration et la fraude, tandis que l'émergence des monnaies numériques de banque centrale (MNBC) et des *stablecoins* inscrit ces enjeux dans un cadre de compétition géopolitique. L'avenir de ce secteur dépendra donc de sa capacité à résoudre ces tensions structurelles entre l'idéal décentralisé, la sécurité et les impératifs d'adoption.

Bibliographie

[1] HABER S. & STORNETTA W. S. (1990, August), "How to time-stamp a digital document", *In Conference on the Theory and Application of Cryptography*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 437-455.

[2] ADAN (2025), « Web3 & Cryptos en France et en Europe : Vers une adoption durable et institutionnelle ».

[3] CHIN G. T. (2025), "China's 'digital renminbi'(e-CNY) as financial inclusion: the global frontier of central bank digital currency", *Global Public Policy and Governance*, 5(1), pp. 63-81.

[4] EUROPEAN PARLIAMENT (2025), "Global currency dominance in the 21st century: where does the euro stand?".

[5] CHAINALYSIS (2025), "The Chainalysis 2025 Crypto Crime Report".

Les défis de la cybersécurité de l'IA

Par Katarzyna KAPUSTA, Bousad ADDAD et Juliette MATTIOLI
Thales

Nous sommes témoins du succès fulgurant de l'intelligence artificielle (IA) qui améliore la prise de décision humaine, en termes de rapidité et de qualité. Malgré ses capacités incroyables et son adoption rapide dans les applications non critiques, l'intégration de l'IA dans des systèmes à haut risque reste problématique car elle soulève de nouveaux défis liés à la confiance, notamment la cybersécurité. Le cycle de vie spécifique des applications à base d'apprentissage automatique et les vulnérabilités intrinsèques qui y sont liées imposent de revisiter les approches classiques à l'analyse des risques. Parmi les menaces les plus importantes figurent les attaques visant à modifier le fonctionnement du modèle. À cela s'ajoute la problématique de sécurisation de l'apprentissage de l'IA, formée sur des données sensibles, contre les fuites d'informations ainsi que la protection des droits d'auteur dans un contexte complexe. En attendant les réglementations, les professionnels cherchent les contremesures qui permettraient d'allier la protection à la performance.

L'intelligence artificielle (IA) améliore la prise de décision humaine, en termes de rapidité et de qualité. Il n'est donc pas étonnant de voir à quel point les géants du numérique et les instituts de recherche internationaux de premier plan ont considérablement fait progresser l'IA, bien qu'ils soient principalement concentrés sur les applications civiles. En effet, le déploiement de l'IA dans le secteur des systèmes critiques ou dans ceux à haut risque nécessite de prendre en compte plusieurs contraintes. Il s'agit notamment de renforcer la confiance dans la prise de décision réalisée par la machine. L'IA doit rester fiable indépendamment des perturbations, internes ou externes. La cybersécurité fait partie des attributs clés de la confiance, car elle permet de garantir un bon fonctionnement face aux agissements d'un attaquant. Ses concepts fondamentaux ne changent pas, mais leur implémentation doit être revisitée pour tenir compte des spécificités de l'IA.

La cybersécurité revisitée

À la différence des applications traditionnelles, les solutions fondées sur l'IA, et en particulier sur l'apprentissage automatique (AA), se nourrissent de données. Leur cycle de vie débute par une collecte de données et le choix d'un algorithme, dit modèle d'IA. Le modèle apprend ensuite à associer des entrées à des sorties souhaitées dans des tâches telles que la classification, la détection, la segmentation, etc. Une fois mis en service, il pourra être réadapté à un nouveau contexte en passant par un réapprentissage sur des données complémentaires. Cette organisation élargit la surface d'attaques potentielles, car un attaquant peut manipuler les données en plus du modèle, et ce à plusieurs stades du processus.

Une stratégie de sécurité efficace commence par l'identification des actifs à protéger, typiquement des données d'entraînement, du modèle ou des données d'entrée/sortie. Elle

se poursuit par une étude des menaces potentielles et de leurs impacts en fonction des capacités de l'attaquant. Dans un scénario « boîte blanche », l'attaquant aura accès à tout le modèle, ses poids et biais, voire ses données d'apprentissage, tandis qu'en « boite noire » il ne pourra que l'interroger. Des mesures correctives peuvent ensuite être mises en œuvre, qui vont soit améliorer la robustesse du modèle, soit ajouter des défenses dans le système environnant.

Se protéger contre l'empoisonnement

Un attaquant ayant accès à la chaîne d'approvisionnement des données d'un modèle cherchera à la manipuler dans le but d'empoisonner le modèle. À la suite d'une telle attaque, les performances du modèle pourraient être dégradées. L'empoisonnement peut notamment servir à 'insérer des fonctionnalités inconnues de l'utilisateur légitime, appelées portes dérobées. Il touche principalement les systèmes qui 's'alimentent des utilisateurs, comme les filtres à spam. Un des exemples d'empoisonnement les plus connus reste le *chatbot* TAY de Microsoft, qui apprenait sur le contenu de Twitter. En 2016, il a dû être mis hors service après que des internautes malveillants ont réussi à lui faire tenir des propos haineux[1].

L'insertion de portes dérobées peut se faire non seulement par une modification directe des données, mais aussi *via* la mise à disposition, en source libre, de modèles déjà infectés. Cette menace pèse particulièrement sur les systèmes de reconnaissance faciale, dans lesquels les portes dérobées sont utilisées pour contourner les règles de détection.

Des techniques standards, telles que les signatures, permettent d'assurer l'intégrité des données et des modèles. Elles peuvent être complétées par des techniques spécifiques à l'IA, qui vont détecter l'empoisonnement en analysant le comportement du modèle sur des exemples spécifiques. Des filtres peuvent également être incorporés dans la chaîne de traitement, en amont et en aval de l'IA, pour supprimer les données potentiellement malveillantes ou contradictoires.

Se prémunir contre les manipulations d'entrées

Une fois le modèle d'IA déployé, un attaquant peut l'induire en erreur en manipulant soigneusement ses données d'entrée. Ce type d'attaque, connu sous le nom d'exemples antagonistes ou adverses, a été inventé pour leurrer des modèles de vision par ordinateur. Il est maintenant établi qu'une modification astucieuse d'une image peut avoir un impact important sur sa perception par l'IA (voir la Figure 1 page suivante).

Le même principe d'attaque s'applique potentiellement à tous les modèles d'AA, même si les exemples issus de la vision par ordinateur sont les plus répandus. Par exemple, l'équipe Friendly Hackers de cortAIx Labs a examiné la possibilité d'une attaque adverse sur une IA de classification de signaux électromagnétiques. Elle a réussi à attaquer le modèle en manipulant légèrement les spectrogrammes des signaux collectés et classifiés par le modèle. En conséquence, l'attaque pouvait leurrer le modèle en l'amenant à prédire la classe d'un signal comme étant une autre. Néanmoins, cette vulnérabilité reste difficile à exploiter en pratique en raison des prétraitements appliqués aux signaux. Cela affecte la perturbation apportée par l'attaquant et rend finalement l'exemple adverse inopérant.

[1] À peine lancée, une intelligence artificielle de Microsoft dérape sur Twitter, https://www.lemonde.fr/pixels/article/2016/03/24/a-peine-lancee-une-intelligence-artificielle-de-microsoft-derape-sur-twitter_4889661_4408996.html

L'inclusion des données perturbées parmi les données d'entraînement – on parle d'entraînement adverse dans ce cas – est d'ailleurs l'une des techniques utilisées pour renforcer la robustesse des modèles d'IA contre les exemples antagonistes. D'autres défenses reposent sur des filtres appliqués aux signaux d'entrée (par exemple : un filtre passe-bas qui lisse le signal et supprime la perturbation). De plus, des techniques ensemblistes faisant appel à plusieurs modèles en même temps sont parfois utilisées bien que cela alourdisse le coût en mémoire et en calcul. Des approches de validation du fonctionnement du modèle par méthodes formelles sont également considérées, notamment pour des applications critiques.

Figure 1 : Exemple d'attaque adverse sur une IA multimodale capable de traiter simultanément des informations visuelles et textuelles (Source : équipe Friendly Hackers de Thales cortAIx Labs France).

Protéger les données

Les modèles d'AA ont la particularité de mémoriser des données qu'ils ont vues pendant leur phase d'apprentissage. Ces données peuvent être sensibles ou confidentielles. Il n'est donc pas étonnant que certains attaquants cherchent à remonter vers ces données en analysant le comportement du modèle. C'est ce qu'on appelle une attaque par inversion de modèle. Il en existe plusieurs variantes. Une autre attaque assez proche, dite d'inférence d'appartenance, a pour but de déterminer si un échantillon de données choisi était présent ou non dans l'ensemble des données d'apprentissage. D'autres attaques sur la confidentialité des données visent à retrouver certaines caractéristiques du jeu de données d'apprentissage. Les attaquants dotés de moyens peuvent aller encore plus

loin. En 2023, l'équipe Thales Friendly Hackers a relevé le défi CAID[2] en démontrant qu'il était possible de reconstituer des informations sur les données d'entraînement, et ce, même si le modèle avait été ajusté (ou réappris dans le but de lui faire oublier les données sensibles) sur de nouveaux ensembles de données avant d'être partagé. Le succès d'une telle démarche est naturellement conditionné, comme pour la plupart des attaques, par le degré de connaissance de l'attaquant concernant le modèle cible et ses ensembles de données.

Une contre-mesure simple contre l'exfiltration des données repose sur la limitation des informations partagées avec les utilisateurs, notamment la suppression des scores de confiance accompagnant les sorties. Pour faire face à des attaques avancées, il est nécessaire d'intégrer des techniques d'anonymisation à l'entraînement. Ces approches reposent le plus souvent sur la confidentialité différentielle, une définition mathématique qui se traduit en pratique par l'ajout d'un bruit spécialement conçu sur les données d'entrée, de sortie, ou dans l'algorithme d'entraînement. Elle apporte des garanties fortes de sécurité, mais parfois au prix d'un impact considérable sur l'utilité du modèle (baisse de performance). Un compromis doit donc être trouvé dans ce cas.

Le désapprentissage, une technique qui vise à faire oublier certaines données, permet de revoir l'influences des données dans le cas des modèles déjà appris. Il consiste en la suppression de l'influence d'une partie des données d'apprentissage sans nécessité de passer par un nouvel entraînement, tout en exploitant idéalement certaines des informations contenues dans les données à oublier (ce qui contribuera à la performance). Il s'applique notamment au « droit à l'oubli », car il donne la possibilité d'effacer des données d'un utilisateur qui ne donnerait plus son accord à leur utilisation. D'autres cas d'usage incluent la suppression de l'influence des données classifiées avant l'export ou la remédiation contre les biais ou les données empoisonnées.

Partager et protéger les modèles

L'objectif derrière la protection de la confidentialité des modèles est de pouvoir partager et d'exécuter les modèles sur des appareils non fiables sans révéler leur architecture, leurs paramètres ou leurs données d'entrée/sortie. Le plus souvent cela correspond au cas d'usage où un modèle est mis à disposition en mode MLaaS (ML *as a service*) dans un *cloud* à confiance limitée ou exposé au vol dans une solution embarquée. Il s'agit d'une variante du problème connu de la protection du code pendant l'exécution. En théorie, elle peut être entièrement résolue à l'aide du chiffrement homomorphe, qui permet d'effectuer des calculs sur des données chiffrées. Malgré le développement de ses adaptations pour l'IA, cette technique n'est encore efficace que pour les modèles relativement petits, car elle entraîne des coûts considérables en termes de puissance de calcul. Les environnements d'exécution de confiance sont une alternative matérielle permettant d'isoler une zone d'exécution dans le processeur.

Pour assurer la traçabilité d'un modèle partagé, le créateur du modèle peut avoir recours à des techniques de tatouage. Inspiré des solutions de marquage utilisées pour les supports multimédias, le tatouage de modèle d'AA vise à protéger la propriété intellectuelle d'un modèle en intégrant une preuve d'origine dans l'architecture ou le comportement du

[2] Hacking d'IA : Thales remporte le challenge de la DGA et présente ses solutions de sécurité renforcée de l'IA à des fins militaires et civiles | Thales Group, https://www.thalesgroup.com/fr/monde/securite/press_release/hacking-dia-thales-remporte-le-challenge-dga-et-presente-ses-solutions

modèle. Les techniques de tatouage peuvent être grossièrement divisées en deux catégories principales : « boîte blanche » et « boite noire ». Dans le tatouage en boîte blanche, la preuve de propriété repose sur une modification secrète intégrée dans les paramètres du modèle ou dans l'architecture du modèle. En boîte noire, elle prend la forme d'une modification secrète intégrée dans le comportement du modèle, comparable à l'insertion d'une porte dérobée légitime.

Faciliter la collaboration

Traditionnellement, l'entraînement repose sur la centralisation des données, ce qui implique de les regrouper en un seul lieu où elles peuvent être exploitées. Toutefois, cette centralisation pose des risques non seulement pour la sécurité des données, mais aussi pour la logistique. L'apprentissage fédéré répond à ces préoccupations en permettant l'entraînement de modèles directement sur des dispositifs locaux, les mises à jour des modèles étant agrégées en un modèle global sans que les données brutes ne quittent chaque dispositif. Il a rapidement été adopté pour des cas d'usage d'IoT (Internet des objets), par exemple pour faciliter l'entraînement des IA d'autocomplétion de texte sur les données venant des téléphones portables. Même si les données locales ne sont jamais explicitement échangées, l'apprentissage fédéré ne protège pas le modèle final des fuites d'information, surtout si un attaquant arrive à s'introduire dans le serveur d'agrégation. Pour s'en prémunir, la procédure d'agrégation des modèles locaux peut être sécurisée avec des techniques de chiffrement homomorphe et de confidentialité différentielle.

Ce que change l'IA générative

Les grands modèles linguistiques (LLM) sont la nouvelle cible des pirates informatiques. Les mêmes propriétés de sécurité sont menacées, mais les attaques prennent désormais des formes légèrement différentes. Inspirée des attaques adverses, l'injection de *prompt* permet aux pirates d'utiliser des entrées (*prompts*) soigneusement conçues pour manipuler le LLM afin qu'il exécute des instructions potentiellement malveillantes. C'est ce qu'on désigne par le terme de *jailbreaking*. Un agent conversationnel basé sur un LLM pourrait ignorer des instructions légitimes et effectuer des actions non prévues, ce qui conduirait à la manipulation des réponses du modèle ou de tout processus décisionnel qu'il influence ou contrôle. Par exemple, une requête adverse pourrait convaincre un *chatbot* de répondre à la question « comment fabriquer une bombe » ou de révéler des informations privées, même si des contre-mesures éthiques étaient conçues initialement pour bloquer de telles questions. Les méthodes de *jailbreaking* les plus populaires consistent à demander à l'IA d'adopter une identité différente, telle qu'un personnage fictif ou un autre *chatbot* soumis à moins de restrictions. Ces attaques peuvent inclure des *scénarii* ou des jeux élaborés (impliquant parfois la traduction de langues, des extraits de code, etc.) dans lesquels l'IA est progressivement amenée à discuter d'actes illégaux, de contenus haineux ou de désinformation. Des stratégies d'attaque plus sophistiquées vont masquer du contenu malveillant dans les données envoyées avec la requête ou aller empoisonner les bases de données auxquelles l'agent fera appel.

L'IA générative ouvre également la voie à une arme de manipulation massive, les *deepfakes*. Des attaquants exploitent les *chatbots* de génération de contenu pour obtenir de fausses voix, images ou vidéos. Celles-ci peuvent être utilisées pour tromper les systèmes biométriques, pour des attaques d'ingénierie sociale ou pour la guerre de l'information.

Les défis d'aujourd'hui et demain

De nombreuses initiatives visent à clarifier l'approche de la cybersécurité de l'IA, comme les rapports ETSI TC SAI[3], le guide NIST[4], l'atlas des menaces MITRE ATLAS[5], ou encore le guide ANSSI[6] ou le projet OWASP Gen AI[7] pour la sécurité de l'IA générative. Elles préparent le terrain pour des critères de certification qui mettraient en place un cadre précis pour la validation de la sécurité des systèmes basés sur l'IA et unifieraient les différentes recommandations. Le défi est naturellement de taille pour des systèmes intégrant des réseaux neuronaux de plusieurs milliards de paramètres et fonctionnant en boîte noire, rendant difficile la compréhension des mécanismes internes derrière chaque décision. L'hybridation avec des systèmes experts à base de règles, approche dite neuro-symbolique, semble une voie prometteuse mais c'est encore du domaine de la recherche.

[3] ETSI - TC SAI, https://www.etsi.org/committee/2312-sai

[4] Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2025.pdf

[5] MITRE ATLAS™, https://atlas.mitre.org/

[6] Recommandations de sécurité pour un système d'IA générative | ANSSI, https://cyber.gouv.fr/publications/recommandations-de-securite-pour-un-systeme-dia-generative

[7] Home - OWASP Gen AI Security Project, https://genai.owasp.org

Les menaces liées aux dépendances des logiciels

Par Vincent GIRAUD
Chaire cyber et souveraineté numérique - IHEDN

Lors du développement de produits informatiques, les dépendances dont font preuve les logiciels produits sont un point de vigilance omniprésent chez les éditeurs et concepteurs. Si elles ont l'avantage d'accélérer ainsi que simplifier massivement le travail, et si elles peuvent permettre de bénéficier d'exécutables et de contenus à la fois robustes et éprouvés, celles-ci apportent également leur lot de menaces.

Ces dernières sont présentes à la fois sur les dépendances qui s'appliquent lors du développement comme sur celles qui se montrent à l'utilisation du logiciel. Par ailleurs, estimer qu'elles sont systématiquement le résultat d'une volonté malveillante ou d'une attaque explicite serait une erreur : beaucoup découlent simplement des caractéristiques même du processus de réutilisation ou d'exploitation de contenus externes. Les menaces et les risques associés sont ainsi particulièrement protéiformes.

Introduction

La production logicielle, de par son caractère essentiellement intellectuel, permet des formes de réutilisation et d'usages particulièrement avancés. Dès les premières versions de tous les systèmes d'exploitation multitâches majeurs, la possibilité d'embarquer et de profiter de briques logicielles tierces pendant le développement a été fournie aux concepteurs, soit *via* une intégration totale lors de la création (lien statique), soit en prévision d'une intégration ultérieure (lien dynamique). Par ailleurs, et de manière générale, l'interconnexion croissante des sociétés démontre un deuxième type d'appui logiciel : celui ayant lieu lors de l'utilisation. Les programmes s'utilisent entre eux *via* des interfaces de programmation, que ce soit localement, au sein d'une même machine, ou à distance, *via* un quelconque réseau.

Ces relations de dépendances se sont rapidement imposées comme des postulats de l'informatique moderne. Les cadres techniques et juridiques autour d'elles se sont développés en les considérant comme évidentes. Les premiers lorsque les systèmes d'exploitation se sont adaptés et lorsque la conception d'interfaces de programmation binaires ou applicatives s'est révélée être un savoir primordial dans ce domaine. Les seconds quand le développement de contrats de licence prenant directement en compte ces modes d'utilisation s'est popularisé.

En parallèle, le développement d'internet et des réseaux a largement facilité le partage de code et d'exécutables, notamment à travers les frontières. La mise en place de dépendances logicielles s'est alors multipliée dans une certaine insouciance. C'est seulement plus tard, lors de l'apparition sur la scène mondiale de plusieurs incidents majeurs, qu'un nouvel éclairage sur cette pratique permettra une remise en question sur le rapport bénéfice-risque, d'abord d'un point de vue purement technique. Les récentes transformations géopolitiques et l'évolution des rapports de force causeront une projection de

cette problématique sur le plan de la souveraineté, révélant ainsi tout l'enjeu d'autonomie stratégique qu'elle contient : dans un monde aussi numérique que le nôtre, une certaine indépendance logicielle est nécessairement un socle dont on doit disposer.

Les avantages et les risques associés aux dépendances logicielles varient selon qu'on les considère lors du développement, ou lors de l'utilisation.

Dépendances de développement

Lors du développement d'un logiciel, le concepteur peut en intégrer d'autres en son sein. Cette pratique est, on l'a vu, omniprésente aujourd'hui ; elle est d'ailleurs récursive : les logiciels intégrés ont eux-mêmes d'autres logiciels intégrés en eux. Ce phénomène de lien indirect, appelé « dépendance transitive », mène souvent à une embarcation en cascade de briques logicielles. Les chiffres présents dans un rapport de 2025 de la société Black Duck[1], spécialisée dans la sécurité des chaînes d'approvisionnement logicielles, sont éloquents. Sur 1 658 projets logiciels analysés, 97 % contiennent des briques logicielles externes en sources ouvertes. En moyenne, il y en a 911 par projet, et 64 % d'entre elles sont présentes par dépendance transitive. Les composants logiciels externes représentent au final la majorité du code : 70 % en moyenne à l'échelle d'un projet.

Il y a plusieurs risques associés aux dépendances de développement. Tous ne découlent pas d'une démarche offensive : certains résultent davantage d'événements comme l'abandon d'un projet, qu'il soit spontané ou causé par un manque de support financier ou institutionnel. On peut également mentionner les difficultés juridiques qui s'imposent lors de la réutilisation de code provenant d'un autre pays. On se concentrera ici sur les trois risques les plus prégnants dans la gestion logicielle : les failles dans le travail de maintenance, la perte de maîtrise ainsi que du savoir-faire, et l'insertion de portes dérobées.

Maintenance

Le plus présent au quotidien est celui lié à la maintenance. Chaque brique logicielle doit généralement être incluse au sein d'un projet dans une version précise. Lorsqu'elles sont mises à jour par leurs développeurs respectifs, le concepteur d'un projet doit rapatrier ces nouveautés : au-delà de nouvelles fonctionnalités pas forcément utiles, elles peuvent également apporter des correctifs face à des failles ou des risques de sécurité découverts en elles.

L'exemple des failles de sécurité découvertes dans la bibliothèque logicielle log4j est le plus parlant. Permettant de gérer les journaux et registres de projets écrits dans le langage Java, elle est particulièrement répandue. Une série de failles rendues publiques en 2021 rendront concrets des vecteurs d'attaque résultant notamment en des exécutions de code arbitraire. La gravité de leurs conséquences et l'échec dans le processus de divulgation responsable causeront d'abord un empressement mondial à identifier puis sécuriser les projets touchés, ensuite, une vague de remises en question sur la forme de plus en plus tentaculaire qu'adoptent les conceptions logicielles de par la masse de dépendances insoupçonnée qu'elles accumulent.

L'entretien, le suivi, la mise à jour et la correction des dépendances d'un projet implique nécessairement un travail manuel : il s'agit au mieux de simplement vérifier le bon fonctionnement par la suite, ou au pire, en cas de non-rétrocompatibilité, de reprogrammer l'utilisation du composant. Bien que l'on puisse en espérer une plus grande automatisation à l'avenir, ce suivi reste coûteux. On estime que dans le domaine du développement

[1] Black Duck (2025), "Open source security and risk analysis report".

logiciel, la majorité des coûts ne sont pas attribués à la conception initiale, mais plutôt à la maintenance[2].

Maîtrise et savoir-faire

Rajouter une dépendance de développement à son projet implique de déléguer une fraction algorithmique de son application à un composant tiers embarqué. Le concepteur initial conserve-t-il une totale maîtrise de cette partie de logique ? Faire une telle délégation est souvent motivé soit parce qu'on ignore comment réaliser la tâche concernée, soit parce qu'on la juge commune au point qu'il serait une erreur de la réimplémenter individuellement. Dans le premier cas, on ne maîtrise pas le procédé de base, dans le second, on décide de renoncer au savoir-faire associé en faisant le pari qu'il sera facilement assimilable si besoin est. Ce raisonnement, qui n'est pas dénué de viabilité, incite cependant à multiplier les dépendances logicielles de développement, au point qu'il devient difficile de les contrôler, surtout en considérant celles qui sont transitives.

L'historique des incidents récents tend à montrer qu'un imprévu auprès d'une brique logicielle populaire peut avoir de larges répercussions, que son contenu logique soit complexe ou non. En 2016, le développeur Azer Koçulu a supprimé 273 composants logiciels qu'il avait publiés sur npm, la principale plateforme de gestion de paquets pour le langage JavaScript. L'un d'entre eux était *left-pad*. Son rôle était trivial : procéder à un bourrage de caractères par la gauche dans un texte. Un grand nombre de concepteurs ont malgré tout préféré rajouter cette dépendance plutôt qu'implémenter la logique par eux-mêmes : le mois qui a précédé son arrêt, *left-pad* avait été installé environ 2 500 000 fois, et était utilisé dans des milliers de composants en sources ouvertes, eux-mêmes potentiellement vastement utilisés. Cet exemple est emblématique des risques portés par les dépendances transitives : *left-pad* était nécessaire pour babel, composant extrêmement populaire, qui lui-même était nécessaire pour React Native, lui aussi extrêmement populaire. Ce type de chaîne de dépendances, ici raccourcie, provoque une exponentiation de la surface d'impact : d'autres projets vastement utilisés comme ember ou atom ont également été touchés. La reprise des activités n'a pas été longue après cet incident car *left-pad* était un composant extrêmement simple (il n'était composé que de 11 lignes de code), mais le champ d'action révélé a néanmoins causé une véritable prise de conscience sur la maîtrise des projets informatiques et sur le savoir-faire dont il faut faire preuve vis-à-vis de leur code source.

Portes dérobées

Un autre risque lié aux dépendances logicielles est plus axé sur la sécurité informatique, dans la mesure où, lui, découle réellement d'une volonté hostile et impacte plus facilement la confidentialité. Il s'agit de l'insertion active de portes dérobées, réutilisées et importées dans les projets par les concepteurs, à leur insu. Celles-ci donnent secrètement à des acteurs malveillants un accès privilégié à des ressources dont l'accès est normalement restreint.

Les chaînes de dépendance pouvant être particulièrement longues et pouvant contenir un large nombre de branches, un composant élémentaire compromis peut obtenir à sa disposition un grand terrain d'action. On peut alors assimiler un tel risque à celui d'une ingérence logicielle. Lorsqu'une telle tentative est découverte, une course contre la montre

[2] Glass R. L. (2001), "Frequently Forgotten Fundamental Facts about Software Engineering", *IEEE Software*, n°3.

est lancée pour identifier toute présence de la brique logicielle compromise parmi toutes celles sollicitées dans un projet, et pour appliquer un correctif complet.

La tentative d'attaque autour de XZ Utils est emblématique de cette problématique et aurait certainement pu être la plus impactante à l'échelle mondiale si elle avait été menée à son terme. En 2024, Andres Freund, ingénieur au sein de Microsoft, a détecté des performances inhabituelles exhibées par son serveur SSH lors des authentifications de clients. En enquêtant sur la source de ce problème, il a découvert que XZ Utils, importé par la suite logicielle systemd, elle-même importée par le serveur SSH, influençait la vérification de certificat de ce dernier, sans raison légitime évidente. La suite des recherches a exposé un mécanisme complexe donnant à l'attaquant un vecteur menant potentiellement à un accès non autorisé ou à une exécution de code arbitraire. Ce montage, inédit par son mode opératoire et son ampleur visée, a été découvert prématurément, et n'a pas eu le temps d'atteindre les versions dites stables des distributions logicielles. Il a néanmoins soulevé de nombreuses interrogations sur la propagation voire la facilitation des portes dérobées par l'utilisation insouciante des dépendances logicielles. Une vaste réflexion a également eu lieu sur les conditions de développement des logiciels en sources ouvertes, et la viabilité de celles-ci. En effet, le processus d'attaque décrit est le résultat d'environ deux ans de manipulation sociale du seul développeur de XZ Utils, Lasse Collin, par un autre développeur malicieux, inconnu mais prétendument appelé Jia Tan. Lasse Collin peinant à soutenir le projet, et souffrant d'après ses propres termes de problèmes de santé mentale à long terme, s'est trouvé dans une situation douloureuse où il était plus susceptible d'accepter une main tendue.

Dépendances d'utilisation

Une fois un logiciel compilé, livré et installé, celui-ci peut avoir des dépendances envers d'autres logiciels durant l'utilisation. En utilisant une interface de programmation applicative *via* un système de communication inter-processus ou *via* des communications réseau, ce type de sollicitation a lieu de manière parfaitement intégrée, mais de façon plus ou moins transparente pour l'utilisateur.

L'enjeu de collaboration entre programmes locaux a acquis une importance majeure dès les années 2000 : c'est à cette période que les systèmes d'exploitation ont commencé à mettre en avant des mécanismes de communication inter-processus plus intelligents, pour répondre à la demande. Sur Linux, afin de disposer davantage de flexibilité que celle offerte par les simples sockets UNIX et les tubes nommés (pipes), on verra apparaître durant cette décennie D-Bus pour les serveurs ainsi que l'informatique bureautique, et Binder pour les téléphones fonctionnant sous Android, chacun motivés par les contraintes techniques associées à leur plateforme.

Sur le réseau, la normalisation de Common Gateway Interface (CGI), qui s'est étalée du début des années 1990 au milieu des années 2000, démontre le besoin associé : pouvoir appeler des instances de logiciels tiers potentiellement extrêmement éloignées géographiquement, avec des paramètres arbitraires, pour recevoir un résultat dynamique. Au-delà de CGI, ce paradigme s'imposera en ligne, en lieu et place du *web* classique dit « statique ».

Les risques associés aux dépendances logicielles lors de l'utilisation sont analogues à ceux des dépendances lors du développement, mais varient d'une certaine manière. Si l'on retrouve rarement des chaînes de dépendances hors de contrôle à l'utilisation, les développeurs peuvent malgré tout accuser un manque de compréhension et de maîtrise vis-à-vis de la logique de l'application globale. Ils doivent tout autant suivre les versions de leurs dépendances. Le problème de la disponibilité est cependant accru à l'exécution des logiciels : en plus de devoir s'assurer que toutes les dépendances sont toujours suivies et entretenues dans de bonnes conditions, il faut également veiller à leur maintien en exécution, puisqu'une erreur interrompant même temporairement leur fonctionnement

aura un impact sur le maintien du service. Le risque de porte dérobée est moindre dans la mesure où les dépendances ne retournent habituellement que des résultats d'opérations, mais peut avoir lieu dans des contextes cryptographiques ou lorsque que des exécutables sont retournés.

L'utilisation de dépendances logicielles sur internet, à l'exécution, présente un ensemble d'enjeux non techniques, mais juridiques et commerciaux. Le caractère international d'internet et la suppression des distances qu'il instaure facilite ces sollicitations logicielles entre entités de divers pays, ce qui s'assimile alors à une vente transfrontalière de service, impliquant ainsi les contraintes légales et réglementaires afférentes.

Conclusion

S'appuyer sur des composants logiciels tiers, que ce soit lors du développement ou lors de l'utilisation, permet de bénéficier d'une flexibilité accrue, et cette pratique a sans conteste été un vecteur de croissance considérable du secteur informatique. Il aura cependant fallu attendre plusieurs incidents techniques majeurs récents, ainsi qu'une reconfiguration géopolitique mondiale inédite pour une prise en compte profonde des risques associés. La connaissance exhaustive des dépendances d'un logiciel, caractérisée par la Software Bill of Materials (SBOM), devient de plus en plus une obligation légale. Un premier pas a été franchi par la Maison Blanche en 2021 avec son ordre exécutif numéro 14028, l'imposant à toute entité fournissant un logiciel au gouvernement fédéral. En Europe, le Cyber Resilience Act développe depuis 2024 cette même exigence, mais dans un champ plus large que celui des gouvernements : celui du marché européen dans sa globalité.

Transition post-quantique : état des lieux 10 ans après l'annonce choc de la NSA

Par Simon ABELARD
Enseignant-chercheur à l'EPITA
(École pour l'Informatique et les Techniques avancées)

Et Ludovic PERRET
Professeur à l'EPITA

Si l'on sait depuis 1994 que l'ordinateur quantique menace les méthodes de chiffrement actuelles, cette menace ne s'est véritablement matérialisée qu'en 2015 à l'appel d'institutions américaines telles que la NSA et le NIST. Dix ans plus tard, il est temps de faire un bilan sur la réalité de la menace quantique, sur les efforts mis en place des deux côtés de l'Atlantique et sur le chemin qu'il reste à parcourir. À première vue, on pourrait craindre que l'Europe soit en retard sur le sujet mais nous proposons une analyse plus fine des forces et des faiblesses du Vieux Continent.

Remerciements
Les auteurs souhaitent remercier Christopher Bonnelly pour sa lecture attentive et ses remarques sur l'article, ainsi que Daniel Boula et Grégoire Postel-Vinay pour leurs commentaires.

Introduction

L'année 2025 marque le début de la transition à grande échelle des infrastructures numériques vers une cryptographie de nouvelle génération, dite cryptographie post-quantique (Fouque, Lafourcade et Perret, 2026), conçue pour résister aux attaques quantiques.

Cette transition s'amorce exactement dix ans après une annonce de la NSA (National Security Agency) américaine, publiée[1] pendant l'été 2015. Les progrès des ordinateurs quantiques remettraient en cause la sécurité à long terme des algorithmes cryptographiques à clé publique classiques, tels que le protocole d'échange de clés de Diffie-Hellman ou le chiffrement RSA.

L'annonce est surprenante et son impact potentiellement colossal puisque la sécurité d'Internet et des communications numériques reposent en grande partie sur ces deux cryptosystèmes, massivement déployés à l'échelle mondiale depuis les années 1980.

Depuis les travaux de Peter Shor (Shor, 1994), nous savons que les ordinateurs quantiques pourraient théoriquement casser ces deux problèmes mathématiques, la factorisation des

[1] https://arstechnica.com/information-technology/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/

grands entiers et le calcul du logarithme discret, sur lesquels reposent respectivement la sécurité de RSA et de Diffie-Hellman. Certes, les résultats de Shor rendent obsolètes les mécanismes de sécurité classiques, mais cette menace, connue de longue date, n'était pas perçue comme critique en raison des capacités très limitées des ordinateurs quantiques de l'époque.

Malgré tout, cette annonce de la NSA a déclenché une mobilisation internationale impliquant, entre autres, des organismes de normalisation, des agences de sécurité, et de nombreux acteurs du monde académique et industriel.

Le résultat le plus visible est le processus de normalisation de la cryptographie post-quantique (Chen *et al.*, 2016) entamé en 2016 par l'institut américain NIST (National Institute of Standards and Technology). Ce processus s'est achevé en 2025 avec la normalisation de cinq nouveaux algorithmes divisés en deux catégories : l'échange de clés, avec deux algorithmes, et la signature, avec trois algorithmes.

Ces algorithmes reposent sur des problèmes et principes mathématiques différents de ceux de RSA et de Diffie-Hellman. Les réseaux euclidiens, les matrices et les polynômes y remplacent les groupes finis, courbes elliptiques et entiers modulaires. En revanche, ces nouveaux cryptosystèmes s'utilisent de la même manière que les anciens, et l'utilisateur final n'y verra (presque) aucune différence.

Les contributions françaises et européenne au processus post-quantique du NIST sont remarquables : quatre des cinq algorithmes normalisés par le NIST ont été co-inventés par des chercheurs travaillant dans des écoles d'ingénieurs ou des universités françaises. Ce pourcentage atteint même 100 % lorsque l'on inclut les contributeurs issus d'institutions européennes. Les travaux préliminaires ayant conduit à ces résultats ont souvent été financés par des fonds publics, notamment par le biais de l'ANR (Agence Nationale pour la Recherche), de BPI France et de fonds européens dédiés à la recherche et à l'innovation.

Dix ans après l'annonce de la NSA, cet article propose un bilan de l'état actuel de la menace quantique, aborde les prochains défis de la cryptographie post-quantique et propose une mise en perspective des stratégies européenne et américaine dans ce domaine. L'Europe sera-t-elle au rendez-vous de la transition post-quantique ?

Menace quantique sur la cryptographie

Si, en 2015, la menace quantique semblait encore lointaine, voire relever de la science-fiction, les progrès accomplis ces dernières années dans le développement des ordinateurs quantiques sont impressionnants : revendication de la « suprématie quantique[2] » par Google en 2019, progrès constants d'IBM, qui suit une feuille de route technologique rendue publique depuis plusieurs années[3], et machines aux capacités croissantes à travers le monde, notamment en Australie, au Canada, en Chine, au Japon, au Royaume-Uni, aux États-Unis, et en Europe, qui n'est pas en reste dans cette course technologique. En 2025, la Commission européenne recensait 39 *start-ups* cherchant à construire un ordinateur quantique (Com, 2025), dont 4 en France.

Un moyen simple d'évaluer les capacités de calcul d'un ordinateur quantique est de compter le nombre de *qubits*, l'équivalent quantique du bit classique. Ce seul critère ne suffit pas à rendre compte de la puissance réelle des machines quantiques actuelles. En effet, les *qubits* sont extrêmement sensibles aux perturbations, ce qui engendre des erreurs et limite leurs performances.

[2] https://www.nature.com/articles/s41586-019-1666-5

[3] https://www.ibm.com/quantum/technology#roadmap

Il convient alors de distinguer les *qubits* dits « logiques », qui sont des *qubits* théoriquement parfaits et auto-corrigés, des *qubits* « physiques », qui, eux, sont sujets à des erreurs et possèdent un temps de cohérence (la durée avant que les erreurs ne se produisent) limité. Habituellement, les communications reliées à la puissance des ordinateurs quantiques correspondent aux *qubits* logiques.

Cependant, une augmentation du nombre de *qubits* logiques n'implique pas nécessairement une amélioration des capacités de calcul. Par exemple, la feuille de route d'IBM annonce 120 *qubits* pour 2025, alors qu'une machine de 156 *qubits* était déjà disponible dès 2024. Après une première phase dédiée à l'augmentation du nombre de *qubits* (par exemple, 5 *qubits* en 2016), IBM semble désormais se concentrer sur l'amélioration de la qualité plutôt que de la quantité[4]. Le nombre de *qubits* est une mesure d'autant plus imparfaite qu'il existe de multiples technologies présentant chacune des avantages et des inconvénients, de sorte que tous les *qubits* ne se valent pas.

Briser la sécurité des algorithmes cryptographiques déployés actuellement nécessiterait la construction d'un ordinateur quantique de grande capacité, doté d'un nombre bien plus élevé de *qubits*. À titre d'exemple, examinons les ressources nécessaires pour factoriser un entier RSA-2048, une clé RSA de 2 048 bits, taille typique de paramètre utilisé en pratique. Avec des machines classiques, il faudrait mobiliser des milliers de supercalculateurs pendant plusieurs siècles pour casser RSA-2048. Ce même calcul ne prendrait que quelques minutes sur une machine quantique, à condition de disposer de 1 399 *qubits* logiques.

En l'état actuel des connaissances, il faudrait environ 1 million de *qubits* physiques pour réaliser ce calcul en quelques heures (Gidney, 2025). Cette dernière évaluation prend en compte des progrès dans l'amélioration de la qualité des *qubits* (Google AI *et al.*, 2024), mais surtout des avancées algorithmiques récentes sur l'algorithme de Shor (Chevignard, Fouque et Schrottenloher, 2024) qui ont permis de réduire significativement les ressources nécessaires pour effectuer ce même calcul. En effet, en 2019, les auteurs (Gidney et Ekerå, 2021) estimaient qu'environ 20 millions de *qubits* logiques seraient nécessaires pour casser RSA-2048.

La marge de progression reste donc encore très significative avant d'obtenir une machine quantique capable de briser la cryptographie actuelle. Cependant, les progrès réalisés ces dernières années sont considérables, tant sur le plan matériel qu'algorithmique.

Au-delà de ces aspects scientifiques et technologiques, les investissements réalisés à travers le monde pour la construction d'un ordinateur quantique de grande capacité sont importants et s'élèvent à plusieurs milliards en Europe, en Chine ou aux États-Unis. Au niveau national, le programme PROQCIMA[5], porté par le ministère des Armées et France 2030, est doté d'un budget de 500 millions d'euros et ambitionne de construire un ordinateur quantique de 128 *qubits* logiques en 2032 et 2 048 *qubits* logiques en 2035, machine qui serait notamment capable de briser RSA-2048.

Ces objectifs sont ambitieux et montrent que l'incertitude ne porte pas tant sur la capacité à construire une machine de grande envergure que sur le délai nécessaire pour y parvenir. Le rapport très complet du BSI (2024), l'agence de sécurité allemande, estime, d'une part, que l'arrivée d'un ordinateur quantique de grande capacité interviendra au plus tard en 2040 et, d'autre part, que la plupart des obstacles techniques ont été levés en 2024.

[4] Le lecteur intéressé par des précisions pourra consulter le très complet et détaillé panorama des technologies quantiques (Ezratty, 2024).

[5] https://quantique.france2030.gouv.fr/acces-aux-marches/programme-proqcima/

Cette menace peut malgré tout sembler lointaine, mais elle pèse déjà sur les communications les plus sensibles. En effet, il est d'ores et déjà possible de capturer et de stocker des données chiffrées à grande échelle, en attendant qu'un ordinateur quantique suffisamment puissant soit disponible pour en révéler les secrets. Les objets connectés à longue durée de vie, comme les voitures connectées, les avions, les satellites ou les systèmes d'armes modernes sont également concernés. Déployés pour plusieurs décennies, ils ne disposent souvent d'aucun moyen simple permettant de mettre à jour leurs composants cryptographiques.

Une stratégie américaine constante et structurée

L'objectif de transition vers le post-quantique fixé par la NSA en 2015 n'a pas bougé au fil des années et s'est structuré autour de trois grandes phases. Le processus de normalisation du post-quantique du NIST, mentionné dans l'introduction, constitue la première étape qui s'est achevée en 2025. Cela ne signifie pas pour autant que les activités de normalisation post-quantique sont terminées. Elles se poursuivent sous d'autres formes au sein d'organismes comme l'ETSI, l'IETF ou l'ISO, principalement pour intégrer les normes du NIST dans divers protocoles de sécurité à l'échelle mondiale.

La deuxième phase, officiellement démarrée en 2023, consiste à accompagner les industriels dans la transition post-quantique. Cet accompagnement prend la forme d'un partenariat public-privé au sein du NCCoE[6], laboratoire du NIST qui rassemble plusieurs agences américaines et des acteurs industriels. Dès aujourd'hui, les acteurs américains affichent un niveau de maturité élevé, puisque des entreprises comme AWS, Apple, ou Google ont intégré des solutions post-quantiques dans certaines de leurs offres grand public (navigateur Chrome post-quantique, iMessage post-quantique, ou plateforme d'accès post-quantique au *cloud* AWS). Ces acteurs ne représentent certes pas l'intégralité du paysage économique américain, mais il est indéniable que leur poids suffit à tirer tout l'écosystème vers le haut.

La troisième phase concerne la régulation, avec une loi fixant à 2035 la date limite pour la transition des infrastructures numériques publiques vers le post-quantique (WH, 2025), un schéma de certification des produits de cybersécurité adapté au post-quantique (CMVP, FIPS 203/204) et la dépréciation programmée des normes non résistantes aux attaques quantiques d'ici 2035. Dans (Moody *et al.*, 2025), le NIST indique que des algorithmes comme RSA et Diffie-Helmman ne seront plus acceptés après 2035.

L'Europe à l'heure du post-quantique ?

Malgré l'excellence scientifique de ses chercheurs et de ses universités, l'Europe a quelque peu tardé à se saisir des problématiques politiques et organisationnelles liées à la transition vers la cryptographie post-quantique. On peut, par exemple, s'interroger sur l'absence de contrepartie européenne à la campagne de normalisation du NIST, *a fortiori* quand d'autres acteurs comme la Chine et la Corée du Sud ont lancé leurs propres campagnes.

La France est partie prenante des travaux en cours sur la normalisation du post-quantiques et s'implique activement dans des organismes comme l'IETF, l'ETSI ou lISO, notamment par l'intermédiaire de l'AFNOR, qui coordonne les contributions des acteurs français. Cependant, cette stratégie d'influence reste bien moins développée que celles

[6] https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

déployées par les Américains, les Britanniques ou les Chinois, qui y consacrent des moyens considérables. Cet état de fait n'est pas anodin car l'adoption ou la non-adoption de normes peut se révéler très impactante pour les industriels.

Le constat est similaire au niveau de l'Union européenne. Pour autant, il serait faux de croire que l'Europe n'a rien fait en la matière : scientifiquement parlant, l'Europe n'a pas tardé, puisqu'elle a lancé, entre autres, les projets de recherche ECRYPT-CSA[7] et PQCRYPTO[8] dès 2015, projets qui seront suivis par de nombreux autres. Il est également important de noter que les universitaires se sont saisis du problème en intégrant très rapidement les enjeux du quantique dans les formations, comme la majeure quantique de l'EPITA[9], les masters d'informatique quantique de Sorbonne Université (QI[10]), l'Institut Polytechnique (QMI[11]), etc. L'Europe anticipe également la question des normes puisque l'ETSI a créé un groupe dédié au post-quantique qui produit régulièrement des spécifications.

Dès 2021, l'ENISA a rédigé des rapports sur la cryptographie post-quantique (D'Anvers *et al.*, 2021 ; Bernstein *et al.*, 2022) et sur son intégration (performances, protocoles, hybridation, normalisation). Ces rapports sont cependant essentiellement techniques et ne contiennent que peu de recommandations. Peu après, les agences française et allemandes (ANSSI 22 ; Ehlen *et al.*, 22) ont publié des recommandations sur le choix des algorithmes cryptographiques et plus généralement sur la transition vers le post-quantique. Si on peut saluer le fait que les deux agences partagent une vision très similaire, il n'est pas encore question à l'époque de position commune à l'échelle européenne.

Il faudra attendre avril 2024 pour que la Commission européenne publie une recommandation (EC, 2024) suivie en 2025 d'une feuille de route concernant la transition vers le post-quantique (NIS, 2025) dont les principes fondamentaux sont les suivants :

- Jalons : travaux initiés, et feuille de route de transition post-quantique avant fin 2026 par les agences nationales, transition effectuée avant 2030 pour les applications sensibles et avant 2035 pour les autres applications.
- Modalités : opter pour des solutions hybrides et garantir la crypto-agilité, c'est-à-dire la possibilité de changer d'algorithme cryptographique sans modification du matériel ou des protocoles. Ces deux exigences visent à anticiper l'éventualité qu'un algorithme post-quantique soit cassé (cela s'est produit lors de la campagne du NIST), ou que son implémentation ne soit pas sûre.
- Écosystème : s'assurer que l'Europe dispose de formations de haut niveau en cryptographie post-quantique, définir des critères communs pour la certification de la cryptographie post-quantique et pour l'évaluation du risque quantique, et se doter d'un organe de communication concernant l'impact du quantique.

Cette publication un peu tardive d'une feuille de route illustre que les défis de la transition ne résident pas seulement dans les aspects technologiques, mais aussi dans les dimensions organisationnelles – avec notamment un besoin crucial de coordination (QSFF, 2024 ; Perret et Ribordy, 2025) entre de nombreux acteurs (agences de sécurité, acteurs de la normalisation, régulateurs, industriels, académiques, etc.).

[7] https://cordis.europa.eu/project/id/645421/reporting

[8] https://pqcrypto.eu.org/

[9] https://www.epita.fr/ecole-ingenieurs/informatique-et-technologies-quantiques/

[10] https://qics.sorbonne-universite.fr/formation/programme-de-master

[11] https://quriosity.telecom-paris.fr/qmi/courses.html

À l'échelle industrielle, si les géants de la tech américaine n'ont pas attendu pour être proactifs dans le développement et la transition vers des solutions post-quantiques, les grands industriels européens ne se sont pas encore suffisamment saisis du sujet, à l'exception notable des acteurs visant le marché de la défense ou celui des opérateurs d'importance vitale. On peut citer par exemple Atos et Thales qui ont tous les deux annoncé des versions de leurs modules de sécurité (HSM) supportant les algorithmes post-quantiques standardisés par le NIST.

On peut nuancer ce constat en remarquant le nombre important de *start-ups* proposant des services ou des bibliothèques logicielles pour soutenir la transition vers le post-quantique. Ces acteurs ont une expertise solide et reconnue, mais il est toutefois peu probable que leur petit nombre suffise à couvrir les énormes besoins du marché européen.

Dans la transition vers le post-quantique, l'Europe peut compter sur ses nombreux experts mais il est désormais temps pour elle de transformer l'essai en développant une politique industrielle (D'Auria *et al.*, 2025) aussi claire, harmonieuse et volontariste que celle menée outre Atlantique. S'il ne faut pas s'alarmer de l'absence de campagne de normalisation européenne analogue à celle du NIST, il faut s'assurer que les acteurs européens publics et privés auront des lignes de conduite claires et un accompagnement suffisant pour les mettre en œuvre.

Cela motive certaines institutions européennes à promouvoir des actions sectorielles afin de mettre en place des stratégies adaptées, c'est par exemple le cas dans le secteur financier avec la mise en place, par Europol en 2024, du Quantum Safe Financial Forum (QSFF, 2024), une initiative qui va au-delà des frontières européennes puisqu'elle regroupe également des acteurs britanniques et américains. À plus long terme, il serait souhaitable que l'Europe reprenne un rôle de leader en lançant des travaux de normalisation des protocoles cryptographiques. De nombreuses opportunités restent à saisir dans le domaine : 5G, 6G, standards du CCSDS dans le spatial, etc.

Enfin, le volontarisme américain dans le domaine du post-quantique contraste fortement avec leur peu d'engouement pour la cryptographie quantique. Pourtant, cette dernière offre une approche alternative, permettant en théorie de garantir une sécurité inconditionnelle face aux attaques d'un ordinateur quantique. En revanche, la cryptographie quantique nécessite la mise en place d'une nouvelle infrastructure et se heurte encore à des limitations fortes (absence d'authentification, distance limitée, forte dépendance au matériel employé, faiblesse face aux dénis de service, etc.) soulignées par la NSA et également par plusieurs agences européennes (ABNS, 2024).

Cependant, cela laisse pour le moment une place pour un écosystème quantique européen, avec notamment l'initiative EuroQCI[12] menée par la Commission européenne qui regroupe à la fois des infrastructures terrestres et spatiales. Malgré la relative absence des États-Unis dans ce domaine, la concurrence sera rude, principalement avec la Chine, qui bat de nombreux records et fait figure de *leader* dans le domaine. L'espoir est toutefois permis car l'Europe a pleinement compris que la révolution quantique est un tournant historique dans la compétition économique et géostratégique mondiale, comme en témoigne l'axe quantique du projet EuroHPC[13] Joint Undertaking visant à exploiter des puces quantiques dans le domaine des supercalculateurs et le "Quantum Act" actuellement en préparation (Com, 2025).

[12] https://digital-strategy.ec.europa.eu/fr/policies/european-quantum-communication-infrastructure-euroqci

[13] https://www.eurohpc-ju.europa.eu/eurohpc-quantum-computers_en

Bibliographie

(ABNS, 2024) – ANSSI, BSI, NLNCSA, NCSA (2024), "Position paper on quantum key distribution", https://cyber.gouv.fr/actualites/uses-and-limits-quantum-key-distribution

(ANSSI, 2022) – AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (2022), "ANSSI views on the post-quantum cryptography transition", https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/

(Bernstein *et al.*, 2022) – BERNSTEIN D. J., HÜLSING A., LANGE T. & REKLEITIS E. (2022), "Post-quantum cryptography – Integration study", ENISA, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2824/151162

(BSI, 2024) – FEDERAL OFFICE FOR INFORMATION SECURITY, BSI (2024), "The status of quantum computer development", https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.html?nn=916616

(Chen *et al.*, 2016) – CHEN L., JORDAN S., LIU Y.-K, MOODY D., PERALTA R., PERLNER R. & SMITH-TONE D. (2016), "Report on post-quantum cryptography standards", NIST IR 8105, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

(Chevignard, Fouque & Schrottenloher, 2024) – CHEVIGNARD C., FOUQUE P.-A. & SCHROTTENLOHER A. (2025), "Reducing the number of qubits in quantum factoring", Crypto 2025, https://eprint.iacr.org/2024/222

(Com, 2025) – COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL (2025), "Quantum Europe strategy: Quantum Europe in a changing world", COM (2025), 363 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0363

(D'Anvers *et al.*, 2021) – D'ANVERS J.-P., HÜLSING A. LANGE T., PANNY L., DE SAINT GUILHEM C. & SMART N. P. (2021), "Post-quantum cryptography – Current state and quantum mitigation", ENISA, Publications Office of the European Union, https://data.europa.eu/doi/10.2824/92307

(D'Auria *et al.*, 2025) – D'AURIA V., CHRISTOFI M., EALET F., FUNKE J.-F., KÉNANIAN G., LOIDREAU P., LAURENT E., PERRET L., SENOT O., TELLER M. & VILLARD A. (2025), « Cryptographie post-quantique : quelle stratégie industrielle ? », *Dalloz IP/IT*.

(EC, 2024) – COMMISSION RECOMMENDATION (EU) 2024/1101 (2024), "Recommandation on a coordinated implementation roadmap for the transition to post-quantum cryptography", https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

(Ehlen *et al.*, 2022) – EHLEN S, HAGEMEIER H, HEMMERT T, KOUSIDIS S, LOCHTER MANFRED, REINHARDT S. & WUNDERER T. (2022), "Quantum-safe cryptography – fundamentals, current developments and recommendations", https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4

(Ezratty, 2024) – EZRATTY O. (2024), "Understanding quantum technologies 2024", https://www.oezratty.net/wordpress/2024/understanding-quantum-technologies-2024/

(Fouque, Lafourcade & Perret, 2026) – FOUQUE P.-A., LAFOURCADE P. & PERRET L. (2026), *Cryptographie Post-Quantique*, Dunod (à paraître).

(Gidney et Ekerå, 2025) – GIDNEY C. & EKERÅ M. (2021), "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", *Quantum*, Vol. 5, https://arxiv.org/abs/1905.09749

(Gidney, 2025) – GIDNEY C. (2025), "How to factor 2048 bit RSA integers with less than a million noisy qubits", ePrint arXiv:2505.15917, https://arxiv.org/abs/2505.15917

(Google AI *et al.*, 2024) – GOOGLE QUANTUM AI & COLLABORATORS (2025), "Quantum error correction below the surface code threshold", *Nature*, Vol. 638, https://www.nature.com/articles/s41586-024-08449-y

(Moody *et al.*, 2025) – MOODY D., PERLNER R., REGENSCHEID A., ROBINSON A. & COOPER D. (2024), "Transition to post-quantum cryptography standards", NIST IR 8547, https://doi.org/10.6028/NIST.IR.8547.ipd

(NIS, 2025) – NIS COORDINATION GROUP (2025), "A coordinated implementation roadmap for the transition to post-quantum cryptography", https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

(Perret et Ribordy, 2025) – PERRET L. & RIBORDY G. (2025), "Accelerating the transition to quantum-safe communication: A call for global collaboration and action", Policy brief, G7 Kananaskis, Think7 Canada 2025, https://www.think7.org/publications/accelerating-the-transition-to-quantum-safe-communication-a-call-for-global-collaboration-and-action/

(QSFF, 2024) – EUROPEAN CYBERCRIME CENTRE (EC3), EUROPOL (2024), "Quantum safe financial forum: a call to action", doi:10.2813/5052685, https://www.europol.europa.eu/publications-events/publications/quantum-safe-financial-forum-call-to-action

(Shor, 1994) – SHOR P. W. (1994), "Algorithms for quantum computation: Discrete logarithms and factoring", FOCS 1994.

(WH, 2025) – WHITE HOUSE (2025), "National security memorandum on promoting United States leadership in quantum computing while mitigating risks to vulnerable cryptographic systems", https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

Les enjeux cyber liés aux victimes

Par Jérôme MOREAU
Vice-président et porte-parole de la Fédération France Victimes

Dans un monde de plus en plus traversé par l'utilisation des outils numériques, force est de constater que notre société doit faire face à de nombreuses sources d'insécurité et d'infractions pénales. L'ampleur du phénomène, tant sur le plan économique, psychologique, humain que sociétal et social, doit conduire à promouvoir un accompagnement des victimes de manière pluridisciplinaire, personnalisée et adaptée. Les cyberattaques ont plusieurs buts : usurper les identités et données personnelles, obtenir illicitement de l'argent, ou encore commettre des atteintes de nature sexuelle.

Le réseau France victimes, composé de 130 associations métropolitaines et ultramarines, a su s'adapter pour parvenir à ce que chaque victime ne reste jamais seule. L'expertise, forgée depuis presque une dizaine d'années par l'accueil et l'accompagnement des victimes, porte à croire qu'il convient d'appréhender avec justesse les conséquences des séquelles subies par nos concitoyens, afin de mieux les aider à traverser ces violations de la loi pénale.

Victor Hugo écrivait
« sans cesse le progrès, roue à double engrenage,
fait marcher quelque chose en écrasant quelqu'un ».

Dans le cadre du développement irréversible d'une société gouvernée par l'avancée du numérique, c'est bien ce redoutable constat auquel nous sommes confrontés. Plus que jamais, l'intensification du numérique et l'avancée grandissante des possibilités du cybermonde dessinent, au fil du temps, des défis considérables et souvent néfastes : la commission d'infractions pénales inimaginables jusqu'alors.

Depuis plusieurs années, nous voyons inexorablement émerger un nouveau vecteur d'infractions pénales, à savoir celui lié à l'utilisation abusive et dangereuse des outils et dispositifs numériques, infractions dont l'appréhension a été largement sous-estimée au départ, dont l'intensité des préjudices n'a initialement pas été réellement évaluée, et dont les conséquences peuvent devenir dramatiques, tant elles touchent l'ensemble de nos concitoyens dans les différents aspects de leur vie.

En effet, tous utilisent au quotidien leurs outils numériques, que ce soit pour effectuer des démarches administratives, des achats sur des sites de vente, par le biais des réseaux sociaux, des courriels électroniques, des paiements en ligne *via* des applications diverses, le tout au moyen d'ordinateurs, *smartphones* ou tablettes.

En somme, notre vie quotidienne est gouvernée par la facilité et l'usage intense du numérique qui a envahi nos espaces, même les plus privés. À l'essor d'un monde virtuel idéalisé et infini, s'oppose l'apparition immédiate des victimes d'un réel harassant.

L'actualité et les médias font état d'un nombre important de victimes : 348 000 crimes et délits considérés comme liés au domaine numérique en 2024[1]. Ainsi, aucune catégorie de personnes, aucune structure, aucun citoyen n'est épargné (personnes physiques, entreprises, associations, établissements publics, tous sont concernés).

Désormais, une nouvelle catégorie de victimes est apparue : celle des victimes de cyberattaques.

La Fédération France Victimes[2], comme de nombreux acteurs de l'aide aux victimes, a bien évidemment compris qu'il convenait d'assurer un accompagnement des personnes touchées par ces cyber-infractions, d'autant plus que les préjudices sont protéiformes et ont des conséquences particulièrement dramatiques.

Dotées d'un agrément ministériel, les associations du réseau France Victimes œuvrent à l'accompagnement de toutes les personnes victimes, de manière pluridisciplinaire, avec des juristes, des psychologues, des travailleurs sociaux, de façon gratuite et confidentielle. Le réseau France Victimes est partenaire notamment des forces de police et de gendarmerie, des tribunaux et du ministère de la Justice. Pour adapter toujours mieux les réponses à apporter aux cyber-victimes, France Victimes est également devenue membre, fin 2017, du dispositif national d'assistance aux victimes de cybermalveillance, piloté par le Groupe d'Intérêt Public (GIP) ACYMA[3].

En effet, pour apporter aide et soutien à ces victimes, il est impératif qu'elles dénoncent les faits, qu'elles soient identifiées, afin qu'elles puissent non seulement recevoir l'information relative à leurs droits, mais plus encore, que les préjudices qu'elles subissent puissent être arrêtés voire réparés.

On se heurte, dans ce cadre à des réalités victimaires très diverses, souvent complexes, car dans nombre de situations, les infractions commises et les infracteurs sont disparates, parfois l'auteur est totalement inconnu, impossible à identifier, installé à l'étranger, alors que la victime est proche de nos structures associatives. Il faut alors l'accompagner.

On peut classer les victimes en trois catégories : celles qui seront atteintes économiquement, celles qui seront dépersonnalisées et celles qui seront déshumanisées.

Désargenter

On peut noter plusieurs caractéristiques concernant la situation des victimes en ligne : des extorsions de plus en plus agressives, une accélération des attaques, l'utilisation croissante de l'IA et une menace de plus en plus interne et proche.

120 milliards d'euros en France de préjudices économiques pour les victimes, dans toutes les dimensions, constituent des sommes jamais égalées selon l'agence STATISTA[4].

Entre 2018 et 2024, les demandes d'assistance des dispositifs gouvernementaux sont passées de 28 855 à 423 021. Si nous ne connaissons certainement pas la totalité des infractions commises sur le territoire, on relève une évolution de 18 % en 2024 des fraudes aux virements[5].

[1] Source : ministère de l'Intérieur, infractions liées au domaine numérique enregistrées par les services de sécurité en 2024, 13/08/2025.

[2] www.france-victimes.fr

[3] https://www.cybermalveillance.gouv.fr/

[4] STATISTA se définit comme un portail de statistique et de données de marché.

[5] Source : cybermalveillance.gouv.fr

Très vite, la question économique de l'escroquerie en ligne s'est imposée : l'escroquerie est aussi ancienne que le monde existe, mais aujourd'hui, ce qui change, c'est son ampleur.

Nous avons vu fleurir nombre de techniques ingénieuses de la part des auteurs d'infractions pénales qui ont permis le détournement d'argent et de données personnelles à une échelle particulièrement importante.

Ainsi, combien de personnes ont pu recevoir, par exemple, un SMS relatif à leur compte « Formation »[6], pour le paiement d'une amende en ligne[7], un courriel de la part de la caisse d'assurance maladie[8], des services fiscaux, un avertissement de réception d'un colis ou bien encore un chantage en ligne. Avec l'intelligence artificielle, la technique des infracteurs a évolué vers une efficacité et des difficultés de repérage de plus en plus redoutables.

Deux éléments particulièrement éclairants sont à noter sur ces nouvelles catégories de victimes :

- Le premier concerne la facilité avec laquelle les attaques se produisent, au moins en façade. Toutes les victimes, dans le processus d'escroquerie en ligne, nous livrent le même récit quant à la célérité des détournements et à l'impossibilité de s'apercevoir de l'infraction. Auparavant, nous étions habitués à des stratagèmes plus ou moins élaborés mais qui nécessitaient du temps ; désormais, nous sommes passés à un autre mode opératoire : celui de la rapidité. Ce constat choque particulièrement les victimes qui se sentent impuissantes et totalement dépassées par l'ingénierie utilisée. Dans l'univers de ces cyberattaques, on note aussi un découragement chez elles à déposer plainte, dû aux vicissitudes de la procédure pénale, pourtant simplifiée en la matière, qui leur semble rendre impossible toute poursuite ou indemnisation[9].
- Le second a trait au nombre de victimes touchées, ce qui implique deux conséquences : tout d'abord, accompagner tant de victimes suppose des moyens considérables avec des professionnels de plus en plus formés. De plus, les victimes peuvent se retrouver bien seules face à leur événement infractionnel, face à leur écran, objet initial du délit. Pour autant, les pouvoirs publics ont mis en place des moyens et dispositifs d'actions performants et des moyens humains très efficaces pour le signalement et la répression de ces infractions.

De là s'en dégagent trois grands constats concernant ces cyber-victimes :

- Le premier est en lien avec les difficultés persistantes qu'elles rencontrent pour déposer plainte : le processus de dépôt de plainte pour les victimes de cybermalveillance demeure souvent complexe. Nombreuses sont les victimes qui se heurtent encore à un refus de prise de plainte, bien qu'il s'agisse d'un droit fondamental[10]. Par ailleurs, il est fréquent qu'on les dirige systématiquement vers la plateforme THÉSÉE pour déposer une plainte en ligne, en affirmant qu'il s'agit de l'unique option. Or, cette démarche n'est qu'une alternative. Toute victime a parfaitement le droit de se rendre dans un commissariat ou une gendarmerie pour porter plainte, si elle le souhaite.

---

[6] Le 4 juin 2024, deux hommes ont été arrêtés pour avoir détourné à eux seuls 16 millions d'euros sur les comptes CPF, suite aux enquêtes diligentées par Tracfin et de l'Office national antifraude. Cette ampleur des détournements illustre le caractère sans précédent des cyberattaques.

[7] À cet égard, voir la publication de l'ANTAI du 18 octobre 2024, « Attention aux SMS, courriels et sites frauduleux ».

[8] Voir l'article publié dans *Ouest France*, le 14 février 2024, « CAF : 600 000 allocataires visés par un piratage ».

[9] Voir à cet égard, la création de la plateforme THÉSÉE pour le dépôt de plainte en ligne, le site PHAROS et les sites du gouvernement Cyber-malveillance ou ANSII.

[10] Article 15-3 du Code de procédure pénale.

- Le deuxième est lié aux suites des plaintes et aux aboutissements concrets qui demeurent très rares : malheureusement, en effet, de nombreuses plaintes sont classées sans suite, car les auteurs sont souvent inconnus, basés à l'étranger, rendant les enquêtes particulièrement difficiles. Les moyens d'investigation restent limités et, bien souvent, ne permettent pas d'aller au-delà de l'identification des fraudeurs.
- Il apparaît enfin essentiel d'évoquer le ressenti de ces victimes, avec un sentiment de culpabilité souvent prédominant, qui aggrave leur isolement : trop souvent, les victimes éprouvent un sentiment de honte, de culpabilité à s'être laissé piéger, ce qui tend à accentuer leur isolement social et à bloquer la libération de leur parole.

Le sentiment de culpabilité des victimes repose sur une donnée assez simple : en quoi ai-je contribué à ma propre infraction pénale et dans quelle mesure mon attitude constitue une faute de nature à atténuer la responsabilité de l'auteur ? Il faut impérativement renverser cette perception des victimes pour les inciter, quand elles se sentiront prêtes, à déposer plainte. C'est tout l'enjeu de l'accompagnement des victimes proposé par les associations France Victimes, afin qu'elles ne restent pas seules.

En cas de préjudice financier important, notamment en cas de transferts de sommes effectués sous l'influence des cybercriminels, il devient extrêmement difficile de récupérer l'argent perdu, faute de dispositifs efficaces. Cela implique dès lors une immunité de l'auteur et une absence de réparation de la victime ce qui, dans les deux cas, n'est aucunement satisfaisant.

Pour autant, la question de leur indemnisation est fondamentale et quand bien même différentes voies existent (selon les situations, assurances, fonds de garantie, remboursements par les organismes bancaires, constitution de partie civile, etc.), permettant l'activation de mécanismes de restauration économique, ces derniers sont perfectibles et gagneraient à être davantage effectifs pour plus de situations de cyber-infractions[11].

Usurper l'identité

Parmi les cyberattaques, on retrouve aussi les usurpations d'identité ou le vol des données personnelles, qui engendrent des conséquences graves pour les victimes, et dont les répercussions nécessitent des accompagnements spécifiques. La finalité de cette infraction pénale est simple : porter une atteinte à la personnalité des victimes, parfois de manière irrémédiable.

L'usurpation d'identité, qui peut sembler de nature simplement factuelle, constitue en réalité l'une des problématiques les plus complexes à résoudre. Elle impose un parcours juridique extrêmement difficile pour les victimes, qui, dans de nombreuses situations, se trouvent confrontées à des problématiques économiques, professionnelles, familiales et sociales dont l'issue apparaît impossible à surmonter.

Par usurpation en ligne, on trouve l'ensemble des attaques visant à porter atteinte à la réputation de la personne ciblée, mais aussi l'utilisation de données personnelles à des fins frauduleuses (souscription d'un prêt, piratage de compte et commission d'infractions pénales, souscription de bail, récupération de prestations, ouverture de services…).

Il en résulte une violation de l'identité, de l'intimité et de la vie privée, de la sécurité économique et financière de la victime, dans la mesure où un ensemble de données personnelles sont utilisées à des fins détournées.

[11] Sur les chiffres relatifs aux victimes d'escroquerie et d'usurpation, en 2024, les 130 associations du réseau France Victimes ont accueilli 13 320 victimes et, au niveau national, 10 277 victimes ont appelé nos services *via* la ligne d'écoute 116 006.

Les victimes d'usurpation d'identité indiquent être particulièrement démunies, bouleversées, en perte de repères identitaires. Même si l'usurpation en ligne constitue un délit[12], il n'en demeure pas moins que la loi ne peut pas venir au secours concret et immédiat de nombreuses victimes : il s'agit de reconstituer ce qui a été détruit, il faut restaurer ce qui a été détourné, ce qui n'est pas simple.

Cette problématique appelle une double réflexion :

- Premièrement, beaucoup de victimes éprouvent un sentiment légitime de dépossession, de dépersonnalisation, de retrait de toute forme de personnalité individuelle qui était pourtant la leur jusqu'à présent et qui était le fondement juridique et social de leur vie. Cette technique d'infraction pénale engendre un impact majeur sur la santé mentale et psychologique des victimes. Il ne faut pas sous-estimer l'impact également sur leurs proches qui se trouvent eux-mêmes impliqués, de fait, par cette usurpation.

Partant de là, il est impératif d'accompagner juridiquement, socialement et psychologiquement toutes les victimes, afin qu'elles soient de nouveau « réhabilitées » socialement et reconnues dans leur bonne foi.

- L'autre plan est en lien avec les difficultés à faire valoir leurs droits et à aboutir à la manifestation de la vérité dans un délai rapide et raisonnable. Même si la loi pénale protège, même si les différentes procédures peuvent être entamées, le défi est de rétablir les conséquences de ces usurpations. Les victimes se trouvent face à une lente inertie de la part des institutions et administrations, dans une situation où elles doivent prouver leur bonne foi, rétablir une vérité. Beaucoup d'entre elles indiquent que ce sont des efforts de plusieurs mois, voire des années, pour obtenir réparation ; humainement et psychologiquement, cela représente une épreuve redoutable.

Déshumaniser

Pour conclure sur la question des cyberattaques, il est impératif d'évoquer la question des infractions à caractère sexuel et des crimes à l'encontre des mineurs. L'arnaque aux sentiments a été largement évoquée dans la presse, faisant état d'une volonté d'exploitation de la tristesse, de la solitude et de la recherche de sentiments amoureux.

Nous observons également une criminalité organisée en matière de violences sexuelles sur mineurs : entre 2019 et 2023, nous notons une augmentation de 87 % des signalements de contenus d'abus sexuels en ligne où des mineurs sont impliqués[13]. D'ailleurs, la France s'est dotée en 2023 d'un nouveau service : l'Office Mineurs (OFMIN), afin de lutter plus efficacement contre les infractions sexuelles en ligne et la pédocriminalité.

Avec cette cybercriminalité, nous passons à une troisième dimension : celle de la réification des personnes, qui consiste à les transformer en objet, avec une finalité certes économique, mais aux conséquences humaines catastrophiques : viols en direct, vol de sentiments, images pédopornographiques en ligne, etc.

La restauration des victimes s'inscrit dans la durée, leur accompagnement suppose de les sécuriser, de leur prodiguer des soins et un soutien psychologique dans le cadre d'un parcours judiciaire et associatif renforcé et coordonné.

Encore une fois, ces infractions ne sont pas nouvelles, mais leur mode de diffusion et leur origine se singularisent avec ce que nous avions connu il y a plus de 20 ans.

[12] Article 226-4-1 du Code pénal (avec de possibles circonstances aggravantes).

[13] Source : CN2R, 11 septembre 2024.

Face à l'augmentation grandissante des victimes de cyberattaques, il nous appartient, à France Victimes, de leur apporter une réponse individualisée, en parallèle de l'action de la justice et des investigations menées. Nous avons le devoir, dans une société en pleine mutation, de rester vigilants et de protéger les plus vulnérables et l'ensemble des personnes qui sont touchées par une infraction en ligne. Ce qui unit toutes ces victimes, c'est que l'infraction pénale se produit par le truchement du numérique dont on nous vante, régulièrement, sa sécurité et sa performance. Au sein de France Victimes, nous voyons l'autre visage de ce Janus numérique : celui d'un monde qui fait de ses proies des victimes, dont l'accompagnement est indispensable.

Dans une société où les cas de cybermalveillance se multiplient, il devient aussi impératif que le gouvernement et les organismes spécialisés renforcent leurs actions en amont, en investissant davantage dans la prévention des actes de cybercriminalité.

L'adaptation de la gouvernance de la cybersécurité dans un grand groupe

Par Olivier LIGNEUL
EDF

La gouvernance de la cybersécurité s'est progressivement structurée sous l'effet de la montée des menaces et des exigences réglementaires. Initialement rattachée aux directions informatiques, elle a évolué vers une fonction stratégique, intégrant les dimensions opérationnelles, fonctionnelles et métiers. Les grands groupes adoptent différents modèles : tripartite, hybride, centralisé ou encore placée hors de la filière digitale pour garantir l'indépendance.

La gouvernance doit composer avec la complexité organisationnelle, les fusions/acquisitions, la diversité culturelle et réglementaire, mais aussi l'intégration des chaînes de valeur interconnectées. Elle se situe à la croisée des attentes des métiers, de la direction générale et des régulateurs, tout en devant concilier souveraineté, conformité et performance économique. La maturité recherchée repose sur une articulation fine entre stratégie, gestion des risques et pilotage opérationnel, afin d'inscrire la cybersécurité comme un levier durable de résilience et de compétitivité.

La gouvernance de la cybersécurité ne s'est organisée que récemment

La cybersécurité est un métier relativement récent, même vis-à-vis des autres domaines du monde numérique. Apparue dans le domaine des réseaux dans les années 1970, la cybersécurité était à l'époque principalement focalisée sur la confidentialité des informations. Son périmètre s'est ensuite étendu jusqu'à la première décennie des années 2000 aux notions de confidentialité, de traçabilité, d'intégrité et de disponibilité. Pour cette raison, les modalités de gouvernance ont été initialement intégrées à celles des directions informatiques puis des directions des systèmes d'information.

En France, c'est en 2010, face à une menace en plein essor et une Loi de programmation militaire (LPM) qui en a pris conscience, que la cybersécurité a pris corps, notamment au travers de la création de l'ANSSI, qui s'est rapidement affirmée comme l'autorité de référence et le *leader* incontesté de cette discipline, sous l'impulsion de Patrick Pailloux. Inscrits dans la même dynamique et face à une sinistralité grandissante, les grands groupes se sont également adaptés en créant, d'une part, la fonction de RSSI et, d'autre part, en intégrant la menace cyber parmi les risques principaux des entreprises.

D'abord considérée comme une activité technique sous l'égide d'un directeur informatique, la pratique de la cybersécurité s'est assez rapidement structurée au travers de différentes fonctions.

Organisation de la fonction de cybersécurité

La fonction « cyber » est impactée par la complexité de l'organisation des groupes

À l'instar des fonctions d'audit ou de contrôle, la cybersécurité occupe une place transversale au sein de l'entreprise. Un autre champ de complexité apparaît à travers les groupes qui s'appuient sur des principes de subsidiarité entre la tête du groupe et les différentes entités, pour des raisons évidentes de capacité à opérer.

Les groupes sont également très souvent répartis sur plusieurs zones géographiques, soumis à des réglementations locales, et leur appétence au risque est étroitement liée à la culture du pays. La rationalisation des activités de cybersécurité, au-delà des tâches élémentaires (gestion des vulnérabilités, maintien en conditions de sécurité et opérationnelles) doit prendre en compte ces différentes sensibilités. D'autant plus que certaines structures opteront pour une approche de conduite des risques, tandis que d'autres opteront plutôt pour une approche de conformité à des référentiels communs ou sectoriels.

Le modèle organisationnel doit également s'adapter au cycle de vie des groupes, en prenant en compte les évolutions de l'actionnariat des différentes filiales, les fusions et acquisitions, qui influencent directement les modalités de gouvernance de la direction générale. Au travers d'une sorte d'effet miroir, *a posteriori*, la cybersécurité doit s'adapter à ces différentes évolutions.

Les différents modèles organisationnels de la cybersécurité se sont stabilisés

On peut schématiquement considérer les modèles organisationnels autour de trois grandes catégories :

- modèle tripartite ;
- modèle hybride (filière) ;
- modèle en dehors des filières digitales.

Modèle organisationnel tripartite

Traditionnellement, la cybersécurité se partage au sein des organisations au travers de trois grandes fonctions :

- les équipes opérationnelles, en charge de la mise en œuvre des moyens de protection et de réponse à incident ;
- les équipes fonctionnelles, responsables du pilotage des processus et de la coordination des acteurs ;
- et enfin, les équipes déployées au plus près des métiers, occupant des fonctions de Responsable de la sécurité des SI (RSSI) et leurs homologues dans les entités industrielles (RSSII).

L'avantage de ce modèle réside dans sa capacité à consolider les moyens opérationnels, optimisant ainsi la couverture de la cybersurveillance et améliorant la réactivité face aux agressions. Cependant, il génère des tensions entre les acteurs opérationnels et ceux en charge du pilotage, ces derniers n'appartenant pas à la même structure. De même, les arbitrages et choix structurants en matière de cybersécurité demeurent complexes, car potentiellement divergents entre les intérêts propres des différents métiers et ceux, plus globaux, du groupe.

Modèle organisationnel hybride

Afin de s'affranchir les difficultés présentées dans le modèle précédent, il est possible de consolider les ressources opérationnelles, de pilotage et fonctionnelles au sein d'une seule structure centralisée. C'est le choix qui a été retenu par le groupe EDF dans le cadre de sa transformation numérique début 2025.

Ainsi, les processus de cybersécurité sont intégrés de bout en bout depuis la capacité opérationnelle jusqu'à celle du pilotage et interagissent avec les RSSI/RSSII au travers d'un modèle de filière, complémentaire à la structure managériale traditionnelle. L'autre avantage réside dans le fait que l'ensemble des ressources est consolidé en un seul endroit et peut, de ce fait être optimisé au sein d'un modèle économique plus lisible et performant.

Cependant, sous l'autorité d'un directeur exécutif Transformation et Efficacité Opérationnelle ou d'un directeur exécutif du Digital positionné au plus haut niveau de l'entreprise, il convient de s'assurer d'un maillage avec les fonctions de gouvernance du SI, les autres fonctions *corporate* (*risk management*, audit, direction financière, DRH) et les entités opérationnelles (opérateur IT).

Modèle où la cybersécurité n'est pas dans la filière digitale

Rattachement : Secrétariat général / Direction des risques / Direction financière

Afin de pouvoir assurer une indépendance de la cybersécurité vis-à-vis des acteurs du digital de l'entreprise, il peut être également envisagé d'opter pour un modèle où la cybersécurité rend compte au secrétaire général, à la direction des risques, voire directement à la direction générale. Ce modèle permet d'opter pour des choix qui pondèrent différemment l'équilibre entre la trajectoire technologique et les conséquences financières de l'évaluation de chacun des risques.

Siège faisant appel fortement à l'externalisation

D'autres groupes, très fortement décentralisés, ne souhaitent pas s'impliquer fortement dans certaines fonctions de support ou opérationnelles. Des approches d'externalisation complètes de la fonction cybersécurité peuvent être envisagées en faisant appel un acteur majeur à qui sera délégué la cybersurveillance, le maintien en conditions de sécurité et la réponse à incident.

Ce modèle impose de s'assurer que les fonctions *corporate* sont dotées d'une capacité de contrôle accrue afin de garantir que les différents acteurs, notamment au niveau de l'infogérance, restent conformes aux différentes réglementations applicables à l'entité.

La cybersécurité est désormais l'un des facteurs composant la performance des métiers

Les directrices et directeurs de la cybersécurité de groupe souffrent de schizophrénie... En effet, les activités opérationnelles des groupes s'appuient de plus en plus sur une fonction digitale qui leur est essentielle. Ainsi, il est nécessaire de trouver le juste milieu entre un soutien au métier qui n'impactera pas négativement la performance de son activité et produira des effets efficaces au niveau de sa protection. De plus, il faut éviter une banalisation de cette fonction à impact, qui, au fur et à mesure, voit s'écrêter la prise en compte des exigences de cybersécurité et affaiblit la résilience de la structure.

D'un point de vue plus pratique, il est nécessaire de se poser la question du positionnement des règles et de leur pertinence au regard de ce qu'elles vont apporter au niveau de protection de la structure et de la réalité de l'effet de leur application. Enfin, légitimement, un principe de liberté pour les entités doit s'instaurer au fur et à mesure que

la confiance s'établit entre les différentes structures. Ainsi, les responsables de sécurité des systèmes d'information de l'IT et des systèmes industriels s'approprient les concepts de gouvernance cyber de leur groupe et les intègrent dans les organes de gouvernance de leurs propres structures.

L'émancipation de la gouvernance de la cybersécurité impose de développer un nouveau modèle d'intégration dans la gouvernance du numérique

De fait, la cybersécurité se retrouve à la jonction :

- de la gouvernance du numérique, qui veut s'assurer qu'elle est correctement protégée et qu'elle fait les bons choix de déploiement de ces solutions dans un équilibre entre sécurité et agilité du SI, dans un optimum économique ;
- des directions métier, qui exigent légitimement de bénéficier d'une réactivité dans le cadre d'une réponse à un incident (attaque par rançongiciel, fraude au président, espionnage, etc.) ;
- des autres fonctions de la direction générale, qui veulent s'assurer que le risque, très souvent coté à un niveau élevé, reste maîtrisé aussi bien au niveau de sa couverture que de l'efficacité des mesures qui permettent de le réduire.

Aux frontières de la gouvernance de la cybersécurité d'un groupe, d'autres exogènes sont apparus

Les grands groupes travaillent de plus en plus en mode filière avec l'ensemble des acteurs de leur chaîne de valeur (*supply chain*) et en interconnectant les différents systèmes d'information. Du coup, un effet de ruissellement, voire d'amoncellement, des mesures et choix de cybersécurité au sein de ces filières doit être régulé. Ceci apporte également un niveau de complexité supplémentaire, puisqu'il est nécessaire de faire converger les différents acteurs, qui sont de moins en moins dans une situation de donneur d'ordre/exécutant.

Certains modèles d'entreprises étendues commencent à porter leurs fruits :

- la convention cyberdéfense du ministère des Armées avec les principaux industriels de défense permet de fluidifier l'échange d'informations et renforcer notamment la sécurisation des sous-traitants face à un nombre croissant de cyberattaques ;
- créée en 2011 par Airbus, Airbus Group, Dassault Aviation, Safran et Thales, BoostAeroSpace exploite une plateforme numérique aéronautique européenne qui intègre des mécanismes de coopération en cybersécurité. Puis le programme AirCyber de standardisation et harmonisation de la cybersécurité au sein de la *supply chain* aérospatiale et défense a permis de regrouper plus de 200 membres[1].

[1] https://boostaerospace.com/wp-content/uploads/2025/06/OnePager_AirCyber_FR.pdf

La position des États évolue au travers de la réglementation et de la souveraineté

Si vis pacem, para bellum

Des éléments exogènes à la gouvernance de l'entreprise influencent désormais les prises de décisions des acteurs de la cybersécurité. La réglementation se durcit au fur et à mesure que la sinistralité s'étend, et que les organisations mafieuses et malveillantes s'organisent. De plus, les États, dans un contexte géopolitique incertain, développent leur capacité de cyber-guerre pour peser sur les conflits armés traditionnels. Se pose alors la problématique de la relation entre les structures étatiques et les forces de cybersécurité des groupes qui se voient apposer, de fait, la nécessité de trouver le juste équilibre entre la réponse aux exigences de la réglementation et la capacité à pouvoir l'appliquer. De même, la coopération opérationnelle entre les États et le secteur privé mériterait d'être plus développée.

La gouvernance de la cybersécurité, en tant que ressource capacitaire de défense de l'entreprise, doit donc consolider ses modalités de fonctionnement avec les forces opérationnelles des États, les acteurs sectoriels et les autres organes traditionnels de l'entreprise.

Une définition de la souveraineté s'impose

Pour les opérateurs les plus critiques, il est nécessaire de définir ce qui relève des choix de l'entreprise et de son intérêt économique et ce qui relève des principes qui la transcendent et qui répondent aux intérêts des citoyens des pays dans lesquels celle-ci est implantée.

Ainsi, la notion de souveraineté peut être perçue comme étant supra vis-à-vis des intérêts directs du groupe par les salariés qui la composent. Il est donc nécessaire que la gouvernance de la cybersécurité identifie ces différents champs d'influence, afin d'éclairer la direction générale sur ces aspects qui dépassent la performance opérationnelle et économique de l'entreprise.

Volet opérationnel

L'aspect opérationnel de la cybersécurité a dû évoluer rapidement au regard des enjeux auxquels elle doit faire face

Initialement perçue comme un « simple » moyen technique, pilotée par des ingénieurs dont le rôle est de se protéger d'attaquants qui essaient de percer les systèmes d'information ou de les espionner, la cybersécurité opérationnelle a dû affronter la réalité d'une asymétrie croissante entre attaquants et défenseurs. En effet, la menace cyber est devenue protéiforme, elle se concrétise par l'action de groupes agiles, véloces, financés et en croissance exponentielle. Des éléments de doctrine et des tactiques associées ont émergé au fur et à mesure que l'industrie du service de cybersécurité (MSSP) s'organisait.

Afin de prendre en compte cette nouvelle réalité, les équipes opérationnelles ont relié leurs différentes missions aux multiples défis qu'elles doivent relever :

- une fonction de protection permettant de filtrer un premier niveau de volume d'attaque ou de tentative d'agression, que l'on pourrait qualifier de mineur. Cette fonction permet également de prendre en compte les vulnérabilités les plus critiques, parmi plus de 20 000 publiées par an, et d'accompagner les métiers pour protéger les systèmes d'information exposés ;

- une fonction de cybersurveillance, qui repère des activités malveillantes contre les activités les plus critiques, définies par les directions métier de l'entreprise ;
- une fonction de réponse à incident, qui permet de s'assurer de l'arrêt et idéalement de la résorption, d'une agression contre les données et processus contenus dans le système d'information ;
- des fonctions de réduction de leurs propres faiblesses et d'amélioration de la connaissance des attaquants, à travers des équipes dédiées à l'analyse du renseignement en sources ouvertes, à l'analyse des groupes d'attaquants et à l'analyse géopolitique des ressources capacitaires des adversaires potentiels. La vérification du niveau de résilience des SI s'appuie sur des activités d'audit et de *threat hunting*.

Malheureusement, les mécanismes d'agression, pilotés par des acteurs malveillants déterminés, évoluent dans le temps, nécessitant une organisation et des tactiques particulièrement agiles, obligeant les grands groupes à réorganiser leur cyberdéfense régulièrement.

Les équipes opérationnelles sont constituées de femmes et d'hommes dans toutes leurs dimensions

La maturité de la gouvernance de la cybersécurité ayant progressé, des problématiques plus traditionnelles de gouvernance commencent à émerger. L'affaire Pegasus, mise en lumière en 2021 par une enquête sous l'égide du consortium de journalistes de Forbidden Stories, a révélé l'utilisation d'un logiciel espion invasif vendu par la société israélienne NSO à des États, et a démontré que des capacités étendues de système de surveillance ont un impact direct sur les démocraties. En conséquence, les États ont interdit aux entreprises d'utiliser des solutions techniques trop intrusives, limitant ainsi leur capacité à pouvoir identifier rapidement et efficacement les agressions et les activités malveillantes et illégales les plus complexes.

Enfin, les équipes de cybersécurité étant constituées d'êtres humains, elles se retrouvent quelquefois en situation de conflit d'intérêts face à des salarisé malveillants, qu'elles connaissent par ailleurs, et avec des concepts éthiques non alignés sur leurs propres opinions.

Le caractère impératif de la mise en œuvre de moyens de défense efficaces engendre des spécificités propres à la cybersécurité

Les attaquants cherchant à exploiter les failles du système d'information dès leur publication – voire les processus internes de l'entreprise – il est impératif de mettre en œuvre des dispositifs de maintien en condition opérationnelle et de sécurité qui soient efficaces, adaptés et évolutifs.

De plus, l'agilité et la capacité d'adaptation des attaquants imposent aux entreprises un niveau de compétences constant, des budgets de formation conséquents et des salariés qui acceptent de devoir constamment renouveler leurs connaissances. Le vivier des acteurs de la cybersécurité est de plus en plus sollicité, créant des tensions pour les ressources, au fur et à mesure que la demande sur le marché du travail a grossi. À ce stade, en dehors de l'embauche de jeunes diplômés pris en charge par les filières de formation plus spécialisées, pour les profils expérimentés, il apparaît assez illusoire de pouvoir construire une GPEC dans un contexte aussi mouvant. Cependant, on voit apparaître des solutions à moyen terme, soutenues par les organisations professionnelles, le ministère du travail et de l'emploi, l'ANSSI et le programme France 2030.

Les moyens techniques déployés dans les SI utilisés par les équipes de cybersécurité proviennent en majorité des États-Unis, exposant les groupes à des risques de dépendance technologique, de *vendor lock-in* et à une influence accrue de la souveraineté américaine. L'*open source*, souvent cité comme une alternative, ne peut être crédible qu'à partir du moment où l'on maîtrise complètement les mécanismes techniques sous-jacents ; que l'on maintien des compétences dans le temps et la capacité à faire évoluer la solution *via* les contributeurs. Ces aspects sont dépendants de la capacité du groupe à financer, former et recruter.

Conclusion

En synthèse, les métiers et les fonctions de cybersécurité se trouvent de plus en plus intriqués et doivent faire face ensemble à une menace en constante évolution. Il est désormais nécessaire d'analyser de plus en plus profondément les stratégies des attaquants qui pour certains d'entre eux sont des États.

La complexité croissante des entreprises et des systèmes d'information impose aux acteurs qui gouvernent la cybersécurité de progresser dans leur niveau de maturité et de mieux intégrer cette complexité, afin d'interagir plus facilement avec les autres acteurs de la gouvernance de l'entreprise qui n'ont pas la même perception de ce nouveau métier.

Enfin, il n'y a pas encore assez de recul pour faire émerger le consensus du juste niveau d'investissements dans le domaine de la cybersécurité tout en préservant un modèle économique soutenable. Cet aspect demeure une source de tension et ne permet pas de s'appuyer sur des feuilles de route acceptées et considérées comme légitimes par toutes les fonctions de l'entreprise.

Cybersécurité et sécurité physique : une réponse unifiée face aux menaces hybrides

Par Arnaud TANGUY
Directeur de la Sécurité du groupe AXA

Dans un contexte mondial en transformation, marqué par des enjeux géopolitiques, économiques et écologiques, les menaces hybrides s'intensifient et se complexifient. Attaques combinant vecteurs numériques et physiques, incidents environnementaux ou sociétaux fragilisent la résilience des systèmes. Face à ces risques, les réglementations NIS2 et DORA imposent une gestion intégrée, une gouvernance globale et une réponse coordonnée. Cependant, l'organisation traditionnelle, souvent cloisonnée, montre ses limites : redondances, silos, inefficacités, délais d'intervention.

La nécessité d'adopter une approche holistique, intégrant cybersécurité, sécurité physique, continuité d'activité et gestion de crise, devient stratégique. Elle s'appuie sur une gouvernance unifiée, des processus mutualisés et l'usage innovant de l'intelligence artificielle pour anticiper, détecter et répondre plus efficacement aux menaces, renforçant ainsi la résilience opérationnelle.

Pourquoi maintenant ? Les menaces hybrides montent en puissance

Dans un monde en profond bouleversement géopolitique, économique et écologique le panorama des menaces pour les entreprises évolue rapidement, avec en particulier l'émergence de menaces hybrides qui mêlent cyber et sécurité physique. Les attaques combinent ainsi des vecteurs cyber et physiques dans des scénarios de plus en plus sophistiqués :

- des attaques informatiques aux effets immédiats sur le monde réel (par exemple : des aéroports dont les vols ont été immobilisés[1]) ;
- des intrusions dans des bâtiments pour perpétrer des attaques informatiques ;
- la manipulation de capteurs physiques à distance pour endommager des équipements industriels (cas de l'attaque Stuxnet contre des centrifugeuses nucléaires[2]).

Les menaces environnementales et sociétales pèsent aussi sur la résilience des systèmes d'information :

- des pics de chaleur mettant hors service des centres de données informatiques[3] ;

[1] https://www.lemonde.fr/economie/article/2025/09/21/la-situation-s-ameliore-dans-plusieurs-aeroports-europeens-touches-par-une-cyberattaque_6642251_3234.html

[2] https://fr.wikipedia.org/wiki/Stuxnet

[3] https://www.challenges.fr/entreprise/tech-numerique/les-data-centers-resisteront-ils-a-la-montee-des-temperatures-un-enjeu-vital-pour-nos-donnees-et-pour-leconomie_621143

- des évènements géopolitiques[4] ou sanitaires[5] perturbant la chaîne d'approvisionnement en composants électroniques.

Dans ce contexte, la pression réglementaire s'intensifie et converge vers une sécurité unifiée. Dans la finance, DORA (*Digital Operational Resilience Act*) impose une résilience opérationnelle de bout en bout ; dans les autres secteurs, NIS2 fixe des exigences similaires. L'objectif : une gestion homogène des risques et un pilotage unifié, où les risques cyber sont évalués aux côtés des risques géopolitiques et de sûreté, afin de rationaliser la réponse à incident et de réduire les silos.

Ces évolutions interrogent l'organisation et la stratégie de sécurité des entreprises. Elles plaident pour une approche holistique : une sécurité intégrée qui allie anticipation, protection et gestion de crise efficaces.

Le diagnostic est posé. Tentons de comprendre pourquoi nos modèles d'organisation en silos ne sont plus adaptés à la réalité de ces menaces, et comment les faire évoluer sans perdre l'expertise.

Les limites de l'approche traditionnelle : les silos à l'épreuve du réel

L'intégration de la cybersécurité avec les autres disciplines de sécurité représente une réelle opportunité pour bâtir une gouvernance cohérente au sein d'un groupe international. Cependant, certaines barrières organisationnelles, culturelles et technologiques peuvent compliquer cette convergence.

Le défi tient à une double réalité : la structure décentralisée des multinationales, nécessaire pour répondre aux marchés locaux, engendre des pratiques hétérogènes en matière de sécurité ; les équipes de cybersécurité opèrent souvent à part des structures en charge de la sécurité physique, de la sûreté, de la gestion de crise et de la résilience opérationnelle.

L'organisation sécuritaire traditionnelle reflète souvent l'histoire de l'entreprise plus que la réalité des menaces. La cybersécurité, née comme une sous-fonction de l'informatique, reste souvent rattachée à la DSI avec une vision très technique et technologique ; la sécurité physique, héritée des services généraux, reste centrée sur l'accès aux locaux et la protection des personnes ; la continuité d'activité est gérée de manière dispersée, avec des plans locaux peu coordonnés ; la gestion de crise dépend fréquemment de la communication ou de la direction générale, avec un déclenchement souvent réactif.

Conséquences : des inefficacités structurelles coûteuses et des angles morts dans le pilotage. Parmi les symptômes les plus fréquents : duplication d'analyses de risques sur des périmètres identiques, conclusions d'audits non mutualisées, outils cloisonnés, coûts de licences et de maintenance multipliés, remontées d'informations et d'incidents lentes ou incomplètes, budgets dispersés, stratégies désalignées, indicateurs clés (KPIs) parfois contradictoires, réponses aux incidents tardives ou fragmentées, fragilisant la stabilité opérationnelle.

En parallèle, la transformation s'accélère. Les méthodes Agiles, l'IA et les nouvelles technologies exigent des processus de sécurité simplifiés, une meilleure visibilité de l'impact des risques sur l'activité et une gestion d'incidents plus efficace. La recherche d'optimisation organisationnelle et budgétaire invite, elle, à réduire les redondances.

[4] https://www.alternatives-economiques.fr/taiwan-point-de-fragilite-de-leconomie-mondiale/00113775

[5] https://www.forbes.fr/technologie/crise-des-semi-conducteurs-penurie-et-recherche-de-souverainete-technologique/

Le diagnostic est posé. Comment passer d'une juxtaposition d'équipes à un système intégré, sans perdre en expertise ?

Orchestrer la sécurité : vers une sécurité holistique

Pour faire face aux menaces hybrides, l'entreprise doit passer d'un ensemble d'équipes séparées à une organisation convergée.

La mise en œuvre d'une « sécurité holistique » vise à redéfinir le périmètre sécuritaire en faisant converger cybersécurité, sûreté, sécurité physique, continuité et gestion de crise dans un continuum de sécurité unifié. À la clé : une gestion cohérente des risques, des décisions plus rapides et une résilience renforcée.

Le levier n°1 de cette transformation est une gouvernance unifiée. Le rattachement stratégique au comité exécutif ou au conseil d'administration légitime les prises de décision, les arbitrages et les investissements. Une direction de la sécurité globale porte une responsabilité de bout en bout avec une vision à 360° sur l'ensemble des sujets sécurité.

Le pilotage s'appuie sur une « tour de contrôle » unique : un tableau de bord commun, des indicateurs consolidés, comparables et actionnables. On sait qui décide, quand, et sur la base de quelles données.

Le modèle opérationnel s'appuie sur une organisation matricielle combinant expertise et cohérence : les centres d'excellence préservent l'expertise technique spécialisée (par exemple, sécurité de l'information, architecture technique, sûreté…) ; les fonctions transverses (gestion des risques, contrôle interne, stratégie, veille et anticipation de la menace) en assurent la cohérence globale.

Résultat : l'expertise est conservée, les doublons disparaissent, les coûts cachés (outils, audits, plans redondants) diminuent, la conformité devient plus lisible.

La clé du succès : déployer par étapes, avec jalons et communication claire, afin d'élever le niveau de sécurité sans interrompre la protection en place.

Transformer sans casser : une approche par étapes

Unifier, oui, mais sans rupture de service et sans perte d'efficacité. La transformation doit être progressive, lisible et pilotée. Une première étape consiste à unifier la gouvernance : regrouper les équipes existantes sous une direction unique, clarifier les rôles et responsabilités, définir des circuits d'escalade, et s'appuyer sur un parrainage explicite du comité exécutif. Ensuite, harmoniser les processus transverses : aligner les pratiques de gestion des risques, des incidents, des crises et de la continuité, établir des référentiels communs, des niveaux de service et des seuils d'alerte partagés. Enfin, mutualiser les outils et les données : mettre en place un tableau de bord unique et des référentiels partagés (actifs, risques, fournisseurs).

La conduite du changement est un levier central. Elle repose sur une communication transparente expliquant les raisons du mouvement, les bénéfices attendus, le calendrier et les jalons, avec des canaux dédiés aux questions-réponses. Elle s'appuie aussi sur les compétences : parcours de formation intensifs, certifications, montée en compétences pluridisciplinaires (par exemple en binômes cyber/sûreté) et communautés de pratique. La valorisation des équipes passe par la reconnaissance, de nouvelles responsabilités, des opportunités de mobilité interne et des objectifs alignés.

Pour maîtriser le risque de transition, on conserve les contrôles existants pendant la bascule, on phase les déploiements, on teste *via* des pilotes, et on fixe des critères de sortie ainsi que des métriques de stabilité.

Une fois ce cadre en place, les gains deviennent rapidement visibles. Prochaine étape : les bénéfices tangibles et mesurables.

Des gains mesurables, au-delà de la conformité

En intégrant de façon cohérente les risques cyber, géopolitiques et physiques sous une supervision centralisée, l'entreprise améliore l'anticipation, la détection et l'efficacité de la réponse aux incidents comme de la gestion de crise. Au-delà de la conformité, cette approche accélère la décision, clarifie les priorités et optimise l'allocation des ressources.

Valeur métier : quand la sécurité devient un avantage

La convergence de la sécurité transforme le dialogue avec les fonctions métier. En comprenant mieux leurs priorités (*business*, réglementation, réputation), on favorise une co-construction de solutions et de services intégrant la sécurité dès leur conception. La résilience est calibrée selon la criticité, avec des RTO/RPO (objectifs de reprise et de point de reprise) différenciés et une gestion des risques unifiée.

Résultat : la sécurité se repositionne en avantage compétitif. Côté client et société, cela se traduit par des services plus fiables, une continuité renforcée et des incidents moins fréquents et moins graves, renforçant la confiance.

Résilience organisationnelle renforcée : détecter, corréler, agir

La vision 360° des risques transforme la détection et l'anticipation des menaces. La corrélation des signaux faibles (cyber, physiques et humains) permet d'identifier plus tôt les situations à risque. L'intégration de l'IA permet d'anticiper des menaces et de développer des modèles de risque intégrés et d'automatiser certaines réponses. Les scénarios combinés simulent des incidents multi-dimensionnels pour mieux évaluer la résilience de nos organisations.

La réactivité et la coordination s'améliorent également : des processus unifiés simplifient les circuits décisionnels, clarifient les seuils d'activation des cellules de crise et garantissent une communication cohérente.

La continuité d'activité adopte une approche holistique : plans intégrés alignant cyber/physique/métiers, exercices transverses réguliers, sites de secours sécurisés de manière homogène et contrôle renforcé des fournisseurs critiques avec des plans de contingence adaptés. Concrètement, on réduit les délais de détection et de rétablissement, tout en diminuant les doublons et les coûts cachés.

Prochaine étape : comment accélérer et amplifier ces résultats ?

Perspectives et recommandations – L'avenir de la sécurité holistique

Nous sommes aujourd'hui à un tournant stratégique. La fonction sécurité a l'opportunité de s'élargir pour intégrer des compétences complémentaires et mieux répondre

aux menaces émergentes : intelligence économique (veille concurrentielle, protection de l'innovation, stratégies d'influence) et lutte antifraude (analyses comportementales et transactionnelles). Elle peut aussi jouer un rôle moteur dans les politiques ESG (critères environnementaux, sociaux et de gouvernance des entreprises), en contribuant à la sécurisation des *data centers*, à la réduction de l'empreinte carbone et à la résilience des chaînes d'approvisionnement.

L'essor des technologies émergentes (intelligence artificielle, Internet des objets – IoT, calcul quantique, réalité augmentée) ouvre la voie à de nouvelles capacités de détection, de prédiction et d'automatisation, transformant profondément les pratiques en matière de sécurité. L'IA, en particulier, permet de corréler des événements multi-sources, de toujours mieux détecter des anomalies comportementales et d'automatiser les réponses aux incidents

Finalement, l'évolution des menaces (on parle maintenant de guerre hybride ou de criminalité hybride, mêlant attaques physiques, cyber et désinformation) poussera à approfondir l'hybridation des fonctions de sécurité, en y intégrant la défense informationnelle, la lutte contre la désinformation et la protection contre les manipulations et l'influence cognitive.

En résumé, la question n'est plus "si" mais "comment" accélérer cette transformation : quels périmètres intégrer en priorité, quelles compétences développer et quelles technologies déployer pour créer, durablement, plus de résilience et de valeur ?

À RETENIR : LA CONVERGENCE COMME IMPÉRATIF STRATÉGIQUE

Face aux menaces hybrides, maintenir une sécurité en silos n'est plus tenable. La convergence organisationnelle devient un impératif pour préserver la résilience et la compétitivité. Les secteurs précurseurs (finance, énergie, télécoms) montrent que, audelà de la conformité, cette transformation crée une valeur tangible et durable.

Trois bénéfices clés se dégagent. D'abord, l'efficacité opérationnelle : des coordinations plus rapides et la suppression des redondances. Ensuite, la valeur métier : la sécurité devient un partenaire stratégique des fonctions *business*, au service des priorités et de l'expérience client. Enfin, la résilience renforcée : une continuité d'activité efficace et une meilleure capacité d'adaptation aux menaces émergentes.

Pour réussir, il faut élargir les compétences et unifier la gouvernance, afin d'équilibrer défenses techniques, compétitivité et confiance des clients. L'objectif : un cadre de décision à la fois flexible et robuste, qui aligne les équipes, les processus et les investissements sur une même ambition de performance et de sécurité.

Témoignage d'un RSSI de collectivité locale : le cas de Marseille

Par Jérôme POGGI
Responsable de la Sécurité des Systèmes d'Information (RSSI)
de la municipalité de Marseille

Cet article vise à décrire la situation de la cybersécurité au sein des collectivités locales. Il montre une grande disparité entre les systèmes d'information et leurs niveaux de protection, sachant que ces collectivités gèrent des données sensibles et des services critiques, ce qui les rend attractives pour les cyberdélinquants.

L'arrivée du Référentiel Général de Sécurité (RGS) a contribué à l'intégration de la sécurité dans les projets métiers, mais le budget cyber est souvent perçu comme un « centre de coût ».

La directive NIS v2 imposera aux entités concernées de respecter un ensemble de règles de sécurité, cependant les petites collectivités resteront vulnérables, sauf si les ressources, l'expertise et les solutions des plus grandes sont mutualisées avec les plus petites.

En conclusion, la cybersécurité doit être vue comme un enjeu stratégique et non comme un simple coût ; une approche globale (prévention, formation, mutualisation) est indispensable pour assurer la protection des services publics et préserver la confiance des citoyens.

Situation et spécificités des collectivités en cybersécurité

À la fin du XX^{e} siècle, la France s'est progressivement décentralisée, créant une multitude d'entités autonomes dans bien des domaines. Le fait qu'il y ait une multitude d'acteurs autonomes – plus de 35 000 communes, 100 départements, 13 régions et divers établissements publics de coopération intercommunale (EPCI) – a entraîné une disparité des systèmes d'information, tous présentant des niveaux hétérogènes de cybersécurité.

Du fait de la décentralisation, l'État a transféré certaines de ses compétences aux collectivités territoriales, leur conférant ainsi une certaine autonomie, notamment sur la manière de gérer les différentes données sensibles dont elles ont la responsabilité (état civil, fiscalité, services sociaux). Cette autonomie en fait des cibles potentielles, souvent vulnérables pour les cyberattaques.

Certaines collectivités ont en outre la responsabilité de gérer des services critiques (eau, électricité, transports), dont la perturbation peut avoir des impacts significatifs sur la population et qui présentent donc un intérêt pour les cyberdélinquants, agissant avec

des attaques telles que les franchises de rançongiciels (*ransomware*[1]) et surtout les APT (*Advanced Persistent Threat*[2]).

Cette autonomie se ressent aussi dans la réglementation : les collectivités territoriales ne sont pas astreintes aux mêmes règles que les entités de l'État, ni aux mêmes sanctions. Cette indépendance constitue une force, mais peut aussi devenir une faiblesse, car la pression pour faire évoluer la cybersécurité y est moins forte. Beaucoup de mes confrères et moi-même espérons que la directive NIS v2 contribuera à atteindre un niveau de maturité cyber suffisant, toutefois elle ne pourra pleinement être appliquée aux petites collectivités. Il subsistera toujours une disparité importante, même si une solution est possible.

Les jalons cybersécurité et réglementation

Arrivé en 2008 au service sécurité du SI de la Mairie, j'ai constaté que la cybersécurité dans les collectivités territoriales n'était pas du tout une priorité, mais plutôt une contrainte sans levier apparent d'amélioration possible. L'arrivée du Référentiel Général de Sécurité (RGS[3]) nous a permis de « forcer » un référencement, une catégorisation de toutes nos applications et téléservices, ce qui a été l'occasion de pousser l'amélioration de notre cybersécurité à tous les niveaux, et surtout côté métiers. Cette étape a permis une première prise en compte de la sécurité dans les projets métiers utilisant l'informatique. Le métier a commencé à nous voir comme un « partenaire » et non un frein à tous ses projets.

Ce travail a été très bénéfique pour la priorisation des actions lors de la reprise sur incident après la compromission généralisée à laquelle nous avons dû faire face la veille du premier tour des élections municipales de 2020, dans un climat de confinement dû au Covid. L'année 2020 fut une année noire pour une multitude d'autres collectivités : le début d'un réveil généralisé, mais malheureusement avec des suites limitées aux grandes collectivités, car elles seules avaient les moyens humains et financiers pour passer le cap de la simple reconnaissance de l'utilité de la sécurisation des systèmes d'information à leur mise en œuvre concrète.

Prochainement la directive NIS v2[4] va entrer en vigueur, plus exactement sa version française, et va réguler 18 types d'entités. Les principales obligations de la directive sont que chaque entité régulée (lors de la rédaction de l'article, nous ne savions pas officiellement si les collectivités territoriales allaient être régulées, cependant il est certain que les plus importantes le seront) devra fournir certaines informations à l'ANSSI[5], mettre en place

[1] Logiciel permettant de prendre en otage, par des moyens cryptographiques, les données numériques d'une société et la libération de ces données se fait contre paiement d'une rançon en cryptomonnaie.

[2] APT : menace numérique ayant les ressources et capacités de type étatique.

[3] Le Référentiel Général de Sécurité (RGS), pris en application de l'ordonnance n°2005-1516 du 8 décembre 2005, vise à instaurer la confiance numérique dans les échanges électroniques. Il s'adresse à toutes les autorités administratives et contient essentiellement : une procédure d'homologation de sécurité, qui repose sur une analyse de risques, ainsi que la mise en place de fonctions de sécurité conformes aux exigences du RGS.

[4] La directive NIS 2 (en français : Sécurité des Réseaux et des Systèmes d'Information) vise à renforcer le niveau de cybersécurité des structures économiques et administratives des États membres de l'UE. Elle cible 18 secteurs d'activités répartis en 2 catégories : les entités essentielles et les entités importantes.

[5] L'ANSSI (Agence nationale de la sécurité des systèmes d'information) est un service français à compétence nationale, rattaché au Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), chargé de la sécurité des systèmes d'information nationaux.

des mesures de gestion des risques adaptées, et déclarer ses incidents de sécurité. En cas de manquement, des sanctions financières pourront être imposées. Là se pose le dilemme du contrôle de l'État sur des collectivités territoriales, justement indépendantes de l'État.

Comment sanctionner ? Il me semble que la sanction financière n'est pas la solution, car elle priverait les citoyens de services assurés par la collectivité, ce serait le citoyen qui serait sanctionné et non la collectivité. Une autre piste serait celle que la Cnil utilise aussi : la sanction par le fait de rendre public le manquement en matière de sécurité. Cette action me semble la plus adaptée car elle impose à la collectivité de garder la confiance de ses citoyens, sans action de l'État qui pourrait être interprétée comme un non-respect de son indépendance.

Cependant, cet éveil est complexe, car la cybersécurité a un coût, et les petites collectivités n'en ont pas les moyens, qu'ils soient humains, techniques ou financiers. Il faut sensibiliser les agents, les instances dirigeantes et aussi les élus.

Les chantiers en cours et à venir

Le « combat » pour obtenir les budgets humains et financiers

C'est une tâche constante que d'obtenir des budgets, et ce pour plusieurs raisons : la cybersécurité est trop souvent vue comme un centre de coût sans « rentabilité ». Les équipes sécurité achètent, installent, mettent en place, font infogérer de nombreuses solutions de sécurité, le RSSI impose des contraintes de sécurité, fait ou fait faire des contrôles, des audits, met à jour des faiblesses, des vulnérabilités, mais tout cela est souvent vu comme non rentable car invisible. Il ne se passe rien, donc cela ne sert à rien !

Tant qu'il n'y a pas d'accident ou d'incident, la cybersécurité est considérée comme inutile. C'est William H. Webster[6], ancien directeur du FBI qui l'a si bien et simplement dit : "Security is always too much until the day it is not enough". Cela fait plus de 20 ans que je navigue sur le bateau de la cybersécurité (en passant, auparavant, nous appelions cela « sécurité informatique »), et malheureusement c'est une constatation que nous, professionnels de la cyber, faisons toujours depuis tant d'années. Comment se fait-il que la cybersécurité soit aussi sous-estimée ? Heureusement, ce n'est pas partout, surtout auprès de grandes entités, mais pour ce qui concerne les collectivités, c'est encore trop souvent le cas.

Oui, nous entendons encore cela, voire même : « Mais l'équipe sécurité est largement suffisante ! », alors que d'autres équipes ont encore la possibilité de se renforcer. D'après l'ANSSI, il faut au minimum un ratio d'un agent dédié à la cybersécurité pour 1 500 utilisateurs du système d'information, et le compte n'y est jamais.

Un de mes pairs s'est même vu répliquer par son DGS[7] : « Depuis que nous avons un RSSI, il y a plein d'incidents de sécurité, il faut supprimer le RSSI », alors qu'il ne faisait que sa mission de relever et de référencer les incidents de sécurité. Dans ces conditions, il n'est pas possible de travailler sereinement et efficacement. Il s'est heureusement rapidement trouvé un nouveau poste dans une autre collectivité mais il n'est malheureusement pas un cas isolé.

[6] Président du Conseil consultatif sur la sécurité intérieure (en anglais, Homeland Security Advisory Council) de 2005 à 2020. Il est auparavant directeur du Federal Bureau of Investigation (FBI) entre 1978 et 1987 puis directeur de la Central Intelligence Agency (CIA) de 1987 à 1991.

[7] Directeur général des Services : le plus haut responsable administratif dans les collectivités territoriales.

Ce combat, une fois gagné, c'est-à-dire la reconnaissance de l'utilité de mettre en place des mesures de sécurité et d'avoir un service sécurité, suppose ensuite de disposer d'un budget en conséquence, avec des crédits en investissement mais aussi en fonctionnement, car toutes les solutions de sécurité nécessitent un « abonnement » ou de la maintenance. C'est là que commence le deuxième challenge : obtenir des budgets récurrents pour garder un niveau de sécurité toujours suffisant et conforme à l'état de l'art.

Souveraineté et budget

Tout cela nous amène à une nouvelle réflexion : dans le contexte géopolitique très tendu actuel, nous devons nous réorienter vers des solutions dites « souveraines », ou au moins essayer de faire tourner l'économie française. En tant que collectivité territoriale et service public, nous avons le devoir de servir le citoyen, non seulement en termes de service, mais aussi d'un point de vue économique, car nous fonctionnons avec de l'argent public.

Nous avons donc le devoir de faire circuler cet argent vers des sociétés françaises, de faire marcher l'économie française. Ce sont quand même nos impôts. Autant que cet argent serve aux citoyens français et non à de « obscurs » fonds d'investissement étrangers, qui ne font que peu tourner l'économie nationale, voire ne payent que très peu d'impôts en France.

Le code des marchés publics, ne nous permet pas de vraiment favoriser l'économie française, les appels d'offres des marchés publics devraient intégrer des considérations de souveraineté dans un contexte de cyberguerre pour user des exceptions prévues à cet effet dans le code des marchés publics. On peut aussi déplorer que des sociétés françaises qui font d'excellents produits ne soient pas retenues lors d'appels d'offres au profit de solutions de grands opérateurs étrangers au simple motif « qu'il faut faire comme tout le monde car on a moins de chances de se tromper » et ce n'est malheureusement qu'une des excuses les moins ubuesques.

Faire travailler les sociétés françaises en plus de les faire progresser et de les rendre plus compétitives, présente également l'avantage d'avoir une meilleure maîtrise sur les données gérées par le prestataire, car celui-ci est soumis au droit français et européen. Sans parler du sempiternel problème des lois extraterritoriales des États-Unis, il faut que les collectivités reprennent la main sur leurs données et leurs budgets, et cela ne peut se faire que grâce à l'utilisation de solutions françaises et européennes.

L'avenir de la cybersécurité dans les collectivités

Un coup de « turbo » ?

Faut-il un coup d'accélération dans la cybersécurité des collectivités territoriales ? La réponse est sans hésitation : oui ! Il y en a déjà eu plusieurs : en 2020 le réveil des collectivités qui découvrent qu'elles sont aussi des cibles, et la part du plan « France Relance » dévolue à la cybersécurité, pilotée et financée par l'ANSSI. Le premier réveil a été douloureux, mais dans la sécurité des systèmes d'information, comme nous l'avons déjà vu, l'incident a toujours été, malheureusement, un déclencheur. Cependant, l'ANSSI a fait de très gros efforts lors du plan France Relance, tant en termes d'apport au pilotage que, surtout, d'aide financière pour les collectivités qui en avaient besoin et en démontraient une utilisation pertinente. Cette aide a été très bien utilisée. De nombreuses entités ont pu en bénéficier et améliorer réellement leur niveau de protection cyber. Cependant, seules les entités ayant des capacités budgétaires suffisantes ont pu en bénéficier. Pourquoi ? Tout simplement parce que le financement était basé sur une aide par délivrance de subvention, et donc les entités ont dû faire l'avance. Lors des Jeux Olympiques et Paralympiques de Paris 2024, l'ANSSI a aussi aidé les entités hébergeant des épreuves, mais cela s'est

organisé différemment sur le plan financier, vraisemblablement pour être plus réactif, mais surtout parce que cela pouvait impacter la sécurité des Jeux et donc de l'État.

Toutes ces actions ont permis d'élever le niveau de cybersécurité des grandes entités, mais comment s'occuper des petites ? À mon humble avis, il n'y a qu'une solution : la grande sœur ou le grand frère !

La grande sœur

Les grandes collectivités devraient avoir le devoir d'aider les plus petites, en leur apportant un soutien logistique, technique et matériel. C'est possible en mutualisant, en standardisant les solutions, les hébergements… Nous le voyons, les DSI des métropoles disposent de moyens techniques, de connaissances, de compétences et surtout d'un personnel bien plus conséquent que les petites entités. C'est quelque chose qui se fait déjà, mais n'est pas encore suffisamment généralisé, car il y a des freins. Ces freins sont parfois très importants : différence de bord politique, peur de perdre son indépendance et d'être redevable d'une autre collectivité, peur de ne pas avoir les crédits… Mais ces questions, ces peurs et ces freins ne devraient pas exister ! Nous sommes tous au service du citoyen français, nous sommes le service public !

La question de la relation contractuelle entre la grande sœur et le petit frère peut prendre différentes formes : soit les deux parties concluent une convention, soit elles se retrouvent au sein d'un groupement de collectivités pour une mission bien définie, comme c'est prévu pour les syndicats de communes, ou encore en participant au capital social d'une SCIC[8].

Écologie, *open source* et budgets

Le nerf de la guerre, c'est le budget de fonctionnement, nous le voyons tous, il est en forte baisse, et la cybersécurité n'est pas toujours estimée à sa juste valeur. Il faut donc faire au moins aussi bien, mais avec moins. À la ville de Marseille et au grand dam de certains, nous avons fait le choix de nous orienter vers l'*open source*. Cela ne veut pas dire que nous ne payons plus rien, mais que nous avons réduit nos frais de fonctionnement et les avons transformés en frais de service de maintenance, de prestation, d'hébergement vers des sociétés françaises ou européennes, qui nous permettent d'avoir un service, certes moins fourni que si nous étions chez un des GAFAM[9], mais avons-nous vraiment besoin d'un tel niveau de service ? Il est clair que non.

Une évaluation rapide du parc, de son utilisation et de nos utilisateurs, pourrait même nous amener à réduire le parc des postes Windows et macOS à 20 %, car maintenant il suffit d'un navigateur pour quasiment tout faire : *webmail*, application, suite collaborative (Collabora ou OnlyOffice pour la bureautique), visio, *tchat,* etc. En basculant vers 80 % de postes Linux, nous serions tout aussi productifs, moins dépendants de logiciels propriétaires et cela nous permettrait de garder encore trois ou quatre ans de plus nos ordinateurs. Ce serait mieux pour la planète, mieux pour les budgets, mieux pour la maîtrise des systèmes et donc mieux pour nos concitoyens. Mais on constate trop souvent des refus par méconnaissance et par peur de ne pas être comme les autres… même s'il est clair que les GAFAM exercent un fort lobbyisme contre cette idée.

---

[8] Juridiquement, une SCIC (Société Coopérative d'Intérêt Collectif) est une société coopérative de forme SA, SARL ou SAS. De forme privée et d'intérêt public, la SCIC associe des personnes physiques ou morales autour d'un projet commun alliant efficacité économique, développement local et utilité sociale. Voir https://www.les-scop.coop/les-scic

[9] GAFAM ou GAMAM est l'acronyme des géants du Web – Google (Alphabet), Apple, Facebook (Meta), Amazon et Microsoft – les cinq grandes firmes américaines qui dominent le marché du numérique. Elles sont aussi appelées les *Big Five* ou *Big Tech,* appellation la plus usitée en anglais.

Conclusion

La cybersécurité ne peut plus être perçue comme un centre de coût sans intérêt, ou au mieux une préoccupation technique isolée, mais bien comme un enjeu stratégique pour les collectivités.

Face à la multiplication des menaces numériques, les acteurs locaux publics doivent adopter une approche plus globale, intégrant prévention, formation et résilience numérique, tout en maintenant un haut niveau d'exigence dans le renforcement des infrastructures critiques.

Par ailleurs, la coopération inter-collectivités, le partage d'informations et la mutualisation des ressources et de moyens permettront non seulement d'assurer plus efficacement la sécurité de leurs systèmes d'information, mais aussi de renforcer la confiance des citoyens dans les services publics numériques.

Ainsi, la cybersécurité devient non seulement un bouclier contre les risques, mais également un levier de modernisation et d'innovation au service du bien commun.

Témoignage d'une association humanitaire

Par Fabien LEMARCHAND
Président de Hack4Values

Les ONG sont aujourd'hui en première ligne face aux crises humanitaires, mais aussi face à une menace invisible : la cybercriminalité. Une attaque réussie peut bloquer une mission de sauvetage, couper un hôpital de ses données vitales ou faire disparaître la confiance des donateurs. Pour y répondre, Hack4Values, une association née en France en 2021, a créé le premier programme de Bug Bounty solidaire gratuit pour les ONG. En mobilisant une communauté de *hackers* éthiques, elle protège ceux qui protègent. À travers ce témoignage, nous partageons les enjeux, les résultats et l'urgence de reconnaître le rôle des *hackers* éthiques pour construire une cybersécurité humanitaire durable.

Un monde plus vulnérable, des ONG en première ligne

Un milliard de personnes dans le monde dépendent aujourd'hui directement de l'action d'organisations non gouvernementales. Pourtant, la moitié d'entre elles a déjà été victime d'une cyberattaque.

Les conséquences dépassent largement le numérique : 7 ONG sur 10 pourraient fermer leurs portes après une attaque réussie. Derrière ces chiffres, il y a des vies humaines mises en danger, des actions solidaires paralysées, une confiance citoyenne brisée.

Perdre l'accès à son portefeuille de donateurs, c'est arrêter net l'action sur le terrain.

Perdre le contact avec des bénévoles déployés en zone de crise, c'est les exposer, eux et les populations qu'ils aident.

Perdre ses données, c'est perdre la confiance.

Naissance d'une réponse citoyenne

C'est pour répondre à ce défi que nous avons fondé Hack4Values en 2021, autour d'un principe simple : protéger ceux qui protègent.

Nous avons voulu offrir gratuitement aux ONG un dispositif jusqu'ici réservé aux grandes entreprises : le Bug Bounty.

Figure 1 : Logo de Hack4Values (Source : Hack4Values).

Ce modèle repose sur une idée puissante : transformer les *hackers* éthiques en alliés. Là où les cybercriminels exploitent les failles, nos volontaires les révèlent et aident à les corriger.

Comment ça marche ?

Concrètement, une ONG définit avec nous le périmètre de ses systèmes numériques à tester. Une communauté de *hackers* éthiques – aujourd'hui plus de 50 bénévoles répartis en Europe et au-delà – se mobilise pour rechercher des vulnérabilités. Chaque faille découverte fait l'objet d'un rapport clair, confidentiel et documenté. L'ONG dispose alors d'un plan d'action pour corriger et renforcer sa sécurité.

En trois ans, Hack4Values a :

- accompagné plus de 20 ONG majeures (MSF, Action Contre la Faim, SOS Méditerranée, Handicap International, Surfrider Foundation, La Protection Civile, etc.) ;
- identifié plus de 500 vulnérabilités critiques et élevées ;
- renforcé la protection numérique de millions de bénéficiaires indirects.

Ce que disent les ONG

Les témoignages parlent d'eux-mêmes :

- « Hack4Values aide SOS Méditerranée à protéger ses sites internet et à garantir l'accès du public aux informations essentielles sur la crise humanitaire. » – Responsable sûreté, SOS Méditerranée ;
- « C'est un privilège de bénéficier de ce dispositif. L'aide précieuse de Hack4Values contribue à apporter un niveau de sécurité essentiel pour continuer notre mandat humanitaire. » – Manuel Javier Casas Jimenez, responsable de la production et l'Infrastructure Informatique de Médecins Sans Frontières.

Une aventure humaine autant que technologique

Hack4Values, c'est aussi une rencontre entre deux mondes :

- des ONG concentrées sur l'urgence, parfois sans moyens IT structurés ;
- des *hackers* éthiques passionnés qui mettent leurs compétences au service du bien commun.

Cette collaboration crée un cercle vertueux : les ONG gagnent en sécurité, les *hackers* trouvent un cadre éthique et utile pour exercer leur talent.

Un enjeu de société : reconnaître les *hackers* éthiques

Mais cette démarche révèle aussi une limite : le vide juridique autour du rôle des *hackers* éthiques. Aujourd'hui, signaler une faille en France peut encore exposer un *hacker* bénévole à des risques pénaux. Beaucoup renoncent à alerter, par peur de poursuites judiciaires.

Nous plaidons donc pour une reconnaissance officielle du *hacker* éthique comme lanceur d'alerte numérique, avec un cadre légal clair, un code de conduite partagé et la possibilité de signaler directement aux organisations concernées.

Nous pourrions pour cela nous inspirer du modèle belge, qui a ouvert la voie en instaurant un cadre légal permettant aux chercheurs en sécurité de signaler des vulnérabilités sans risquer de sanctions, à condition de respecter des principes d'éthique et de proportionnalité. Un modèle performant nous semble fondé sur deux piliers : la collégialité et la reconnaissance par les pairs, à travers un code de conduite national et une charte d'éthique partagée ; et une coopération structurée avec les autorités compétentes (ANSSI, CNIL, Campus Cyber, etc.), afin d'éviter toute dérive ou auto-proclamation.

Vers une cybersécurité humanitaire

La cybersécurité n'est pas seulement une affaire d'États ou d'entreprises : elle est devenue une condition de survie humanitaire.

En 2025, Hack4Values continue de se développer, organise des événements de Live Hacking solidaire (notamment au ministère de l'Économie à Paris, avec plus de 50 *hackers* mobilisés), et ambitionne de couvrir l'ensemble des 17 Objectifs de Développement Durable de l'Onu.

Nous croyons à une cybersécurité offensive mais profondément humaine : centrée sur la confiance, la collaboration et la protection des plus vulnérables.

Conclusion

Protéger une ONG d'une cyberattaque, c'est protéger les populations qu'elle aide, les donateurs qui la soutiennent et la société tout entière.

Hack4Values démontre qu'il est possible de bâtir une cybersécurité solidaire, durable et positive.

Notre conviction est simple : en reconnaissant et en soutenant les *hackers* éthiques, nous renforcerons notre résilience collective. Car face aux menaces numériques, la seule vraie arme, c'est la coopération.

Intégration de la cybersécurité dans les métiers industriels

Par Fabrice BRU
Président du Club des Experts de la Sécurité
de l'Information et du Numérique (CESIN)

Longtemps focalisée sur la sûreté de fonctionnement et la sécurité physique, l'industrie a pris conscience tardivement de la menace numérique, révélée par Stuxnet (2010), WannaCry/NotPetya (2017) puis les vagues d'attaques de 2021-2022. Dans un contexte géopolitique marqué par l'action de groupes *proxies* d'État menant désinformation et cyberattaque[1] pour affaiblir les économies et institutions, la cybersécurité industrielle devient un enjeu stratégique majeur. Or, la spécificité des systèmes d'information industriels en complexifie la protection.

Cet article met en lumière trois leviers : intégrer le risque cyber dans les processus industriels, développer des technologies hybrides IT/OT (jumeaux numériques, IoT, convergence des protocoles) et investir dans des compétences mixtes, à travers la formation continue, les cursus académiques et le partage entre pairs. L'intégration de la cybersécurité apparaît ainsi non comme une contrainte, mais comme un facteur de résilience, de performance et de compétitivité.

Introduction

La prise de conscience des risques numériques dans les environnements industriels (Operational Technology, OT) s'est révélée beaucoup plus tardive que dans le domaine des technologies de l'information (IT). Dès 1988, l'épisode du Morris Worm constitue un jalon fondateur de la cybersécurité : il démontre la vulnérabilité systémique des réseaux informatiques[2]. À l'inverse, dans les systèmes industriels, il faut attendre 2010 et la découverte du *malware* Stuxnet pour que s'impose l'idée qu'une attaque informatique puisse altérer physiquement un procédé industriel[3]. Les campagnes massives de rançongiciels WannaCry et NotPetya en 2017, puis les vagues d'attaques de 2021-2022 (notamment contre des hôpitaux[4]), ont confirmé que la menace numérique pèse désormais directement sur la continuité des systèmes d'information industriels[5]. Comme le rappelle l'Agence

[1] CSIS, 18 mars 2025 : https://www.csis.org/analysis/russias-shadow-war-against-west

[2] BDM, 28 janvier 2025 : https://www.blogdumoderateur.com/histoire-morris-worm-premiere-cyberattaque-internet/

[3] Wikipedia Stuxnet : https://fr.wikipedia.org/wiki/Stuxnet

[4] DSIH, 29 octobre 2024 : https://dsih.fr/articles/5664/comment-les-hopitaux-de-plus-en-plus-cibles-se-protegent-contre-les-cyberattaques

[5] Dragos, 2025 : https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf?hsLang=en

nationale de la Sécurité des systèmes d'information[6] dans sa Méthode de classification des systèmes industriels, les environnements OT présentent des spécificités propres : durée de vie très longue des équipements, contraintes de disponibilité et de latence, protocoles hétérogènes, et culture organisationnelle centrée sur la sûreté de fonctionnement. Ces caractéristiques expliquent une intégration encore partielle de la cybersécurité dans les référentiels industriels. Trois enjeux se dessinent pour combler ce déficit : intégrer la cybersécurité dans le processus industriel, favoriser le développement de technologies hybrides IT/OT, et développer des compétences mixtes.

Intégrer le risque cybersécurité dans le processus industriel

Une culture du risque centrée sur la sûreté et la sécurité des personnes

Depuis plusieurs décennies, l'industrie s'appuie sur une gestion très mature des risques liés à la sûreté et à la sécurité. Les méthodes d'analyse de risques (AMDEC, HAZOP, arbres de défaillance) visent à protéger les personnes, les installations et l'environnement. Toutefois, l'événement cyber reste souvent absent de ces analyses, alors même qu'une attaque informatique peut impacter directement les personnes, les installations et dégrader considérablement les indicateurs stratégiques suivis par une usine, tels que le compte de résultat ou la performance des lignes de production[7].

Spécificités des systèmes industriels

Plusieurs facteurs propres à l'OT compliquent l'intégration du risque cyber :

- Durées d'amortissement longues : une chaîne de production industrielle peut rester en service plus de 20 ans, bien au-delà des cycles de sécurité numérique. Le maintien en condition de sécurité des procédés industriels doit donc être adapté.
- Référentiels distincts : le modèle Purdue pour la sécurité des systèmes industriels (ICS) ou la norme IEC 62443 s'adressent aux environnements OT, viennent compléter le modèle OSI et les normes ISO 27xxx. Cette dualité demeure encore peu connue des informaticiens[8].
- *Lean management* et excellence opérationnelle : la recherche de performance (réduction des gaspillages, amélioration continue) favorise l'usage accru des données de production, mobilisant ressources et outils *cloud*[9]. Cette évolution accroît la porosité IT/OT et introduit de nouveaux risques liés à l'intelligence artificielle et aux solutions *cloud*[10].

[6] ANSSI, 2022 : https://cyber.gouv.fr/sites/default/files/document/anssi-guide-systemes_industriels-methode_de_classification_v2-0.pdf.pdf

[7] Fortinet, 9 juillet 2025 : https://www.fortinet.com/fr/corporate/about-us/newsroom/press-releases/2025/fortinet-report-ot-cybersecurity-risk-elevates-within-executive-leadership-ranks

[8] IEC, 2018 : https://en.wikipedia.org/wiki/IEC_62443 et ISO27xxx : https://en.wikipedia.org/wiki/ISO/IEC_27001

[9] INRS, décembre 2023 : https://www.inrs.fr/media.html?refINRS=ED%206144

[10] Eurostat, décembre 2023 : https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Cloud_computing_as_a_service_model_for_meeting_enterprises.E2.80.99_ICT_needs

Intégrer l'événement cyber dans les analyses de risques

L'événement cyber doit désormais figurer explicitement dans les analyses de risques industrielles. En effet, le *big data* et l'intelligence artificielle représentent des promesses de gains significatifs de la performance industrielle. Cela permet de concevoir des plans de couverture intégrant des mesures numériques, physiques ou contractuelles (par exemple *via* une cyberassurance). La mise en place d'un centre opérationnel de cybersécurité OT (SOC OT) devient une étape clé. Celui-ci exige des technologies adaptées aux protocoles OT et des analystes formés à la cybersécurité industrielle, capables de dialoguer avec les métiers. Enfin, les organisations doivent disposer de plans de continuité d'activité (PCA) et de reprise après sinistre (PRA) spécifiquement adaptés aux environnements industriels, afin d'assurer une résilience minimale en cas de compromission[11].

Favoriser le développement de technologies hybrides IT/OT

Contraintes d'expérimentation et essor du jumeau numérique

Dans l'industrie, il n'existe qu'un seul environnement critique : la production. À la différence de l'IT, il est impossible de tester dans des environnements distincts (développement, intégration, préproduction). Le jumeau numérique apparaît alors comme une solution clé, permettant de simuler l'impact d'une modification ou d'une cyberattaque sans perturber l'usine réelle[12]. Sa généralisation constitue un enjeu majeur des prochaines années.

IoT industriel et équipements connectés

La diffusion de l'IoT transforme en profondeur les usines : capteurs, véhicules autoguidés (AGV), convoyeurs intelligents et tablettes de contrôle prolifèrent. Ces dispositifs accroissent la productivité, mais nécessitent une gestion centralisée et sécurisée de la flotte, idéalement intégrée aux standards IT[13].

Accès distants et convergence des protocoles

La télémaintenance et la connexion croissante des systèmes industriels à Internet augmentent la surface d'attaque. Les solutions de protection doivent être capables d'interpréter à la fois les protocoles IT (TCP/IP) et OT (Modbus, Profinet, OPC UA). La convergence technologique est indispensable pour éviter la multiplication des standards et garantir une supervision unifiée[14].

[11] Secomea, 2025 : https://secomea.com/blog/ot-security-trends/ot-cybersecurity-year-in-review-and-key-takeaways-for-2025/

[12] APEC, 2025 : https://corporate.apec.fr/files/live/sites/corporate/files/Espace%20M%C3%A9dias/pdf/Cybersecurite_industrielle.pdf

[13] TXOne, 2024 : https://digital.txone.com/media/txone-networks-2024-annual-ics-ot-cybersecurity-report/

[14] Zero Networks, 6 mai 2025 : https://zeronetworks.com/blog/ot-security-trends-2025-escalating-threats-evolving-tactics

Les menaces persistantes liées aux supports amovibles

Si la mise à jour par clé USB a quasiment disparu des environnements IT, elle demeure fréquente dans l'industrie. Ces supports constituent un vecteur de risque majeur : infection, sabotage, espionnage. Le développement de technologies spécifiques de contrôle et de décontamination reste une priorité pour limiter ces attaques[15].

Développer des compétences mixtes

Sensibiliser et former tous les acteurs

Une stratégie de cybersécurité industrielle repose sur l'engagement de tous, du dirigeant à l'opérateur. Sans un appui fort du top management, toute démarche cyber restera limitée, voire inefficace. La directive NIS2, qui s'appliquera prochainement à de nombreux secteurs industriels en Europe, impose déjà une responsabilisation accrue des dirigeants[16]. Cette exigence doit cependant être étendue à l'ensemble du tissu industriel, au-delà des seules entités essentielles ou importantes.

Construire des équipes pluridisciplinaires

La convergence IT/OT ne peut se limiter aux aspects techniques ; elle repose également sur une collaboration humaine et organisationnelle. La constitution d'équipes mixtes, associant automaticiens et experts cybersécurité IT, favorise l'émergence d'un vocabulaire commun et d'une confiance réciproque. Ces conditions sont indispensables pour trouver le juste équilibre entre performance industrielle et réduction du risque cyber. Une gouvernance cohérente entre entités garantit que la sécurité ne soit pas perçue comme un frein, mais comme un facteur de compétitivité.

Développer de nouvelles compétences hybrides et partager les savoirs

Les besoins croissants en profils mixtes (automaticiens formés à la cybersécurité, spécialistes IT connaissant l'OT, experts du jumeau numérique) nécessitent un effort massif et concerté sur trois volets complémentaires :

- Formation continue en entreprise : de nombreux industriels mettent en place des programmes internes de spécialisation cyber pour les automaticiens, ou de sensibilisation des équipes IT aux contraintes industrielles. Ces initiatives peuvent s'appuyer sur des services externes ou être développées en interne.
- Formation académique initiale : les écoles d'ingénieurs et universités ouvrent progressivement des filières hybrides, intégrant cybersécurité industrielle et modélisation numérique[17].
- Partage entre pairs et communautés professionnelles : au-delà des dispositifs formels de formation, les associations professionnelles jouent un rôle clé. Ainsi, la communauté industrielle du CESIN (Club des Experts de la Sécurité de l'Information et du Numé-

[15] SANS, mars 2025 : https://info.opswat.com/hubfs/OT%20-%20Assets/Survey_2025-ICS-OT-Budget.pdf

[16] NIS2, 14 décembre 2022 : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32022L2555

[17] France Compétence, 18 juillet 2025 : https://www.francecompetences.fr/app/uploads/2025/07/Liste-Metiers-en-evolution-ou-en-emergence_juillet_2025.pdf

rique) fédère une communauté de directeurs cybersécurité OT pour débattre, partager, documenter et promouvoir leur expérience[18]. Cette communauté intervient lors de salons professionnels pour sensibiliser aux menaces susceptibles de fragiliser la performance des chaînes de production industrielle, dans le contexte géopolitique actuel. Enfin, les RSSI Industriels ont également l'opportunité d'échanger et de débattre avec d'autres associations et fédérations d'équipementiers et contribuent à la rédaction de livres blancs (GIMELEC[19]).

Conclusion

L'intégration de la cybersécurité dans les métiers industriels s'impose comme un impératif stratégique. L'analyse a montré que si la culture du risque est historiquement solide dans l'industrie, elle demeure trop centrée sur la sûreté et la sécurité physique, négligeant encore l'événement cyber. Les spécificités des environnements OT imposent d'adapter les référentiels, de mettre en place des SOC OT et de déployer des PCA/PRA adaptés. La convergence IT/OT, portée par les jumeaux numériques, l'IoT, la télémaintenance et la gestion des supports amovibles, et l'intelligence artificielle reste encore inachevée. Enfin, la réussite de cette transformation repose sur les compétences humaines. La directive NIS2 constitue un levier de responsabilisation, mais seule une stratégie concertée de formation – académique et continue – permettra de combler le déficit de ressources et d'ancrer durablement une culture cyber industrielle.

Bibliographie

ANSSI (2022), « Méthode de classification des systèmes industriels », Paris.

APEC (2023), « Profils cybersécurité industrielle », Paris.

BUSINESS RESEARCH INSIGHTS (2023), "Operational technology cybersecurity market 2023-2033".

CSIS (2025), "Russia's shadow war against the West", Washington, Center for Strategic and International Studies.

DRAGOS (2025), "OT cybersecurity report: A year in review".

DSIH (2024), « Comment les hôpitaux (de plus en plus ciblés ?) se protègent contre les cyberattaques ».

ENISA (2023), "Threat landscape for industrial control systems", Athènes, ENISA.

EUROSTAT (2023), "Cloud computing – Statistics on the use by enterprises", Bruxelles, Commission européenne.

FORTINET (2025), "OT cybersecurity risk elevates within executive leadership ranks".

FRANCE COMPÉTENCES (2025), « Liste des métiers en évolution ou en émergence ».

GIMELEC (2025), « Cyber OT – Maintien en condition de sécurité ».

GMI INSIGHTS (2023), "Industrial cybersecurity market report 2023-2032".

[18] CESIN : https://cesin.fr/articles-slug/?slug=366-Lab+Industriel+-+Livrables+-+Guide+de+suivie+du+RSSI+en+environnement+industriel

[19] GIMELEC, Cyber OT : publication du Livre blanc « Maintien en condition de sécurité », https://gimelec.fr/cyber-ot-poublication-du-livre-blanc-maintien-en-condition-de-securite/

IEC (2018), “Norme IEC 62443 – Security for industrial automation and control systems”, Genève, IEC.

INRS (2021), « Lean manufacturing – Définition et risques associés », ED 6144, Paris, INRS.

ISO (2018), “ISO/IEC 27001 – Information security management systems”, Genève, ISO.

LANGNER R. (2011), “Stuxnet: Dissecting a cyberwarfare weapon”, *IEEE Security & Privacy*, 9(3), pp. 49–51.

OPSWAT (2025), “ICS-OT Budget Survey”.

RANSOMWARE.LIVE (2025), “Plateforme de suivi des victimes et activités des groupes de ransomware”, Hudson Rock, https://www.ransomware.live/

SECOMEA (2025), “OT cybersecurity year in review & key takeaways”.

SPAFFORD E. H. (1989), “The internet worm program: An analysis”, Purdue Technical Report CSD-TR-823.

TXOne NETWORKS (2024), “Annual ICS-OT Cybersecurity Report”.

UNION EUROPÉENNE (2022), « Directive NIS2 », Bruxelles, Parlement européen.

ZERO NETWORKS (2025), “OT security trends: Defending against escalating threats and evolving tactics”.

Revue nationale stratégique, OS12 – vers une stratégie nationale de cybersécurité 2025-2030

Par Jonathan COLLAS
Conseiller industrie et numérique au Secrétariat général de la défense et de la sécurité nationale (SGDSN)

La Revue nationale stratégique 2025 a fixé l'ambition d'une résilience cyber de premier rang, dans un monde marqué par l'hybridation des menaces et la dépendance accrue aux infrastructures numériques. La Stratégie nationale de cybersécurité 2025-2030 en est la déclinaison opérationnelle. Elle fait le choix de la consolidation : capitaliser sur plus de quinze ans d'expériences – de la création de l'ANSSI aux stratégies successives, de la Revue stratégique de cyberdéfense au plan France 2030 – pour franchir un cap.

Cinq piliers structurent cette ambition : développer les talents, renforcer la résilience nationale, entraver la menace, maîtriser les fondements numériques et agir en Europe et à l'international. Obligations proportionnées, accompagnement, gouvernance ouverte et mobilisation de la filière française se combinent pour donner à la France et à l'Europe la confiance nécessaire face aux défis du cyberespace.

Introduction

La Stratégie nationale de cybersécurité 2025-2030 s'inscrit dans la continuité d'un effort engagé depuis plus de 15 ans et constitue la déclinaison directe de la Revue nationale stratégique 2025. Elle ne se contente pas d'ajouter un plan de plus : elle consolide les acquis, répond à l'évolution de la menace et trace une trajectoire claire vers une résilience cyber de premier rang. Pour en mesurer la portée, il convient de rappeler le contexte stratégique et institutionnel qui la rend nécessaire, avant d'en présenter les grands piliers et la méthode de mise en œuvre.

Au-delà de ces piliers, quelques idées fortes structurent la démarche française. La consolidation en est le fil conducteur : il ne s'agit pas de repartir de zéro, mais de capitaliser et d'accélérer sur les bases déjà construites. Les talents occupent une place centrale, car la ressource humaine demeure la condition *sine qua non* de toute résilience. La stratégie entend également banaliser la gestion de crise par la prévention et la généralisation des exercices, afin d'entraîner l'ensemble de la Nation.

Elle repose sur une logique de proportionnalité : des obligations claires et exigeantes, mais adaptées à la criticité des acteurs, complétées par des dispositifs d'accompagnement pour garantir un changement d'échelle soutenable. Elle affirme aussi la nécessité d'une entrave crédible de la menace, en mobilisant tous les leviers disponibles, y compris l'attribution publique lorsque cela s'avère nécessaire.

La maîtrise des fondations numériques constitue une autre priorité. Cryptographie, évaluation, certification et développement d'une industrie européenne robuste sont

indispensables pour garantir la sécurité, la confiance et la résilience de nos systèmes numériques. Elle contribue également à renforcer notre capacité – et notre autonomie – d'action en cas d'incident majeur. L'Europe joue ici un rôle de multiplicateur de puissance à travers ses instruments, ses réseaux, la réserve cyber de l'Union, ainsi que des coopérations pragmatiques avec l'OTAN, qui renforcent l'interopérabilité, le partage d'alertes et la préparation collective face aux menaces.

Enfin, la stratégie affirme la cybersécurité comme une véritable politique publique conduite sous l'autorité du Premier ministre, exercée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) et l'ANSSI. Elle nécessite une gouvernance ouverte, associant au-delà des administrations spécialisées, les collectivités, les entreprises, la recherche, la société civile et les communautés professionnelles comme Inter-CERT, dans un jeu coordonné et transparent.

Ces principes expriment à la fois la philosophie et la méthode françaises : une démarche de consolidation, d'ouverture et de responsabilité partagée.

Pourquoi une nouvelle stratégie nationale ?

Un environnement stratégique en mutation

La « révolution numérique » est l'une de ces ruptures silencieuses qui transforment le monde plus sûrement que les fracas de l'histoire. Nos vies, nos économies et nos institutions reposent désormais sur des infrastructures critiques et des flux de données dont la vulnérabilité fait peser un risque systémique. Le cyberespace est devenu un théâtre de puissance, reflet et prolongement des tensions géopolitiques. C'est un espace de compétition, de contestation et parfois d'affrontement désinhibé, où s'entrecroisent espionnage, sabotage, extorsion et désinformation.

Comme ses partenaires, la France fait face à une menace intense, diffuse et polymorphe. Elle touche tous les pans de la société : administrations, collectivités, hôpitaux, entreprises stratégiques comme PME, universités ou associations. Les cyberattaques – qu'elles soient étatiques, criminelles ou hybrides – peuvent causer des dommages considérables, allant du vol de données sensibles à la paralysie d'infrastructures vitales. Elles affectent aussi la chaîne de valeur économique et fragilisent la confiance collective.

Ces pressions s'exercent particulièrement sur les technologies de rupture : *cloud* concentrant des données critiques, intelligence artificielle générant de nouveaux vecteurs d'attaque, informatique quantique susceptible de mettre en défaut les mécanismes cryptographiques actuels. Dans un tel contexte, la cybersécurité n'est plus seulement un enjeu technique : elle devient un impératif stratégique conditionnant la souveraineté, la prospérité et la sécurité nationale.

La continuité d'une vision française

Depuis le Livre blanc sur la défense et la sécurité nationale de 2008, la France a progressivement bâti un modèle de cybersécurité solide et reconnu : séparation des volets défensif et offensif, création d'une agence nationale dédiée (ANSSI), montée en puissance d'une filière industrielle et scientifique, ancrage européen et international.

Les stratégies de 2011 et 2015 ont constitué une première réponse structurée face aux menaces. La Revue stratégique de cyberdéfense de 2018 a consacré la nécessité d'une doctrine claire, en consolidant le modèle français. En 2021, un milliard d'euros a été mobilisé dans le cadre du plan France 2030 pour accélérer le développement des capacités industrielles et scientifiques nationales.

Cette trajectoire a permis à la France de se doter d'un capital d'expérience unique : une ressource humaine qualifiée, des centres de recherche de pointe, des acteurs publics et privés mobilisés collectivement, ainsi que des capacités défensives et offensives crédibles.

La déclinaison de la Revue nationale stratégique 2025

Pour autant, la nature des cyberattaques évolue rapidement : hybridation croissante entre acteurs étatiques et cybercriminels, intensification des campagnes de sabotage ou d'espionnage, multiplication d'outils intrusifs disponibles sur le marché noir. Cette réalité appelle une adaptation constante.

La Revue nationale stratégique 2025 fixe pour la France l'ambition d'une résilience cyber de premier rang, en faisant de la cybersécurité un pilier de sa défense globale. La Stratégie nationale de cybersécurité 2025-2030 en est la déclinaison opérationnelle. Elle ne procède pas d'une rupture, mais d'une logique de consolidation : capitaliser sur plus de 15 ans d'efforts, tout en adaptant nos dispositifs à l'intensification et à la systémisation de la menace.

Les grands piliers de la stratégie nationale 2025-2030

La Stratégie nationale de cybersécurité 2025-2030 repose sur cinq piliers complémentaires, qui traduisent l'ambition française de bâtir une résilience cyber de premier rang. Ensemble, ils dessinent un cadre d'action cohérent, articulant formation, prévention, entrave, maîtrise technologique et coopération internationale.

Pilier 1 – Faire de la France le plus grand vivier de talents cyber d'Europe

La capacité de la France à disposer d'une main-d'œuvre qualifiée est la condition *sine qua non* de toute résilience. Face à une pénurie mondiale de compétences, la stratégie place les talents au premier rang des priorités. L'action se déploie à trois niveaux.

Dès le plus jeune âge, il s'agit de diffuser une culture inclusive de la cybersécurité, en l'intégrant aux parcours éducatifs et civiques, avec une attention particulière à l'égalité de genre et à l'ouverture sociale. Dans la formation et la reconversion, une plateforme nationale d'orientation sera mise en place, appuyée par des outils de formation continue et des passerelles renforcées entre disciplines scientifiques, mais aussi entre secteurs public et privé. Enfin, à l'échelle européenne, la France soutient la création d'un socle commun de compétences, la mobilité professionnelle et l'émergence de cursus harmonisés. L'objectif est clair : transformer une contrainte mondiale en avantage stratégique, en faisant de la France le plus grand vivier de talents cyber d'Europe.

Pilier 2 – Renforcer la résilience cyber de la Nation

Dans un contexte où les attaques deviennent de plus en plus systémiques, la résilience doit être l'affaire de toute la Nation. La stratégie engage une politique ambitieuse de prévention et de sensibilisation, incarnée par une marque nationale sur le modèle des grandes campagnes de santé publique ou de sécurité routière. Elle s'appuie également sur un vaste programme d'exercices de crise multi-niveaux – territoriaux, sectoriels, nationaux, européens – afin de banaliser la gestion de crise et de tester l'articulation des réponses.

Le niveau de cybersécurité sera relevé de façon proportionnée : des obligations fortes pour les services et infrastructures vitaux, alignées sur la directive NIS2 ; un accompagnement

spécifique pour les acteurs les moins matures ; et des incitations adaptées pour le reste du tissu économique et social. Enfin, pour faciliter l'accès aux dispositifs, la stratégie prévoit des parcours simplifiés, avec la création d'un portail national de la cybersécurité du quotidien et l'intégration de la plateforme 17Cyber comme guichet unique pour les victimes de cybermalveillance. En somme, il s'agit d'entraîner la Nation entière à faire face à la menace.

Pilier 3 – Entraver l'expansion de la cybermenace

La France choisit de rendre les cyberattaques plus coûteuses et plus risquées pour leurs auteurs, en mobilisant tous les leviers disponibles : judiciaires, techniques, diplomatiques, militaires et économiques. Le Centre de coordination des crises cyber (C4), placé sous l'autorité du SGDSN, voit son rôle renforcé pour fédérer l'ensemble des administrations compétentes, au-delà du cercle initial (ANSSI, COMCYBER, DGSE, DGSI, DGA, MEAE). Il peut désormais proposer à l'autorité politique une palette d'options allant jusqu'à l'attribution publique des auteurs d'attaques.

La stratégie renforce également le partenariat avec les acteurs privés, en particulier *via* la communauté InterCERT France et la mise en place d'un filtre de cybersécurité destiné au grand public. Elle consolide enfin l'ancrage européen, notamment par le recours au régime de sanctions issu de la Cyber Diplomacy Toolbox de l'UE[1] et par un partage accru d'informations opérationnelles entre États membres.

Pilier 4 – Garder la maîtrise de la sécurité de nos fondements numériques

L'économie et la société reposent sur des technologies critiques – réseaux, systèmes d'exploitation, cloud, logiciels, cryptographie – dont la vulnérabilité peut entraîner des conséquences durables. La stratégie vise à réduire nos dépendances en soutenant l'industrie française et européenne de cybersécurité, grâce à l'innovation, à la consolidation et à l'export.

Dans le cadre du plan France 2030, plus d'un milliard d'euros ont été mobilisés pour développer cette filière. Cet effort s'accompagne d'un soutien accru à l'internationalisation des entreprises françaises, reconnaissant que le seul marché national ne suffit pas pour assurer leur montée en puissance. À titre d'exemple, en janvier 2025, Business France et ses partenaires ont ainsi conclu un accord visant à accroître la visibilité de l'écosystème français à l'étranger : cartographie des acteurs et des marchés prioritaires, identification des besoins émergents et déploiement d'actions concrètes pour soutenir l'export.

Enfin, la stratégie anticipe les ruptures technologiques – cryptographie post-quantique, intelligence artificielle, *cloud* – afin de sécuriser dès aujourd'hui les systèmes de demain, de prévenir les nouvelles vulnérabilités qu'elles emportent et de préserver notre capacité à détecter, protéger et agir face aux cybermenaces futures.

[1] Le Conseil de l'Union européenne a mis en place en mai 2019 un cadre juridique permettant d'imposer des mesures restrictives ciblées à l'encontre de personnes physiques ou morales, ainsi que d'États, responsables de cyber-attaques majeures, ou ayant fourni un soutien financier, technique ou matériel à de telles attaques. Le Conseil l'a récemment appliqué, en janvier 2025, en inscrivant trois individus de l'unité 29155 du GRU (renseignement militaire russe) pour une série de cyber-attaques contre l'Estonie en 2020.

Pilier 5 – Soutenir la sécurité et la stabilité du cyberespace en Europe et à l'international

La France affirme sa vocation à être une puissance cyber responsable, contribuant à la sécurité collective et à la stabilité du cyberespace. Cet engagement passe par la promotion d'un cyberespace sûr, ouvert et démocratique, fidèle aux valeurs européennes. Il se traduit également par une participation active aux grandes initiatives internationales, telles que l'ONU, l'Appel de Paris[2], le Processus de Pall Mall[3] ou encore l'Appel d'Accra[4].

La stratégie consolide aussi les dispositifs européens de coopération : réseau CSIRT, mécanisme CyCLONe, réserve cyber de l'UE et réponses coordonnées en cas d'attaque majeure. Ce pilier fait de l'Europe un multiplicateur de puissance, garantissant que la cybersécurité soit à la fois un levier d'influence et un impératif de protection.

La méthode française : proportion, accompagnement, gouvernance ouverte

Proportion : des exigences adaptées à la criticité

La France a fait le choix d'une approche proportionnée, qui distingue les obligations selon la criticité des entités. Les services et infrastructures les plus vitaux – administrations de l'État, opérateurs d'importance vitale, infrastructures critiques – doivent atteindre un niveau de sécurité très élevé, capable de résister aux attaques les plus sophistiquées. Pour un périmètre plus large d'entités, les obligations sont fixées en cohérence avec la directive NIS2, garantissant une harmonisation européenne et une extension progressive du champ de la cybersécurité réglementée. Enfin, pour l'ensemble du tissu économique et social non soumis à régulation, l'État privilégie l'incitation et le soutien, afin d'éviter une fracture entre organisations protégées et organisations vulnérables. Cette logique graduée vise à faire évoluer tout le pays, sans créer de décrochage.

Accompagnement : rendre la cybersécurité accessible à tous

La stratégie affirme que la cybersécurité doit être à la portée de tous. Elle prévoit la création d'un portail national de la cybersécurité du quotidien, conçu comme une porte d'entrée claire et pratique pour l'ensemble des publics. La plateforme 17Cyber en devient le guichet de référence pour les victimes, au-delà des seules entités soumises à des obligations particulières. Des programmes spécifiques sont prévus pour accompagner les

[2] L'Appel de Paris du 12 novembre 2018 pour la confiance et la sécurité dans le cyberespace est un appel à réagir ensemble face aux nouvelles menaces qui mettent en danger les citoyens et les infrastructures. Il s'articule autour de neuf principes communs de sécurisation du cyberespace, https://pariscall.international/fr/principles

[3] Le processus de Pall Mall est devenu la principale plateforme multi-acteurs pour échanger sur les normes et standards régissant le développement, l'achat, le transfert et l'utilisation des capacités d'intrusion cyber disponibles sur le marché. Il s'inscrit dans la continuité des efforts initiés par l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, en application du cadre international existant pour un comportement responsable des États. Sa deuxième conférence s'est tenue à Paris les 3 et 4 avril 2025. Il comprenait alors 27 États.

[4] L'Appel d'Accra, lors de la Conférence mondiale sur le renforcement des capacités cyber (GC3B) du 29 au 30 novembre 2023, demande aux gouvernements et aux organisations mondiales d'intégrer la cybersécurité dans les cadres de développement et les stratégies de coopération internationale, afin de renforcer la résilience numérique.

acteurs les moins matures, en particulier les collectivités et les PME. Un label de confiance permettra de valoriser les efforts de sécurisation, contribuant ainsi à une dynamique vertueuse dans les chaînes de valeur économiques. Enfin, l'accompagnement s'appuiera sur un maillage territorial et sectoriel, grâce à des relais locaux et professionnels qui feront vivre la cybersécurité au plus près des réalités de terrain.

Gouvernance ouverte et partagée

Le pilotage de la stratégie repose sur une gouvernance ouverte, pensée comme une véritable politique publique de cybersécurité, à la hauteur d'un défi qui engage l'ensemble de la Nation. Sous l'autorité du Premier ministre, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) assure la coordination, en lien étroit avec l'ANSSI et les grands ministères concernés.

Lorsqu'il s'agit de répondre à une cyberattaque d'ampleur, le Centre de coordination des crises cyber (C4) occupe une place centrale : il fédère les compétences de l'ANSSI, du COMCYBER, de la DGSE, de la DGSI, de la DGA et du ministère de l'Europe et des Affaires étrangères, et propose des options à l'autorité politique, y compris l'attribution publique des attaques.

Mais cette architecture ne se limite pas à la gestion de crise. La France fait de la cybersécurité une politique publique dont la gouvernance se veut ouverte et inclusive : elle associe les collectivités territoriales, les entreprises, les organisations professionnelles, le monde académique et la société civile. Les communautés d'experts, comme InterCERT France, en constituent des relais essentiels.

Enfin, cette ouverture dépasse les frontières nationales : elle trouve naturellement son prolongement dans les dispositifs européens (réseau CSIRT, CyCLONe, réserve cyber de l'UE) et internationaux.

Conclusion – La consolidation comme méthode, 2030 comme cap

La Stratégie nationale de cybersécurité 2025-2030 s'inscrit dans la continuité des efforts engagés depuis plus de 15 ans et dans la déclinaison directe de la Revue nationale stratégique 2025. Elle ne prétend pas réinventer l'existant mais le consolider, en l'adaptant à l'intensification et à la systématisation de la menace.

Cette stratégie repose sur une conviction forte : la cybersécurité n'est pas un domaine réservé aux experts, mais une condition, parmi d'autres, de la souveraineté, de la prospérité et de la liberté collectives. Elle s'articule autour de cinq piliers clairs, portés par une méthode singulièrement française : des obligations proportionnées, un accompagnement accessible, une gouvernance ouverte et partagée.

L'objectif est unique et mobilisateur : hisser la France au rang des nations de cybersécurité de premier plan. D'ici 2030, ce cap se traduira par des milliers de talents formés, une Nation entraînée à gérer les crises, une menace mieux entravée, une maîtrise renforcée des fondements numériques grâce à la mobilisation de la filière française et une voix française et européenne crédible dans la gouvernance internationale du cyberespace.

La consolidation, en somme, c'est la garantie de capitaliser sur ce qui a été construit, d'élever le niveau de protection, et de donner à la France, à l'Europe et à leurs citoyens la confiance nécessaire pour aborder l'avenir numérique.

Bibliographie

Livre blanc sur la défense et la sécurité nationale, 2008.

Stratégie de la France en matière de défense et de sécurité des systèmes d'information, 2011, Secrétariat général de la défense et de la sécurité nationale (SGDSN).

Stratégie nationale pour la sécurité du numérique, 2015, SGDSN.

Revue stratégique de cyberdéfense, 2018, SGDSN.

Stratégie nationale d'accélération pour la cybersécurité, 2021, Gouvernement – Plan France 2030.

Revue nationale stratégique 2025, 2025, SGDSN.

Cybersécurité et métiers du numérique : un enjeu stratégique pour l'État

Par Stéphanie SCHAER
Directrice interministérielle du numérique (DINUM)

À l'heure où la transformation numérique s'accélère au sein des administrations, la cybersécurité devient un enjeu stratégique qui engage directement la qualité du service public et dépend étroitement des ressources humaines dédiées. Les cyberattaques qui visent les institutions rappellent une évidence : la sécurité des systèmes dépend autant des technologies que des femmes et des hommes qui les utilisent. Attirer les talents, former et sensibiliser l'ensemble des agents, développer une culture partagée : telles sont les conditions auxquelles s'emploie au quotidien la direction interministérielle du numérique (DINUM) pour renforcer la résilience de l'État et affirmer sa souveraineté numérique.

La transformation numérique de l'administration française a profondément modifié la place des métiers du numérique. Longtemps cantonnés à une fonction de support technique, ils constituent désormais une capacité stratégique au même titre que la logistique, la sécurité ou les finances publiques. Le rapport conjoint de l'Inspection générale des Finances et du Conseil général de l'Économie (IGF–CGE, 2023) avait dressé un constat sans appel : l'État doit recruter 3 500 agents supplémentaires dans les métiers du numérique en cinq ans. La pression est particulièrement forte sur la cybersécurité, où la croissance et la sophistication des attaques imposent un renforcement rapide des équipes.

Dans ce contexte, la direction interministérielle du numérique (DINUM) agit comme DRH inter- ministérielle de la filière numérique. Sa mission est claire : attirer, fidéliser et former les talents, tout en accompagnant la professionnalisation des agents déjà en poste, en travaillant à ces objectifs en lien étroit avec l'ensemble de la communauté interministérielle, tant les services RH ministériels que les directions du numérique au sein de chaque pôle ministériel.

En matière de cybersécurité comme pour d'autres verticales du numérique, les enjeux sont loin d'être une affaire exclusivement technique mais engagent directement les ressources humaines qui conditionnent la qualité même du service public.

Les administrations publiques à l'épreuve des attaques cyber

Les administrations publiques sont devenues des cibles de choix pour les cybercriminels, en raison des données sensibles qu'elles détiennent et de la criticité de leurs missions. En mars 2024, une attaque a visé de très nombreux services numériques hébergés sur le Réseau interministériel de l'État. Plus récemment, plusieurs hôpitaux des Hauts-de-France ont vu leurs serveurs attaqués, compromettant l'identité de milliers de patients.

Ces exemples, loin d'être exhaustifs, révèlent une réalité : la cybersécurité ne peut se limiter aux infrastructures techniques. Elle repose aussi sur la vigilance quotidienne et la

réactivité d'agents publics capables de comprendre, d'anticiper et de contrer les risques. Former et sensibiliser devient alors un impératif stratégique pour garantir la continuité des services publics et préserver la confiance des citoyens.

Le facteur humain : première vulnérabilité, premier levier

Près de 80 % des incidents trouvent leur origine dans une erreur humaine : clic sur un lien piégé, mot de passe insuffisant, configuration défaillante. La première ligne de défense, ce sont donc les agents eux-mêmes. Recruter des experts cyber est indispensable, mais insuffisant.

La véritable force de l'État réside dans sa capacité à faire de chaque agent, quel que soit son métier, un maillon actif de la cyber-protection.

La montée en compétences de l'ensemble des agents passe par des dispositifs dédiés. Le Campus du numérique public, inauguré en janvier 2024, développe ainsi des modules spécifiques de sensibilisation. En diffusant une culture commune de sécurité, il contribue à transformer une vulnérabilité structurelle en levier de résilience.

Le rôle stratégique des ressources humaines

La cybersécurité révèle une évidence trop souvent négligée : les enjeux ne sont pas uniquement techniques, mais profondément humains et organisationnels. La robustesse d'une filière repose sur des politiques cohérentes de recrutement, de formation, de mobilité et d'accompagnement de carrière. C'est pourquoi directions numériques et directions RH travaillent de concert pour inscrire la sécurité dans les parcours professionnels, promouvoir la diversité et soutenir l'évolution des compétences.

Cette dimension touche aussi à l'expérience collaborateur : attirer et fidéliser des talents suppose de créer un environnement de travail qui donne envie de s'engager durablement. La DINUM déploie en interministériel des dispositifs inédits, tels que des programmes de stages et d'embarquement, des communautés apprenantes ou encore des programmes d'accompagnement. L'attention portée à la diversité et à la mixité dépasse l'exigence d'égalité : dans un domaine stratégique comme le numérique et la cybersécurité, il s'agit aussi d'un levier de performance et de souveraineté. Une feuille de route interministérielle spécifique a d'ailleurs été élaborée, articulant actions de sensibilisation, événements et réseaux de pairs.

Construire des carrières numériques attractives et durables

Cette politique RH doit néanmoins s'incarner dans des perspectives de carrière tangibles, surtout face à la concurrence d'un secteur privé particulièrement dynamique. La réinternalisation de 345 postes en 2024 témoigne de la volonté de l'État de maîtriser ses compétences critiques, notamment en *cloud* et cybersécurité. Le programme « Entrepreneurs d'intérêt général » offre, quant à lui, une passerelle entre expertise privée et missions publiques d'intérêt général. La publication d'un nouveau référentiel des rémunérations en 2024 permet par ailleurs de rapprocher les conditions offertes par l'État de celles du marché, sans renoncer à la spécificité des missions de service public.

Mais l'attractivité ne se conçoit pas sans fidélisation. La constitution d'une communauté interministérielle des ingénieurs du numérique, déjà forte de 300 membres, et le lancement du parcours Programme interministériel du numérique (PINUM) destiné aux

cadres A+ traduisent l'ambition de bâtir de véritables trajectoires professionnelles dans l'État. La mobilité interadministration, désormais encouragée et valorisée, complète cette dynamique et participe à l'ancrage d'une filière numérique publique capable de retenir ses talents tout en répondant aux besoins stratégiques du pays.

La formation, pilier de la souveraineté numérique

Si l'attractivité et la fidélisation sont des piliers emblématiques de la politique RH du numérique public, la formation constitue un troisième pilier fondamental qui nourrit d'ailleurs les deux autres. Le Campus du numérique public, en deux ans d'existence, s'est imposé comme un outil central de diffusion des compétences. Son action se déploie auprès des cadres dirigeants – 205 directeurs déjà formés – mais aussi de l'ensemble des agents : plus de 10 000 d'entre eux ont suivi en 2025 des modules consacrés à l'intelligence artificielle, tandis que des programmes spécifiques portent sur les méthodes agiles et sur l'évaluation des compétences *via* Pix.

Au-delà de la technicité, le Campus cherche à ancrer une culture commune, condition de la résilience collective. C'est particulièrement vrai en cybersécurité, où il coopère avec le Campus Cyber pour proposer des actions conjointes de sensibilisation et des parcours spécifiques destinés aux responsables publics.

La cybersécurité comme laboratoire des politique RH

La cybersécurité concentre toutes les tensions de la filière : besoins croissants, pénurie de talents, forte concurrence du privé. Elle impose à l'État de tester de nouvelles approches en matière de recrutement, de formation et de fidélisation. Dans ce domaine, l'État ne peut pas se limiter à former des experts hautement spécialisés ; il doit aussi sensibiliser l'ensemble de ses agents, bâtir des partenariats solides avec le secteur privé et s'appuyer sur le monde académique.

À ce titre, la cybersécurité joue un rôle de laboratoire : les solutions développées pour ce secteur, qu'il s'agisse d'attractivité, de formation ou de gouvernance, préfigurent celles qui pourront être généralisées à l'ensemble des métiers du numérique.

Une gouvernance collective pour une stratégie durable

L'ampleur des défis impose une gouvernance partagée. La DINUM agit aux côtés de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), des ministères, des collectivités et du Campus Cyber, dans une logique de réseau. Cette coopération permet de mutualiser expertises et retours d'expérience, de développer des programmes conjoints de formation et de sensibilisation, et d'accroître l'attractivité des carrières publiques. La France s'inscrit ainsi dans une dynamique européenne, la Commission ayant fixé l'objectif de former 20 000 experts cyber d'ici 2030.

Perspectives : vers une filière consolidée

L'année 2026 sera marquée par un approfondissement de ces dynamiques. La consolidation de la filière numérique publique ne se réduit pas à la modernisation technique ou à la création de nouveaux dispositifs : elle incarne une transformation profonde de l'action

publique. L'attractivité des talents, la construction de carrières durables, la montée en compétences et la coopération entre acteurs dessinent une politique RH inédite où les métiers de la cybersécurité jouent le rôle de catalyseur.

Au-delà des réponses immédiates aux menaces, il s'agit de bâtir une capacité d'anticipation et de résilience collective, condition indispensable à la continuité du service public et à la confiance des citoyens. En investissant dans ses métiers du numérique, l'État affirme une ambition claire : non pas subir la révolution numérique, mais la mettre au service de la souveraineté et de l'intérêt général.

Figures 1 et 2 : Les équipes de la DINUM (Source : DINUM).

Face au défi Cyber : entreprises et écoles, un duo essentiel

Par Sylvain GOUSSOT
Directeur général de l'EPITA, École d'ingénieurs en informatique

Et Marie MOIN
Directrice de SECURESPHERE, le centre de formation continue de l'EPITA

Volume et complexité croissants, évolutions technologiques majeures, risques économiques et réputationnels, tous ces éléments constituent le cocktail explosif des cybermenaces. Les entreprises et les institutions ont l'impérieuse nécessité de disposer de ressources suffisantes, compétentes et à l'état de l'art. Les dirigeants le savent bien : quand les compétences manquent et que l'exposition aux risques croît, il faut des plans d'action vigoureux et se tourner vers les acteurs proposant des ressources compétentes : c'est le cas des écoles d'ingénieurs du numérique, qui disposent à la fois d'une offre de formations initiales mais aussi d'une offre de formations continues. De l'autre côté du miroir, les écoles du numérique ont besoin des acteurs économiques pour adapter leurs formations et répondre à la demande. Ce duo apparaît comme indispensable pour former les équipes et contrer les menaces cyber d'aujourd'hui et de demain.

Les multiples facettes des professions de la « filière cyber »

La « filière cyber » désigne l'ensemble des métiers, compétences et acteurs qui contribuent à la sécurité des systèmes d'information et à la protection des données et infrastructures numériques. Elle englobe aujourd'hui un spectre extrêmement large de fonctions : de l'opérateur de supervision assurant le *monitoring* en temps réel d'un SOC (Security Operations Center), jusqu'au chercheur en cryptographie post-quantique, en passant par les analystes en réponse à incident, les ingénieurs en sécurité applicative, les architectes sécurité, les *pentesters*[1], les experts en *forensic*[2], les RSSI ou encore les conseillers en gouvernance et conformité réglementaire (RGPD, NIS2, DORA, etc.).

Cette diversité tient à la profonde transversalité de la cybersécurité : elle mobilise des savoirs et savoir-faire relevant de l'informatique, des télécoms, des mathématiques, mais

[1] Ou « *hacker* éthique », le pentester (de l'anglais "penetration testing" teste la résilience d'une entreprise ou organisation ou d'un système aux attaques cyber en jouant le rôle de l'attaquant pour détecter les failles.

[2] L'analyse forensique consiste à investiguer des systèmes d'information après un incident cyber, comme un piratage ou un vol de données. Elle analyse l'ensemble des données du SI pour comprendre ce qu'il s'est passé et en déduire les remédiations nécessaires.

aussi du droit, de la gestion des risques, de la psychologie comportementale ou encore de la communication de crise.

Loin de se limiter à un domaine purement technique, la filière cyber est devenue une filière stratégique, au croisement de multiples disciplines, qui irrigue l'ensemble des secteurs économiques et industriels.

Du point de vue des acteurs économiques, il serait contre-productif de n'aborder la filière cyber qu'à travers le prisme des formations d'ingénieurs. Les besoins en cybersécurité sont massifs et concernent tous les niveaux d'expertise :

- des profils opérationnels de niveau bac+2/bac+3 capables d'exécuter des procédures, de surveiller des journaux d'événements et de maintenir une infrastructure sécurisée ;
- des profils de niveau intermédiaire (bac+3/bac+4) capables de conduire des projets, d'automatiser des tâches de supervision, de configurer des politiques de sécurité ou d'administrer un SOC ;
- et des profils experts ou de pilotage stratégique (bac+5/doctorat) qui conçoivent des architectures sécurisées, auditent, innovent ou orientent la politique globale de cybersécurité d'une organisation.

Le ComCyber (Commandement de la cyberdéfense), rattaché à l'État-major des armées, illustre parfaitement cette logique : il recherche activement des titulaires de bachelors, et pas seulement des ingénieurs. Il a compris que le maillon opérationnel est le plus critique en volume et que le temps de montée en compétence de ces profils est bien plus court, ce qui en fait un levier essentiel pour résorber la pénurie.

Cette réalité du terrain explique l'essor des formations professionnalisantes dans la filière :

- BTS CIEL (Cybersécurité, Informatique et réseaux, Électronique), qui forment en 2 ans des techniciens capables de mettre en œuvre les bases de la sécurité réseau et système ;
- BUT Réseaux et Télécoms ou Informatique, qui permettent en 3 ans d'acquérir des compétences avancées en supervision, administration système et sécurité ;
- Bachelors cybersécurité dans les écoles spécialisées ou d'ingénieurs, qui forment en 3 ans des profils directement opérationnels sur les postes d'analyste SOC, de technicien sécurité ou de gestionnaire d'incidents.

Ces formations courtes sont très recherchées par les entreprises et les administrations, qui les perçoivent comme un réservoir immédiat de talents. Elles répondent aussi à une nécessité structurelle : le besoin de main-d'œuvre qualifiée dépasse très largement le vivier d'ingénieurs disponibles.

Lutter efficacement contre les cybermenaces, une affaire de management ?

En première approche, la cybersécurité est souvent perçue comme une affaire exclusivement technique. Cette représentation s'explique : les attaques informatiques exploitent des vulnérabilités complexes, et leur neutralisation requiert des compétences de haut niveau en réseau, cryptographie, développement sécurisé ou architecture système.

Mais cette image est réductrice. Elle occulte un élément essentiel : la cybersécurité n'est pas qu'un défi technologique, c'est avant tout un défi organisationnel et humain. Les incidents majeurs montrent systématiquement que les failles les plus critiques ne proviennent pas uniquement de faiblesses techniques, mais de dysfonctionnements dans

la gouvernance, l'anticipation, la coordination, la prise de décision, la formation des employés et la gestion du changement.

Autrement dit : renforcer la cybersécurité d'une organisation, c'est mener une transformation managériale à part entière.

Les entreprises et institutions qui parviennent à bâtir une cybersécurité robuste partagent une caractéristique commune : elles ont su mobiliser un arsenal de compétences transverses en complément de l'expertise technique. Ces compétences sont souvent sous-estimées mais décisives :

- management stratégique : définition d'une vision, articulation entre les enjeux *business* et les priorités sécurité, allocation des ressources, pilotage par les risques ;
- conduite du changement : planification et accompagnement des évolutions organisationnelles nécessaires (nouvelles procédures, nouvelles équipes, nouveaux outils), formation continue, communication interne ;
- ressources humaines et GPEC : anticipation des besoins en compétences, cartographie des savoir-faire existants, construction de parcours professionnels en cyber, fidélisation des talents rares ;
- éthique et responsabilité sociétale : prise en compte des impacts sur la vie privée, les libertés individuelles, la confiance numérique et la réputation de l'entreprise.

Ces dimensions relèvent directement du management de haut niveau, et non du seul champ de l'ingénierie. Elles conditionnent pourtant l'efficacité et la pérennité des investissements techniques.

Les dirigeants d'entreprise, les décideurs publics ou les responsables de grandes organisations ont une expérience précieuse : ils ont souvent eu à mener de profondes transformations industrielles, technologiques et humaines (transition numérique, automatisation, réorganisations, fusions, etc.).

Ces expériences leur ont appris une réalité fondamentale : aucune transformation durable ne réussit sans placer l'humain au cœur.

La cybersécurité n'échappe pas à cette règle. La mise en place d'une politique cyber efficace implique :

- d'obtenir l'adhésion des équipes ;
- de faire évoluer les pratiques et les comportements ;
- de créer un climat de confiance autour des enjeux de sécurité ;
- et de construire un écosystème de compétences collaboratif, où experts techniques, responsables métiers et instances dirigeantes coopèrent étroitement.

Lutter contre les cybermenaces suppose donc de passer d'une logique de conformité technique à une logique de culture organisationnelle.

Cela implique :

- d'aligner la cybersécurité sur la stratégie globale de l'entreprise ;
- d'intégrer les considérations de sécurité dans toutes les décisions managériales (achats, RH, innovation, relations clients) ;
- et de responsabiliser l'ensemble des parties prenantes, y compris les comités de direction et les conseils d'administration.

C'est à ce niveau que se joue aujourd'hui la différence entre les organisations vulnérables et les organisations résilientes : celles qui réussissent à faire de la cybersécurité un levier

de performance et non une contrainte, et qui transforment leurs collaborateurs en acteurs conscients, compétents et engagés de la sécurité numérique.

Aux fins de relever ces défis humains et organisationnels, les écoles d'ingénieurs ont depuis longtemps des programmes de formation qui intègrent ces dimensions dans l'acquisition de compétences. Les étudiants et futurs jeunes diplômés manqueront certes d'expérience dans ces champs de compétence mais auront *a minima* les premiers réflexes qui ne les cantonneront pas à l'exercice de leur savoir-faire technique. Les programmes de formation continue ne sont plus seulement destinés à des collaborateurs, cadres et managers des fonctions techniques mais également à toutes les forces vives des organisations.

Acquérir des compétences ou former ses équipes ? Un choix souvent présenté… mais artificiel

Face à l'ampleur des cybermenaces et à la pénurie de talents disponibles, les dirigeants se trouvent souvent face à un dilemme apparent : recruter des experts déjà opérationnels ou former leurs équipes existantes pour les faire monter en compétences.

En réalité, cette opposition est trompeuse. L'un ne peut plus se concevoir sans l'autre :

- les profils « prêts à l'emploi » sont rares et chers ;
- et les formations longues prennent du temps à produire leurs effets.

La seule stratégie soutenable consiste à articuler acquisition et développement des compétences dans une logique d'écosystème. Autrement dit, intégrer en continu de nouveaux talents tout en faisant évoluer en parallèle les collaborateurs en poste, pour créer une dynamique d'apprentissage permanent.

Or, cet objectif suppose que les formations elles-mêmes soient extrêmement réactives et étroitement connectées aux besoins du terrain.

La cybersécurité est un domaine qui évolue à une vitesse inédite : nouvelles attaques, nouvelles réglementations, nouvelles technologies (IA générative, *cloud* souverain, quantique, etc.).

Les cursus doivent donc s'actualiser en permanence, anticiper les compétences émergentes et proposer des formats flexibles, adaptés aussi bien aux jeunes en formation initiale qu'aux professionnels en reconversion ou en formation continue. Cela exige un modèle pédagogique qui dépasse les silos traditionnels et qui associe étroitement tous les acteurs de la filière.

Les écoles d'ingénieurs et de spécialité occupent une position singulière et stratégique dans cet écosystème. Elles se trouvent au croisement de tous les flux de savoirs et de besoins. Elles captent les signaux faibles de l'innovation scientifique et technologique grâce à la recherche. Elles traduisent les besoins opérationnels et les contraintes réglementaires en compétences grâce à leurs liens étroits avec les entreprises et institutions. Elles s'alignent sur les priorités de souveraineté, de résilience et de sécurité économique en réponse aux recommandations des gouvernements et agences nationales. Elles préparent les futurs experts et cadres dirigeants en formation initiale. Elles assurent la montée en compétences et la réorientation des professionnels déjà en activité vers les métiers en tension.

Ce positionnement en fait de véritables « maillons d'adaptation », capables d'agréger les tendances, d'orienter les contenus et de déployer rapidement les formations adéquates. Ce sont, en somme, des capteurs et des catalyseurs : elles perçoivent les besoins émergents, mobilisent leurs réseaux académiques et industriels, et transforment ces signaux en offres de formation concrètes et opérationnelles.

Dans un domaine où les menaces se réinventent chaque semaine, cette capacité à aller plus vite est déterminante. Elle seule permet de réduire le temps de latence entre l'apparition d'une nouvelle menace et la disponibilité de compétences adaptées, de renforcer la souveraineté numérique et de garantir la résilience des organisations. C'est cette agilité systémique, à la fois académique, scientifique et industrielle, qui doit guider l'action publique et les choix d'investissement en matière de formation cyber.

Aller à la rencontre les uns des autres : une dynamique collective et sociétale

Renforcer la filière cyber ne peut pas reposer sur un modèle linéaire et cloisonné de formation puis d'embauche. Il faut dépasser la relation « école → stage → emploi » pour bâtir de véritables partenariats continus et intégrés entre les écoles et les entreprises.

Concrètement, cela suppose que les entreprises :

- interviennent tout au long du parcours des étudiants, dès les premières années (conférences, projets tutorés, situations d'apprentissage et d'évaluation (SAE), mentorat, participation aux jurys) ;
- ouvrent leurs environnements techniques à travers des challenges, des immersions, des visites ;
- et co-développent des contenus pédagogiques avec les équipes enseignantes.

Dans ce modèle, les étudiants ne sont plus seulement formés pour rejoindre le marché, ils sont acteurs du marché dès leur formation : ils participent à des *hackathons* ou des CTF (Capture The Flag, les *hackathons* de la cyber), des compétitions techniques et des projets concrets, en collaboration directe avec les entreprises, les institutions et les chercheurs.

C'est cette approche immersive et partenariale qui permet d'accélérer leur professionnalisation tout en nourrissant l'innovation pédagogique.

Encore faut-il que les jeunes générations aient envie d'investir ce champ exigeant.

Les signaux sont encourageants : dans l'enquête de rentrée menée par l'EPITA auprès de ses nouveaux entrants, 65 % d'entre eux considèrent que la cybersécurité est le domaine qui les attirent le plus.

Plusieurs leviers peuvent expliquer selon nous cet attrait croissant :

- la forte présence de la cyber dans les séries et les films, qui en donnent une représentation positive et valorisante ;
- l'engagement citoyen et de défense, qui motive de nombreux jeunes à contribuer à la protection des institutions et des infrastructures ;
- et une sensibilité accrue à l'importance des données personnelles et aux considérations éthiques, très marquée dans cette génération.

Cet intérêt spontané est un atout majeur, mais il doit être entretenu et canalisé par une pédagogie qui met en valeur le sens et l'impact sociétal des métiers du numérique sécurisé.

Former des experts cyber ne suffit pas : encore faut-il que leurs compétences diffusent et irriguent l'ensemble du tissu économique et institutionnel. C'est ici que le rôle sociétal des écoles et des grandes institutions prend tout son sens.

À travers leurs réseaux et leurs dispositifs, elles doivent contribuer à : essaimer les compétences dans les territoires, accompagner les PME, les collectivités, les hôpitaux,

les administrations qui sont souvent les plus vulnérables aux cyberattaques, mettre à disposition leurs ressources pédagogiques et leurs expertises, et soutenir les initiatives de montée en compétences collectives portées par les pouvoirs publics.

Un programme comme CYBIAH piloté par le Campus Cyber, lieu totem de la cybersécurité qui rassemble les principaux acteurs nationaux et internationaux du domaine, accompagne gratuitement les TPE, PME, structures de l'économie sociale et solidaire et collectivités franciliennes dans leur montée en maturité cyber, en proposant un parcours complet allant de la sensibilisation à la mise en œuvre de solutions personnalisées, illustre cette logique de mobilisation nationale coordonnée, où chaque acteur, écoles, entreprises, institutions, État, contribue à la protection de l'écosystème numérique français.

Conclusion

Former à la cybersécurité devient alors un acte citoyen, qui vise à protéger non seulement les grandes entreprises stratégiques, mais aussi les services hospitaliers, les infrastructures territoriales et l'ensemble des usagers du numérique.

Témoignage d'un recruteur de profils cyber sur l'évolution des besoins

Par Odile DUTHIL
Directrice cybersécurité du groupe Caisse des Dépôts (CDC)

La cybersécurité est devenue un enjeu majeur pour les entreprises et les institutions publiques. Avec l'augmentation exponentielle des cyberattaques et l'émergence de nouvelles menaces, notamment liées à l'intelligence artificielle (IA), les besoins en experts en cybersécurité n'ont jamais été aussi élevés.

Pourtant, le secteur fait face à une pénurie chronique de talents, exacerbée par une offre de formation insuffisante et un manque d'attractivité auprès des jeunes diplômés. La cybersécurité est donc depuis plusieurs années un secteur en tension, confronté à une pénurie structurelle de talents.

Dans ce secteur en tension, la Caisse des Dépôts s'appuie à la fois sur une ouverture des postes à l'externe, mais privilégie également la mobilité professionnelle en interne du groupe CDC. La force d'une équipe repose sur sa diversité et sur la complémentarité de ses profils, qu'il est indispensable de former régulièrement et à qui il faut proposer de s'épanouir professionnellement.

Contexte de la menace : une cybercriminalité en expansion

Les cyberattaques se multiplient et se sophistiquent. Selon le rapport sur la cybermenace de 2023 de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), le nombre d'attaques recensées en France a augmenté de 37 % entre 2022 et 2023.

Les *ransomwares*, les attaques par *phishing* et les intrusions ciblées représentent les principales menaces. Selon le baromètre du CESIN (Club des experts de la sécurité informatique et numérique), une entreprise sur deux est touchée par les cybermenaces en France. Le coût des cyberattaques est également élevé, puisque le coût moyen d'une violation de données s'élève à 4,45 millions de dollars (source : IBM Security).

Dans ce contexte de menace très élevée, la transformation numérique a évidemment aussi un impact. La généralisation du télétravail, l'adoption massive du *cloud* et les ruptures technologiques ont élargi la surface d'attaque des organisations. Selon Gartner (Tendances en cybersécurité 2024), 60 % des entreprises ont accru leurs dépenses en cybersécurité en 2024, mais peinent à trouver les compétences nécessaires pour sécuriser leurs infrastructures.

L'évolution des besoins en personnels : une demande en forte croissance

Cependant, cette course technologique exige des experts capables de maîtriser ces outils, ce qui accentue la demande en compétences spécialisées. Selon l'ISC2[1], dans son étude sur la pénurie de talents en cybersécurité, le déficit mondial en professionnels de la cybersécurité atteint 3,4 millions de postes non pourvus en 2024. En France, plus de 15 000 emplois restent vacants (source : Syntec Numérique - Baromètre des emplois en cybersécurité).

Cette pénurie de ressources s'explique d'une part par une offre de formation insuffisante malgré la multiplication des formations en cybersécurité. Ainsi, en France, seulement 2 500 étudiants sortent chaque année avec un diplôme en cybersécurité (source : ANSSI).

Les écoles peinent à attirer des étudiants car beaucoup se tournent vers des filières plus généralistes comme l'informatique ou le management. D'autre part, le secteur souffre d'un manque d'attractivité, et les métiers restent méconnus voire mal perçus et assimilés à des métiers très techniques et austères. Ce qui explique d'ailleurs le manque de diversité, seulement 20 % des professionnels sont des femmes (source : Clusif).

Enfin, l'offre de compétences nationales ou européennes en cybersécurité rentre en concurrence avec celles des GAFAM.

Stratégies de formation : comment combler le déficit ?

Pour inverser la tendance, plusieurs leviers doivent être actionnés. Cela passe par le développement de formations adaptées (certifications, partenariats écoles-entreprises) qui sont indispensables, mais également par l'investissement dans la reconversion professionnelle pour élargir le vivier de talents. Les certifications (CISSP, ISO 27001 Lead Implementor ou Auditor, ISO 27005) permettent une montée en compétences rapide. Des plateformes spécialisées proposent des parcours adaptés aux besoins des entreprises.

Le Clusif (Club de la Sécurité de l'Information Français) a publié en 2024 un livrable intitulé « Inclusion et Diversité dans la Cybersécurité »[2], qui propose une grille détaillée des métiers et des compétences nécessaires pour renforcer l'attractivité du secteur. Ce document établit une cartographie des métiers et des compétences et identifie 12 familles de métiers en cybersécurité, ainsi que les parcours de formation recommandés (diplômes, certifications, expériences professionnelles). Ce livrable est conçu pour être un outil pour les recruteurs et les formateurs.

Le CESIN propose de participer à des universités d'été et au congrès annuel où ses membres, les RSSI (Responsables de la Sécurité des Systèmes d'Information), peuvent échanger sur les sujets d'actualité et les meilleures pratiques, sans tabou.

La reconversion professionnelle est ainsi un levier clé pour élargir le vivier de talents, en cassant les stéréotypes et en valorisant des profils variés. Des reconversions depuis d'autres domaines (réseaux, développement, audit) peuvent aider à combler le déficit.

---

[1] L'ISC2, pour *International Information System Security Certification Consortium*, est une organisation internationale à but non lucratif, fondée en 1989, qui se consacre à la formation et à la certification des professionnels de la cybersécurité dans le monde entier.

[2] https://clusif.fr/wp-content/uploads/2023/12/20231208-Inclusion-et-diversite-dans-la-cybersecurite.pdf

Notre stratégie à la Caisse des Dépôts

La Caisse des Dépôts (CDC) et sa filiale CDC Informatique jouent un rôle clé dans la sécurisation des infrastructures critiques et des données sensibles. Face à l'augmentation des cybermenaces et à la pénurie de talents évoquées plus haut, le groupe a mis en place une stratégie de recrutement ambitieuse, combinant diversité des profils, valorisation des *soft skills*, formations certifiantes et parcours professionnels attractifs. Notre stratégie à la Caisse des Dépôts, à la direction des risques du groupe, s'appuie donc à la fois sur une ouverture des postes à l'externe, tout en privilégiant la mobilité professionnelle en interne du groupe CDC.

En effet, comme dans toute entreprise, la cybersécurité à la CDC ne se limite pas aux experts techniques.

Selon une étude d'ISC2 de (2024), 60 % des postes en cybersécurité nécessitent des compétences hybrides, qui combinent des compétences techniques, managériales et juridiques. En effet, les RSSI (Responsables de la Sécurité des Systèmes d'Information) travaillent en étroite collaboration avec les équipes de la DPO (Data Privacy Officer), dans le cadre de la protection des données à caractère personnel. Le groupe est également soumis à de nombreuses réglementations, parmi lesquelles les directives DORA et NIS2 sont les plus récentes.

Dans ce contexte, la tentation est naturellement grande de vouloir recruter ce qu'on appelle trivialement un « mouton à cinq pattes ». C'est toutefois la filière de la cybersécurité de la Caisse des Dépôts qui regroupe l'ensemble des compétences requises, sur lesquelles chaque collaborateur peut s'appuyer individuellement. Il est donc absolument crucial de diversifier les profils et donc les compétences pour constituer ce « mouton à cinq pattes », qui est en fait l'équipe elle-même ! Dans ma direction, j'ai trois équipes : une équipe de RSSI, une équipe d'experts techniques en cybersécurité et une équipe regroupant des experts en gestion des risques et des contrôleurs permanents.

Dans tous les domaines de compétences, la Caisse des Dépôts s'engage à diversifier ses équipes, et cette politique s'applique bien évidemment à la cybersécurité. Nous avons certes besoin d'ingénieurs mais pas seulement !

Nous privilégions la mobilité interne et, donc, nous passons par une phase de reconversion professionnelle, avec l'intégration de profils issus de la direction juridique, de la maîtrise d'œuvre/ouvrage informatique, de l'audit, du contrôle permanent ou des réseaux. La formation joue ainsi un rôle crucial dans notre politique de recrutement, tout comme l'interaction entre collègues, qui est une source de richesse inépuisable. Autre résultat, nous n'avons pas particulièrement cherché à recruter plus de femmes et pourtant, aujourd'hui, la direction de la cybersécurité comprend un tiers de femmes.

De l'importance des *soft skills*

De manière plus globale, ce qu'on appelle généralement les *soft skills* sont cruciales pour les métiers de la cybersécurité au sein de la Caisse des Dépôts, comme c'est le cas dans toute entreprise ou institution publique. Il est aujourd'hui nécessaire pour un collaborateur d'avoir des compétences dans les domaines suivants :

- La communication : expliquer des risques complexes à des non-experts et vulgariser les impacts sur le domaine métier concerné.
- La collaboration : travailler avec les équipes IT, juridiques et métiers. C'est également ce qui est promu dans la réglementation DORA, où il est question de résilience opérationnelle et non plus de cyber résilience. Savoir embarquer les métiers est maintenant une compétence clé !

- La résilience : savoir gérer des crises (*ransomware*, fuites de données). Cela passe évidemment par une phase d'apprentissage, mais surtout par des mises en situation. Les équipes cybersécurité de la Caisse des Dépôts participent aux exercices de crise menés par le Groupe de Place Robustesse de la Banque de France, mais aussi aux exercices Rempar de l'ANSSI. Nous menons notre propre exercice de crise cyber annuel, afin d'entraîner non seulement notre management et nos collaborateurs, mais aussi nos métiers, notre service RH, nos services de communication et notre direction juridique à la gestion de crise.

Une étude de Gartner de 2023 montre que 75 % des échecs en cybersécurité sont liés à des lacunes en *soft skills* (mauvaise communication, manque de *leadership*).

Par exemple, les RSSI viennent de 2 horizons, soit des professionnels en cybersécurité qui ont été recrutés à l'externe, soit des profils internes mais qui ont démontré une véritable appétence pour la cybersécurité et qui ont souhaité évoluer dans le domaine. Deux tiers de l'équipe proviennent d'une mobilité interne et un tiers seulement de l'externe ou d'une filiale. Nous avons donc formé nos collaborateurs, dont la cybersécurité n'était pas le cœur de métier au départ et ce qui peut sembler un obstacle au départ est en fait une vraie richesse ! Les RSSI ont pour mission principale l'accompagnement des métiers de la Caisse des Dépôts et trois activités principales qui sont :

- l'élaboration des analyses de risques pour le développement des projets applicatifs ;
- la sensibilisation des collaborateurs ;
- les contrôles de second niveau.

Pour remplir leurs missions, ils s'appuient sur une équipe d'experts en cybersécurité pour enrichir leurs compétences techniques et sur leur connaissance très fine des métiers qu'ils accompagnent au quotidien.

Les certifications sont souvent un prérequis pour de nombreux postes, et selon Cybersecurity Ventures (2024), 80 % des recruteurs privilégient les candidats certifiés. Toutefois, les collaborateurs peuvent également tout à fait suivre ces formations certifiantes dans le cadre de leur parcours professionnel. Après quelques mois passés dans la direction cybersécurité du groupe, chaque collaborateur peut suivre une formation certifiante et aujourd'hui, 87 % des collaborateurs ont au moins une certification en cybersécurité.

Un écosystème sur lequel s'appuyer

La cybersécurité fait partie des fonctions support de nombreuses entreprises et institutions publiques et c'est le cas à la Caisse des Dépôts. De ce fait, un écosystème s'est constitué notamment au travers d'associations professionnelles telles que le CESIN ou le Clusif. Comme les professionnels de la cybersécurité ne sont pas en concurrence entre eux, même lorsqu'ils travaillent pour des sociétés concurrentes, des programmes de mentorat se sont développés pour permettre à de jeunes RSSI, par exemple, de bénéficier de l'expérience professionnelle de profils plus expérimentés. Les plus expérimentés tirent également avantage d'un regard neuf sur leurs activités ! Ces associations professionnelles sont extrêmement riches et précieuses.

À la Caisse des Dépôts, nous sommes plusieurs membres, dont certains siègent au conseil d'administration, du CESIN et la Caisse des Dépôts est au conseil d'administration du Clusif. Cela permet d'échanger sur les bonnes pratiques mais aussi de repérer les talents, évidemment. D'ailleurs, nous animons l'espace *offsec* (sécurité offensive) du Clusif afin d'échanger sur les meilleures pratiques et les faire connaître également.

Enfin, on ne peut pas parler de recrutement sans évoquer la politique salariale, ni les perspectives d'évolution professionnelle.

La Caisse des Dépôts est assez bien positionnée en matière de rémunération, alignée sur les standards du marché, supérieure à certains secteurs, mais inférieure à celle du secteur bancaire.

Un environnement de travail épanouissant

Néanmoins, la rémunération n'est qu'une facette de la reconnaissance. Celle-ci passe également par des formations régulières et par la valorisation des collaborateurs au sein de leur écosystème. Les participations aux grands salons professionnels comme les Assises de la cybersécurité à Monaco, le Forum in Cyber, etc., ou la contribution à des tables rondes dans les grands événements sont autant de leviers de reconnaissance. Dans la direction de la cybersécurité, nous répartissons les participations aux conférences selon les *desiderata* de chacun en début d'année.

Les valeurs qui sont également véhiculées par la Caisse des Dépôts représentent enfin un levier important pour attirer des talents de l'extérieur. En effet, la contribution de la CDC à la vie économique française, le sens de l'intérêt général, l'apport aux grands enjeux de notre société sont autant d'arguments qui donnent du sens à l'engagement des talents dans notre institution.

En effet, la souveraineté numérique fait partie des axes stratégiques de la CDC et se traduit par le financement de solutions souveraines au travers de filiales, de participation à la croissance de *startups* cyber par le biais de fonds du groupe CDC, l'utilisation de solutions souveraines et une participation active à l'Indice de Résilience Numérique. Autant d'éléments que je mets en avant lors des entretiens de recrutement !

Enfin, il est possible d'évoluer dans le groupe grâce à une filière resserrée, permettant de connaître précisément les besoins d'évolution dans chaque entité.

Comment NIS 2 impacte un territoire : le cas de la Bretagne

Par Yann DIEULANGARD
Chargé d'études et responsable de l'Observatoire du numérique au sein de l'agence Bretagne Next

Et Tiphaine LEDUC
Coordinatrice générale de Bretagne Cyber Alliance

La directive NIS 2 est une opportunité majeure pour des milliers d'entités de mieux se protéger des risques cyber. Avant même sa transposition, la Bretagne a décidé de mettre en place un observatoire NIS 2 permettant d'identifier les établissements concernés sur le territoire régional, de leur proposer un accompagnement et de réaliser un suivi avec l'évaluation de leur maturité cyber. Plus de 2 000 établissements sont concernés par la directive en Bretagne, répartis sur 6 secteurs, dont l'industrie agroalimentaire, la chaîne de fabrication industrielle, le transport et la logistique, et les infrastructures et services numériques.

L'article détaille le travail mis en œuvre pour l'identification et la cartographie des établissements. La méthodologie proposée corrige des biais de définition afin que les particularités régionales soient intégrées, augmentant par là même l'impact de l'application de cette directive. L'observatoire NIS 2 contribue à l'élaboration d'une stratégie régionale de cyber résilience.

La cybersécurité : une filière de pointe au service des filières stratégiques

Avec 180 entreprises, plus de 8 000 emplois et des milliers d'étudiants, la Bretagne est une terre cyber, s'appuyant sur deux piliers, civil et militaire. Conscients des nouveaux enjeux régionaux, nationaux et européens, la Région Bretagne et les collectivités ont structuré la filière cybersécurité avec un campus cyber territorial.

Le campus cyber breton, Bretagne Cyber Alliance est né de cette volonté collective de la Région et de 5 territoires bretons (Brest Métropole, Golfe du Morbihan-Vannes Agglomération, Lannion-Trégor Communauté, Lorient Agglomération et Rennes Métropole) d'agir pour le développement d'une filière régionale majeure et contribuer à la protection des filières économiques et du territoire dans sa globalité.

Ce campus vise à animer et dynamiser la communauté cyber, à favoriser les interactions entre les différents acteurs de la filière et à faire rayonner l'écosystème cyber breton comme une référence en France et en Europe pour un monde numérique plus sûr. Bretagne Cyber Alliance structure son action autour de 4 missions : accompagner la croissance des acteurs économiques de la cybersécurité, conforter la performance de la

recherche et de l'innovation, diffuser la culture de la cybersécurité dans toute la société et répondre aux besoins en compétences.

La directive NIS 2 (Network and Information Security) représente une opportunité majeure pour des milliers d'entités de mieux se protéger des risques cyber. Dans le cadre de son campus territorial, la Bretagne a décidé de mettre en place un observatoire NIS 2, permettant ainsi d'engager des actions pour les filières concernées avant même la transposition. Il ne s'agit nullement de faire une « exception régionale » dans l'application de la directive mais d'être le plus a même de l'appliquer avec discernement et efficacité localement, ceci en coordination et complémentarité avec les services de l'Etat en région

L'observatoire permet de structurer le déploiement de NIS 2 sur le territoire régional en se fondant sur un cycle en 4 phases : connaître, accompagner, mesurer, suivre.

Cet article détaille la méthodologie mise en œuvre pour la première étape : identifier les structures et établissements concernés, prérequis d'une démarche d'accompagnement efficiente.

NIS 2 : L'IDENTIFICATION DES ACTEURS CONCERNÉS

Les critères d'éligibilité d'une entité soumise à NIS 2 (Commission européenne, 2022) se fondent sur 2 éléments :

- l'appartenance à certains secteurs d'activités, 18 au total, qui sont classés en 2 catégories : « Hautement critiques » et « Autres secteurs critiques » ;
- les caractéristiques socio-économiques de l'entité : effectifs, chiffre d'affaires et bilan permettant d'en affiner la classification : « Essentielle » ou « Importante ».

Notion d'entité

NIS 2 s'applique à des « entités » publiques ou privées constituant des entreprises dites moyennes au sens de l'article 2 de l'annexe de la recommandation 2003/361/CE (EU-32003H0361, 2003). L'entité se rapporte au propriétaire de la personnalité morale. Dans une optique de mesure d'impact effective sur un territoire et d'efficience de l'accompagnement au plus près des acteurs, nous verrons comment cette définition peut biaiser la cartographie d'un territoire lorsqu'il y existe une disparité d'activités entre le siège et ses établissements secondaires.

Critères sectoriels

18 secteurs d'activités sont couverts par NIS 2 :

- hautement critiques : administrations publiques, énergie, transport, secteur bancaire, infrastructure de marchés financiers, santé, eaux potables, eaux usées, infrastructure numérique, gestion des services TIC (interentreprises), espace ;
- autres secteurs critiques : services postaux et d'expédition, gestion des déchets, production et distribution de produits chimiques, agroalimentaire, industrie manufacturière, fournisseurs numériques, recherche.

Afin d'identifier au mieux les acteurs concernés par la directive, chaque secteur est scindé en sous-secteurs avec une description des activités s'y référant. Si cela n'aboutit pas directement à une liste de codes d'activités NAF/NACE normalisés au niveau européen (Eurostat, 2008) et attribué à chaque établissement enregistré en France, elle les sous-tend le plus souvent. Il est ainsi assez aisé d'identifier *via* le code d'activité d'une entité si celle-ci peut être concernée par la directive.

ANNEXE I

SECTEURS HAUTEMENT CRITIQUES

Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	— Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil (1), qui remplissent la fonction de «fourniture» au sens de l'article 2, point 12), de ladite directive
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944
		— Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944
		— Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944
		— Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil (2) — Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943 fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944 — Exploitants d'un point de recharge qui sont responsables de la gestion et de l'exploitation d'un point de recharge, lequel fournit un service de recharge aux utilisateurs finals, y compris au nom et pour le compte d'un prestataire de services de mobilité
	b) Réseaux de chaleur et de froid	— Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement européen et du Conseil (3)
	c) Pétrole	— Exploitants d'oléoducs
		— Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		— Entités centrales de stockage au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil (4)
	d) Gaz	— Entreprises de fourniture au sens de l'article 2, point 8, de la directive 2009/73/CE du Parlement européen et du Conseil (5)
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 6, de la directive 2009/73/CE
		— Gestionnaires de réseau de transport au sens de l'article 2, point 4, de la directive 2009/73/CE
		— Gestionnaires d'installation de stockage au sens de l'article 2, point 10, de la directive 2009/73/CE
Secteur	Sous-secteur	Type d'entité
		— Gestionnaires d'installation de GNL au sens de l'article 2, point 12, de la directive 2009/73/CE
		— Entreprises de gaz naturel au sens de l'article 2, point 1, de la directive 2009/73/CE
		— Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	— Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	— Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) n° 300/2008 utilisés à des fins commerciales
		— Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du Conseil (6), aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil (7), et entités exploitant les installations annexes se trouvant dans les aéroports
		— Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) n° 549/2004 du Parlement européen et du Conseil (8)
	b) Transports ferroviaires	— Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil (9)
		— Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, y compris les exploitants d'installation de service au sens de l'article 3, point 12), de ladite directive
	c) Transports par eau	— Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret, telles qu'elles sont définies pour le domaine du transport maritime à l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil (10), à l'exclusion des navires exploités à titre individuel par ces sociétés

Figure 1 : Extrait de la directive NIS 2 - Annexe 1 - Tableau précisant le périmètre de chaque secteur (Source : Commission européenne - Octobre 2025 - https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:02022L2555-20221227&qid=1759415832848).

Toutefois, il existe des descriptions sectorielles pour lesquelles la correspondance avec des codes d'activités NAF/NACE sont inexistantes (exemple : secteur de l'énergie, sous-secteur de l'hydrogène) ou laisse une grande marge de manœuvre d'interprétation du périmètre de compétences à considérer. C'est le cas des fournisseurs de services de sécurité gérés ou

MSSP, pour lesquels les certifications produits ou services – bien qu'utiles – ne sauraient constituer les critères ultimes permettant d'établir l'éligibilité. En Bretagne par exemple, nous disposons de plus de 112 acteurs déclarant assurer des services MSSP, dont plus de 14 sont des entités importantes mais où seules 9 possèdent des certifications de management ou des qualifications de services.

Dans de tels cas, les acteurs régionaux sont amenés à interpréter « localement » les périmètres qui peuvent demeurer flous. Lorsque certains secteurs font ou ont fait l'objet de dynamiques de structuration et de collaboration interrégionale ou européenne, il est toutefois possible de converger avec des partenaires vers une définition commune du périmètre.

Critères socio-économiques

Les entités essentielles ou importantes sont définies selon le degré de criticité du secteur (voir « Critères sectoriels » ci-dessus) et selon la valeur de trois variables socio-économiques que sont la taille de leurs effectifs, leur chiffre d'affaires et leur bilan.

En l'état[1], les entités qui appartiennent à l'un des secteurs d'activité couverts par la directive sont soit des :

- entités essentielles si elles emploient au moins 250 personnes ou ont un chiffre d'affaires annuel supérieur à 50 millions d'euros et un bilan annuel supérieur à 43 millions d'euros ;
- entités importantes si elles ne sont pas des entités essentielles et emploient au moins 50 personnes ou ont un chiffre d'affaires et un bilan annuel supérieur à 10 millions d'euros.

La directive précise par ailleurs que ces critères de seuils doivent être calculés sur l'ensemble des activités – établissements secondaires compris – exercées par l'entité, et non uniquement sur les activités relevant des 18 secteurs d'activités susmentionnés.

Déclinaison en Bretagne

Généralités et spécificités

La Bretagne compte 749 707 établissements actifs au 1er septembre 2025.

Sans tenir compte des critères socio-économiques, 10 % de ces établissements, soit 75 000 œuvrent dans l'un des 18 secteurs couverts par NIS 2, dont 89 % sont des sièges. Une première comparaison avec la situation nationale permet d'établir deux constats :

- il n'y a globalement pas de prévalence régionale concernant le poids[2] des secteurs NIS 2 dans l'économie régionale par rapport à la situation nationale ;
- il existe deux secteurs impactant l'économie régionale qui ne sont pas concernés par NIS 2 : le tourisme et l'agriculture/pêche.

Si nous nous focalisons sur les établissements de plus de 50 salariés – première variable socio-économique servant de critère d'éligibilité et aisément accessible – le périmètre se restreint :

- il en existe 3 950 en Bretagne dont environ 2 000 œuvrent dans un des secteurs NIS 2 ;

[1] Et avant d'être précisées par décret.

[2] En termes de volumétrie des établissements actifs.

- 6 secteurs NIS 2 concentrent 90 % des acteurs régionaux concernés par la directive :
  - la santé,
  - l'administration,
  - l'agroalimentaire,
  - le numérique,
  - le transport,
  - la fabrication.

Des filières régionales critiques mais sous les radars NIS 2

Dans notre travail d'identification, 2 secteurs non couverts par NIS 2 sont ressortis en raison de leur poids dans l'économie régionale. Il s'agit de la pêche[3] et du tourisme[4].

Afin d'évaluer la pertinence de leur intégration dans notre périmètre de surveillance, nous avons estimé :

- l'importance du système d'information (SI) dans la filière ;
- la criticité de l'impact (PIB régional, emploi) dû à un blocage ou une destruction partielle ou totale des ressources SI des acteurs.

Le lecteur trouvera en annexe une description des chaînes de valeurs de chacune des filières et cette estimation. Il ressort de cette évaluation que :

- pour la filière pêche : 3 armements[5] conséquents disposant d'effectifs de plus de 100 salariés ainsi qu'une autorité d'accompagnement/régulation ont été retenus ;
- pour la filière touristique : 22 entités touristiques dépassant les 50 salariés ont été ajoutées au périmètre d'observation.

Méthodologie de recensement

Première approche : via *les unités légales*

Étant donné que NIS 2 considère des « entités », il est tentant dans une première approche de se focaliser sur les unités légales et sièges des établissements. Ceci permet de disposer directement des variables socio-économiques cumulées et de vérifier ainsi aisément l'un des critères d'éligibilité. Cette approche masque cependant deux difficultés majeures qui peuvent entraîner un risque important de sous-évaluation de l'impact local de NIS 2 :

- l'appréciation de l'éligibilité sectorielle ;
- la vérification du caractère « local » de l'entité éligible : est-elle située vraiment située sur mon territoire ?

[3] Première région de pêche française (source : France Agrimer, 2020) : 41,4 % de la valeur totale de la pêche française, 55,7 % du tonnage français, 94 entreprises de mareyage (CA de 667 M€), 56 entreprises de transformation (CA de 1,2 Md€).

[4] 10 % du PIB régional, 9 % des emplois, 20 millions de nuitées à fin août 2025 (source : Tourisme Bretagne).

[5] Scapêche, groupe AgroMousquetaires (Lorient, 56), Compagnie Française du Thon (Concarneau, 29), Armements Bigouden (Le Guilvinec, 29).

Ce double risque existe car si l'interrogation des bases d'unités légales[6] permet effectivement de remonter le cumul des effectifs d'une même entité morale, elle ne permet de remonter qu'une seule activité ainsi qu'une seule localisation, celle du siège. Or, cette activité peut-être en dehors du périmètre sectoriel NIS 2 et cette localisation en dehors du périmètre régional observé.

Il est en effet courant de disposer d'une unité légale classée dans la catégorie « Activités des sièges sociaux » dont le siège est basé à Paris, donc non éligible NIS 2 et hors région alors que l'ensemble de ces établissements secondaires est couvert par NIS 2 et situés en Bretagne ! Dans cette région, le domaine de l'énergie, du traitement des eaux voire de l'agroalimentaire sont concernés.

Seconde approche : via *les établissements*

Il convient donc d'abandonner la seule approche visant à extraire toutes les unités légales situées en région, œuvrant dans un secteur NIS 2 et remplissant les critères socio-économiques au profit d'une recherche d'établissements unitaires qui sont ensuite agrégés *via* leur numéro de Siren à la même entité, puis de vérifier si l'agrégat ainsi formé vérifie les conditions d'éligibilité sectorielle et socio-économiques, en sommant les variables socio-économiques, et en agrégeant les activités dans lesquels œuvrent ces établissements.

Ainsi exposée la démarche apparaît beaucoup plus lourde et complexe. Elle semble toutefois plus pertinente pour éviter une sous-estimation de l'impact de NIS 2.

Qualification de l'éligibilité

Si la vérification de l'éligibilité d'un acteur est importante, la qualification de celle-ci l'est tout autant pour évaluer les criticités d'impact sur un territoire et prioriser des actions d'accompagnement.

La déclinaison opérationnelle de la démarche proposée nous conduit ainsi à exploiter 7 variables sectorielles et socio-économiques, atomiques ou consolidées pour mesurer et qualifier l'éligibilité :

- le secteur d'activité de l'établissement ;
- le caractère d'établissement principal d'un établissement ;
- la localisation géographique de l'établissement ;
- la présence d'établissements secondaires ;
- les effectifs, CA et bilan unitaires des établissements ;
- le cumul de ces variables socio-économiques ;
- l'agrégat des secteurs d'activités des établissements secondaires affecté au niveau du siège afin de mesure la « criticité » sectorielle globale de l'entité.

Ceci nous permet pour chaque acteur de savoir, par exemple, si son éligibilité est :

- Directe : l'entité est constituée d'un établissement situé en région, répondant directement aux critères sectoriels et socio-économiques de NIS 2. Cela concerne 92 % des entités recensées.

[6] Base Sirene de l'Insee par exemple.

- Acquise par agrégat : le cumul des établissements principaux et secondaires d'une même unité légale permet de vérifier les seuils d'éligibilité de NIS 2. Le siège, en ou hors région, hérite de l'agrégat des activités NIS 2 de ses établissements secondaires. La diversité de cet agrégat donne une mesure de la criticité et du niveau d'attention qu'il convient de lui apporter.
- Acquise car faisant partie d'un secteur jugé critique régionalement (*cf.* « Des filières régionales critiques mais sous les radars NIS 2 » ci-dessus).

Résultats : Cartographie et Tableau de bord

Avec le mode opératoire d'identification par établissement proposé et en considérant les 7 variables, le travail de recensement permet de dresser une cartographie de 2 048 acteurs concernés par NIS 2 en Bretagne :

- 1 894 établissements sont directement éligibles à l'application de la directive :
  - 275 entités essentielles et 1 628 entités importantes,
  - 1 444 en secteurs hautement critiques, 450 en « autres secteurs critiques ».
- 122 établissements sont éligibles en tant que participant à un agrégat ;
- 26 établissements de plus de 50 salariés présents dans les secteurs spécifiquement bretons (tourisme, pêche/agriculture) sont traités en tant que « cas spécifiques » dont 3 entités considérées comme importantes de par leur effectif de 250 salariés ;
- 6 établissements extra-régionaux (remplissant ou non les conditions sectorielles de NIS 2) sont éligibles car sièges d'un agrégat d'établissements secondaires situés en Bretagne remplissant les conditions sectorielles et socio-économiques.

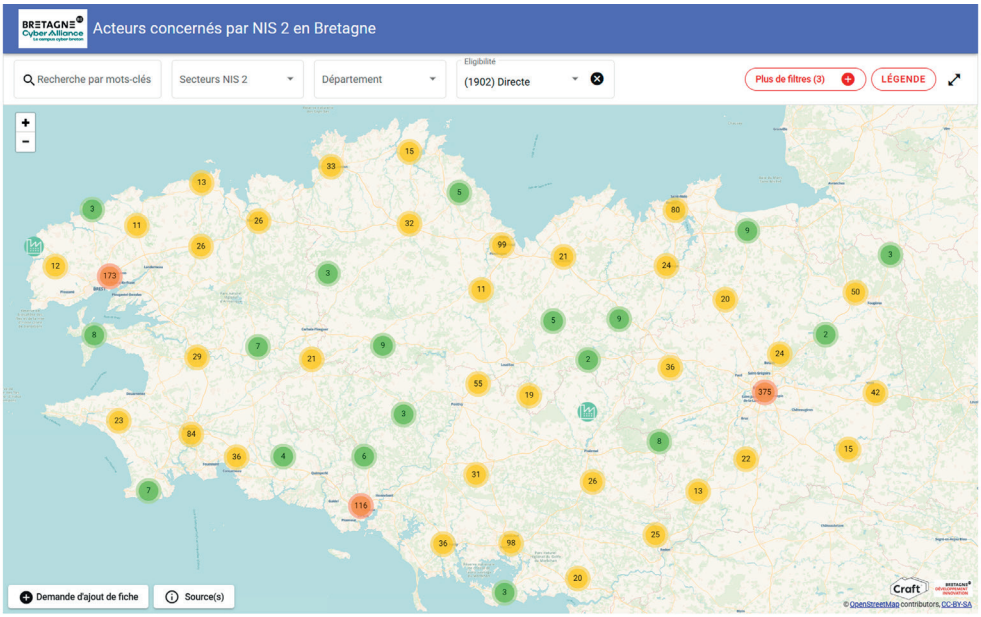

Figure 2 : Cartographie des 1 894 acteurs concernés par NIS 2 *via* l'éligibilité directe (Source : Agence Bretagne Next (ex-BDI), octobre 2025).

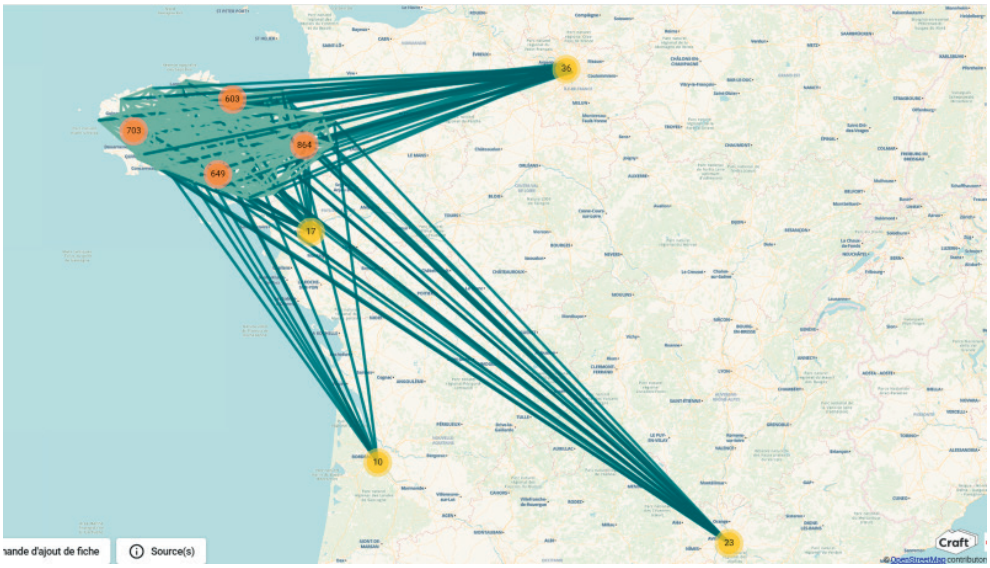

Figure 3 : Cartographie des 2 048 acteurs concernés par NIS 2 en Bretagne, agrégats et secteurs spécifiques compris, avec leur dépendance aux sièges extrarégionaux (Source : Agence Bretagne Next (ex-BDI), octobre 2025).

Figure 4 : Extrait du tableau de bord de suivi de l'impact de NIS 2 en Bretagne (Source : Agence Bretagne Next (ex-BDI), octobre 2025).

Conclusion et perspectives

Le travail présenté dans cet article vise à dénombrer, qualifier et visualiser l'impact de la directive NIS 2 sur un territoire régional. Les acteurs à accompagner sont identifiés par une approche hybride : descendante, par l'application de la directive sur le territoire, et remontante, par une connaissance fine du territoire permettant d'intégrer de

façon *ad hoc* certaines entités. Par la mise en place d'un observatoire NIS 2, la Bretagne favorise l'appropriation de ces informations par toutes les parties prenantes – acteurs économiques, associatifs, institutionnels et de gouvernance – contribuant ainsi à l'élaboration d'une stratégie régionale de résilience cyber sur un périmètre étendu à des filières locales critiques.

Une nécessaire coordination

Ce travail de cartographie illustre également qu'il ne peut y avoir de stratégie de résilience autonome. Les acteurs économiques et institutionnels sont géographiquement éclatés et interdépendants. La fragilité du SI d'un siège social dans le sud de la France peut impacter l'ensemble de ses chaînes de production situées en Bretagne et mettre à mal tout un pan de l'économie de cette dernière. La coopération interrégionale apparaît donc nécessaire.

Il apparaît par ailleurs tout aussi pertinent d'assurer une cohérence et une coordination de l'ensemble de ces stratégies au niveau national. À ce titre, l'ANSSI se révèle comme acteur référent garantissant l'atteinte de ces objectifs. La démarche présentée dans cet article a fait l'objet d'une présentation détaillée à l'Agence nationale, avec la proposition de mettre à disposition la méthodologie au service d'autres régions.

Perspectives

Ce travail de cartographie permet de dresser un état des lieux à un temps T. Il constitue la première brique d'un observatoire visant à mesurer la maturité cyber du territoire et à orienter les choix et priorités d'actions pour le rendre résilient dans la durée.

Annexes

Des améliorations possibles

Ce travail de cartographie pourrait gagner en précision *via* l'accès à des données plus fraiches et exhaustives. Il conviendrait également de préciser certains périmètres sectoriels de NIS 2 afin d'inclure ou non des acteurs dans la cartographie.

Précisions méthodologiques

Qualité des données sources : les effectifs

Plus de 2 000 entités sont concernées par NIS 2 en Bretagne. Pour effectuer cette évaluation, nous nous sommes fondés sur les données d'effectifs issues de la base Craft[7] ainsi que sur le répertoire Sirene®, répertoire des unités légales et des établissements maintenus à jour par l'Insee. Si nous disposions, pour plus de 50 % des acteurs, de données d'effectifs postérieures à 2023, il a fallu s'appuyer, pour l'autre part, sur les chiffres d'effectifs de 2022 présents dans Sirene afin d'évaluer les critères d'éligibilité.

Critères socio-économiques : bilan, CA et effectifs

La détermination des catégories importantes ou essentielles repose en partie sur l'évaluation de seuils sur trois données socio-économiques de l'entité : chiffre d'affaires, bilan et effectifs.

[7] Plateforme logicielle SAAS collaborative d'hébergement et de valorisation de données sectorielles. Opérée par Bretagne Next, également maître d'ouvrage de l'outil, elle permet de structurer et suivre les filières stratégiques en région : https://www.platform-craft.eu/

Si une collecte quasi exhaustive des tranches d'effectifs qui n'est pas nécessairement celles des *équivalents temps plein (ETP)* requis plus précisément par la directive peut être effectuée, celle des bilans et des chiffres d'affaires apparaît beaucoup plus délicate et aléatoire. Par ailleurs, les estimations de ces valeurs, lorsqu'elles sont mises à disposition, sont souvent trop approximatives pour s'y référer avec confiance et opérer un traitement égalitaire pour l'ensemble des entités. Aussi, avons-nous décidé de restreindre les critères socio-économiques aux seules données d'effectifs.

Étant donné que, pour un secteur NIS 2 connu, le seuil sur la variable effectif suffit à établir l'appartenance d'une entité à la catégorie essentielle ou importante indépendamment de celle du bilan ou du chiffre d'affaires, nous avons assumé le fait que l'absence de ces deux informations engendrait potentiellement un biais de sous-évaluation restreint sur l'ensemble du parc concerné et pouvant être corrigé à l'avenir.

Détails des critères sectoriels

La détermination de l'activité d'une entité, donc de son éligibilité première, sur la seule base du code d'activité NAF/NACE associé au Siret n'est pas toujours fiable. Code unique pour un établissement en France, variant rarement au cours de la vie, il traduit souvent mal l'évolution des compétences ou des activités de ce dernier. Aussi, pour près de 40 % de ceux-ci, nous sommes nous fondés sur la qualification sectorielle « Craft », opéré par des partenaires économiques de terrain afin d'accéder à la réalité de l'activité de l'acteur et statuer sur son éligibilité sectorielle.

Le cas de la filière pêche

La filière pêche tout comme la filière tourisme, n'est pas monolithique. Elle est constituée de plusieurs maillons reflétant plusieurs activités. Dans le cas de la pêche par exemple, il faut différencier les activités de cueillette en mer de celles de mareyage, de transport, de préparation/transformation du produit avant sa vente et sa consommation. De façon favorable, plusieurs de ces activités sont couvertes par les secteurs NIS 2 (transport, première transformation qui correspondent souvent au mareyage). Ce n'est pas le cas pour les activités du secteur primaire (la pêche en soi). Toutefois, si l'importance des SI dans les activités de pêche maritime n'est plus à démontrer (pilotage du navire, sécurité à bord, contrôle/commande du matériel de cueillette, communication au sol, traçabilité de la cargaison, tous régis par des SI variablement interopérables) (Boutet, Chauvin, Morel & Tirilly, 2006) et que tous les armements sont équipés d'au moins 3 systèmes numériques de localisation/traçabilité (GPS, AIS[8], VMS[9]), ce sont les fournisseurs numériques – couverts par NIS 2 – qui dispensent ces services qui sont à surveiller en amont. En parallèle des armements, il ne faut pas négliger l'impact que pourrait avoir une attaque sur les autorités délivrant les autorisations de pêche. Certaines ont un statut d'administration et sont donc potentiellement couverts par NIS 2, mais d'autres non. Le Comité régional des pêches maritimes et des élevages marins, structure privée régie par le code rural, en constitue un exemple, car c'est lui qui délivre les autorisations de pêche hors quotas européens aux armements régionaux. Aussi, après analyse et discussion avec les parties prenantes du secteur, hormis quelques acteurs spécifiques inclus de façon *ad hoc*

[8] Automatic Identification System.

[9] Vessel Monitoring System pour transmettre automatiquement des données de position géographique, d'identification du navire, ainsi que la date, l'heure, la vitesse et la route du navire à un centre de surveillance des pêches (CSP).

(3 armements[10] de plus de 100 salariés et une autorité de régulation) nous décidons de ne pas intégrer ce secteur de manière générique dans notre périmètre de surveillance.

Le cas de la filière tourisme

Le cas de ce secteur[11] est différent. Fortement associée à la dimension de « services », la présence et l'importance du SI dans tous ses maillons est avérée. Toutefois, 97 % de ces 9 000 acteurs ont moins de 10 salariés et travaillent avec des SI très faiblement interconnectés. Les logiciels de réservation/comptabilité sont majoritairement dans le *cloud* et ce sont les fournisseurs de services numériques, couverts par NIS 2, qui sont soumis aux obligations de conformité associées. Si nous nous attachons toutefois à considérer les infrastructures privées d'accueil de plus grande taille, deux activités se distinguent :

- L'hébergement/restauration : on entendra ici l'hôtellerie pure (indépendante, franchisée ou faisant partie d'établissements secondaires de grandes chaînes internationales). Rappelons que ce secteur n'est pas couvert par NIS 2. Dans le cas régional, il est souvent augmenté par l'activité complémentaire de thalassothérapie marine qui fait évoluer le plus souvent le code d'activité vers le « bien-être » (sans toutefois tomber dans le champ de la santé, qui est couverte par NIS 2) et nécessite d'élargir le champ d'observation et de recensement.
- Les excursions et les croisières maritimes côtières : couvertes par NIS 2 *via* le secteur des transports mais peu critiques en termes de SI.

À ces acteurs privés, il conviendrait d'ajouter des structures publiques de renseignement et d'informations touristiques au nombre de 70 offices et 200 bureaux en Bretagne. Elles constituent autant de points d'entrée sensibles pour des attaques pouvant fragiliser l'économie touristique régionale. Toutefois, interconnectées entre elles et aux SI d'EPCI voire régional dans le cadre d'une politique d'attractivité globalisée[12] et étant le plus souvent des antennes de structures administratives déjà couvertes par NIS 2, nous ne les intégrons pas dans notre périmètre de surveillance.

Au total, et par le biais d'une approche *ad hoc* ce sont donc uniquement 22 entités touristiques dépassant les 50 salariés que nous choisissons d'inclure dans le périmètre d'observation.

Bibliographie

BOUTET A., CHAUVIN C., MOREL G. & TIRILLY G. (2006), « L'usage des Technologies de l'Information et de la communication dans le secteur de la pêche maritime », Récupéré sur https://www.marsouin.org/IMG/pdf/Rapport_final___Peche_et_TIC.pdf

BREDA T., ASKENAZY P., MOREAU F. & PECHEU V. (2022), « Les entreprises sous-déclarent-elles leur effectif à 49 salariés pour contourner la loi ? », mars 2022, Note de l'Institut des Politiques Publiques, n°82, 8 pages, Récupéré sur https://www.ipp.eu/wp-content/uploads/2022/03/note_seuils_sociaux_admin.pdf

COMMISION EUROPÉENNE (2022), « Directive SRI 2 : la sécurisation des réseaux et des systèmes d'information », décembre 2022, Récupéré sur Commission européenne : https://digital-strategy.ec.europa.eu/fr/policies/nis2-directive

[10] Scapêche, groupe AgroMousquetaires (Lorient, 56), Compagnie Française du Thon (Concarneau, 29), Armements Bigouden (Le Guilvinec, 29).

[11] 10 % du PIB régional, 9 % des emplois, 20 millions de nuitées à fin août 2025.

[12] *Via* le Comité Régional du Tourisme : Organisme fédérateur des acteurs du tourisme en région Bretagne, co-gérant de la marque de territoire marque Bretagne.

EU-32003H0361 (2003), « Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises », (Texte présentant de l'intérêt pour l'EEE) [notifiée sous le numéro C(2003) 1422], Récupéré sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32003H0361

EUROSTAT (2008), « NACE Rév. 2 - Nomenclature statistique des activités économiques dans la Communauté européenne », Récupéré sur eurostat : https://ec.europa.eu/eurostat/fr/web/products-manuals-and-guidelines/-/ks-ra-07-015

ViePublique.fr/295752 (2025), « Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité », 13 mars 2025, Récupéré sur Vie publique : https://www.vie-publique.fr/loi/295752-projet-de-loi-resilience-infrastructures-critiques-cybersecurite#:~:text=Cybers%C3%A9curit%C3%A9-,Le%20projet%20de%20loiProjet%20de%20texte%20l%C3%A9gislatif%20d%C3%A9pos%C3%A9%20au,'ensemble%20de%20l'Union

Adaptation de l'offre aux enjeux de la réglementation européenne

Par Benjamin MORIN et Florent KIRCHNER
Secrétariat général pour l'Investissement (SGPI)

La stratégie nationale pour la cybersécurité du plan France 2030 concourt à l'émergence de champions français de la cybersécurité, tant pour accompagner le développement d'une filière au fort potentiel économique que pour garantir à notre pays la maîtrise des technologies essentielles à son autonomie et à sa résilience. De l'émergence des *start-ups* à la consolidation de l'écosystème, en passant par les défis de la maturation et du passage à l'échelle, cet article revient sur les mesures entreprises par l'État, dans le cadre de France 2030, en vue d'adapter l'offre cyber nationale aux enjeux de la réglementation européenne et aux impacts de la géopolitique mondiale.

Introduction

Dans un contexte marqué par une dépendance croissante des sociétés aux services numériques, par de multiples conflits militaires où l'arme cyber fait partie intégrante des arsenaux des belligérants, et par la remise en cause d'équilibres géopolitiques que l'on pensait acquis, la cybersécurité est plus que jamais un enjeu de résilience pour la Nation.

Face à ce constat, la directive NIS2 et le Cyber Resilience Act (CRA) participent du nécessaire rehaussement du niveau de sécurité des organisations, en obligeant ces dernières à adopter des mesures de cybersécurité, et en contraignant les fabricants d'équipements comportant des éléments numériques à sécuriser les produits qu'ils vendent en Europe.

Ces réglementations ont des répercussions concrètes sur les organisations. Leur mise en œuvre à l'échelle du continent constitue un défi majeur, non seulement pour les organisations qui y sont assujetties, mais également pour constituer une offre souveraine à même de satisfaire la demande.

Cet article présente les mesures mises en place par la stratégie nationale pour la cybersécurité dans le cadre du plan France 2030 qui, collectivement, participent de l'adaptation de l'offre aux enjeux de la réglementation européenne.

France 2030 et la stratégie d'accélération cyber

Le plan France 2030 se donne pour ambition de transformer durablement des secteurs clés de l'économie française par l'innovation technologique, et de positionner la France non pas seulement en acteur, mais bien parmi les *leaders* du monde de demain.

Dans ce cadre, le Gouvernement accompagne le développement de la filière française de la cybersécurité *via* la stratégie nationale pour la cybersécurité. Cette stratégie vise à faire émerger des champions français de la cybersécurité, tant pour accompagner le

développement d'une filière au potentiel économique important que pour garantir à notre pays la maîtrise des technologies essentielles à son autonomie et à sa résilience.

Les mesures qui composent la stratégie cybersécurité du plan France 2030 se veulent à la fois ambitieuses et pragmatiques. Ambitieuses, car ces mesures visent à développer un écosystème scientifique et une offre industrielle capables de soutenir durablement l'excellence française existante. Pragmatiques, car les solutions dont elle oriente et soutient le développement ont pour objectif d'apporter des réponses concrètes aux enjeux de cybersécurité, sans attendre un renversement de l'échiquier technico-économique actuel, dominé dans le domaine du numérique par des acteurs extra-européens.

L'implémentation de cette stratégie se distingue des approches déployées dans les plans d'investissements précédents, et dans les politiques de soutien à l'innovation d'autres pays, par deux facteurs clés. D'abord, elle structure un accompagnement cohérent sur l'ensemble du cycle de l'innovation, depuis la recherche fondamentale jusqu'au déploiement expérimental, en passant par les dispositifs de soutien à la maturation, à la formation, et à la création de communs. Ensuite, elle procède d'une logique de renforcement de la filière industrielle nationale, sans laquelle il ne peut y avoir de nation forte dans le domaine cyber.

Plusieurs défis sous-tendent cette ambition : celui de l'émergence de *start-ups*, celui de la maturation d'offres adaptées aux besoins réglementaires à venir, celui du passage à l'échelle des acteurs, celui de leur expansion à l'Europe et à l'international, et celui de la consolidation.

Le défi de l'émergence de *start-ups*

L'adaptation de l'offre nationale en cybersécurité débute par l'émergence d'entrepreneuses et d'entrepreneurs capables de transformer un concept, une idée, un résultat de recherche en un produit ou un service innovant. Le Cyber Booster et le Programme de Transfert font partie des dispositifs mis en place par la stratégie cyber pour soutenir les initiatives entrepreneuriales.

La création du Cyber Booster, premier incubateur dédié à la cybersécurité, hébergé à Rennes et au Campus Cyber, a ainsi permis depuis 2022 d'épauler 43 *start-ups* dans une phase critique de leur développement. Celles-ci ont déjà levé, en agrégat, plus de 16 M€.

Le programme de transfert de technologies et de connaissances, hébergé dans les locaux du Campus Cyber à La Défense, a été lancé en 2023. Sa vocation est de rassembler acteurs de la recherche, des *start-ups*, de l'industrie et des administrations publiques dans la mise en œuvre de solutions très innovantes. Un programme d'animation scientifique et une forte interaction avec l'écosystème du Cyber Booster permettent de faire émerger une dynamique collaborative unique.

Le bilan à ce stade est encourageant. Selon l'édition 2025 du radar établi par Wavestone et Bpifrance [2], le nombre de création de *start-ups* en France progresse continuellement depuis 2022 (il atteint 180 *start-ups*, 46 *scale-ups* et une licorne mi-2025, avec un début de consolidation). Dans un contexte économique globalement morose, le montant moyen des levées de fonds continue aussi de progresser, la France passant en tête des nations européennes les plus dynamiques dans le domaine de la cybersécurité.

Le défi de la maturation d'offres adaptées aux besoins réglementaires

Partant du constat que l'offre française en cybersécurité comportait des lacunes en ce qui concerne la maîtrise de certaines technologies clés, la stratégie nationale a mis en œuvre

un éventail de dispositifs pour soutenir des projets de recherche et développement portant sur des briques technologiques innovantes et critiques en cybersécurité.

Les technologies identifiées sont critiques du fait de leur sensibilité en termes de sécurité, et appellent autant que possible des solutions maîtrisées, dans une démarche d'autonomie numérique. En outre, elles représentent un marché potentiel de taille pour les acteurs français.

L'évaluation de sécurité et la protection des données font notamment partie des technologies critiques que la stratégie d'accélération cybersécurité a accompagné *via* deux dispositifs successifs, avec pour objectif commun d'anticiper la demande générée par l'entrée en vigueur de la directive NIS2 et des réglementations DORA et CRA.

Le premier dispositif a ainsi cherché à mobiliser l'écosystème français sur la maturation de méthodes et d'outils innovants permettant d'accroître l'efficacité et la compétitivité des évaluations de cybersécurité. Son objectif est de permettre aux démarches de certification de traiter des questions d'automatisation, de résilience, de comparabilité, tout en continuant d'augmenter les niveaux de confiance obtenus, avec pour ambition de placer la France et l'Union européenne parmi les *leaders* mondiaux dans le domaine de l'évaluation de systèmes numériques.

Le second dispositif de maturation a porté sur l'une des clés contribuant à l'autonomie numérique : la protection des données stockées, transmises, ou calculées, selon une acception délibérément large. Étaient ainsi concernées des solutions innovantes permettant de sécuriser des contenus en s'affranchissant de leur contenant (en utilisant par exemple des primitives de cryptographie avancée), de sécuriser les données manipulées par des systèmes d'IA tout au long de leur cycle de vie, de contrôler les accès selon des approches centrées sur les données, ou encore de préparer la migration post-quantique. Au regard de l'importance que revêt la protection des données dans l'évolution des réglementations européennes, disposer d'acteurs très innovants dans ce domaine est un enjeu majeur, tous domaines confondus (centre de traitement de données, systèmes embarqués, installations industrielles).

Le défi du passage à l'échelle

Les évolutions réglementaires européennes s'accompagnent d'une augmentation sans précédent des besoins en cybersécurité émanant de structures très variées. La préparation de la filière cybersécurité nationale à ce changement d'échelle constitue donc un défi majeur. Pour contribuer à le relever, la stratégie nationale a notamment mis l'accent sur deux leviers : la formation et l'automatisation.

Formation de spécialistes

Le domaine de la cybersécurité connaît depuis plusieurs années une pénurie de compétences. Cette carence menace le calendrier de mise en conformité des organisations avec la directive NIS2, ces dernières ne trouvant pas les femmes et les hommes dont elles ont besoin pour évaluer leur maturité cyber, mettre en œuvre les mesures de protection et de gestion d'incidents, ou encore sensibiliser leurs collaborateurs.

L'appel à manifestation d'intérêt « Compétences et Métiers d'Avenir » du plan France 2030 vise à accélérer la formation aux métiers d'avenir et à répondre aux besoins des entreprises et des institutions publiques en matière de formation. Dans ce cadre, les projets soutenus par la stratégie cybersécurité ambitionnent de former 80 000 professionnels de la cybersécurité à horizon 2030 dans les domaines techniques établis de la cybersécurité (évaluateurs ou concepteurs de systèmes, analystes, chercheurs, etc.) et dans des domaines en structuration, non techniques (commerciaux, RH, droit, etc.). Cet effort

inédit de formation de spécialistes cyber s'accompagne d'une attention particulière portée sur la diversité des talents formés et sur l'accessibilité des formations sur l'ensemble du territoire national – métropole et Outre-mer.

Automatisation

L'automatisation est un levier majeur dans le passage à l'échelle des mesures de sécurisation, et un enjeu omniprésent dans les dispositifs d'accompagnement de la stratégie cyber.

Le grand défi « Automatisation de la cybersécurité » lancé en 2021 était en particulier centré sur ce sujet. Les projets soutenus par ce dispositif ont permis de traiter des problèmes de protection de petites structures telles que les PME et de certaines collectivités. Centres hospitaliers et collectivités ont par exemple bénéficié du blocage précoce d'attaques les ayant ciblés, grâce aux solutions soutenues dans le cadre du grand défi. Au-delà des résultats obtenus en matière d'automatisation, les retombées de cet instrument de pilotage de l'innovation unique en son genre ont été positives à plusieurs égards. Le dispositif a ainsi contribué à la création de synergies entre acteurs nationaux de la cyberdéfense et au rayonnement de l'écosystème français sur la scène internationale. Par ailleurs, plusieurs entreprises lauréates ont collectivement donné lieu à d'importantes levées de fonds, témoignant de la valorisation de la prise de risque technologique par l'écosystème privé.

Le défi de la confrontation au réel

La plupart des instruments de la stratégie nationale d'accélération cyber visent à relever le défi des évolutions réglementaires européennes de façon indirecte, en soutenant l'essor d'une offre cyber adaptée aux besoins des organisations. Le programme « Cyber PME » et les parcours de cybersécurité du plan France Relance font figure d'exception, en ce qu'ils consistent à accompagner directement les organisations dans le rehaussement de leur niveau de protection. Ce faisant, ces dispositifs permettent d'éprouver l'offre en la confrontant à la réalité des besoins.

Pilotés par l'Agence nationale de Sécurité des systèmes d'information, les « parcours de cybersécurité » ont pour leur part consacré 100 millions d'euros du plan France Relance à la sécurisation de 945 structures, composées de collectivités territoriales et d'établissements publics, dont 133 établissements de santé. Le bilan tiré de ce programme [1], clôturé budgétairement en 2024, est positif. Pour ses bénéficiaires, il a d'abord permis de constituer des bases solides pour anticiper les évolutions réglementaires européennes, grâce au rehaussement significatif de leur sécurité. Il a également permis de renforcer l'offre de prestations locales et de produits nationaux ou européens, ces derniers ayant bénéficié de près de 75 % des investissements. Le programme a aussi permis de mesurer les progrès à entreprendre pour augmenter la part occupée par les éditeurs hexagonaux dans les acquisitions de produits (environ le tiers des montants investis).

Plus récemment, le programme Cyber PME s'adresse prioritairement à des PME ou des ETI des filières de l'aéronautique civile et de l'énergie. Il comporte deux phases. La première consiste en une évaluation du niveau de sécurité des entreprises lauréates et aboutit à un plan d'action. La seconde porte sur la mise en œuvre des recommandations du plan d'action, et inclut le co-financement de produits ou de services de cybersécurité. Le niveau de promotion des offres nationales par les prestataires retenus par les bénéficiaires du dispositif fera partie des indicateurs de succès de ce programme, dont le bilan est attendu en 2026.

Le défi de l'internationalisation

Le développement de l'offre française en cyber passe par la conquête de marchés extranationaux par les acteurs industriels de la filière.

Cette logique est omniprésente dans les instruments qui composent la stratégie nationale pour la cybersécurité. En commençant par sensibiliser au plus tôt et en aguerrissant les entrepreneurs aux enjeux de l'internationalisation, notamment dans le cadre du programme d'incubation du Cyber Booster. Ensuite dans la conception des programmes de maturation de technologies pour permettre un positionnement compétitif des offres nationales dès l'entrée en vigueur des réglementations européennes, et leur mise en œuvre dans un processus de solidarité internationale. Enfin, en conjuguant la dynamique d'investissement française à celle qui prend place au niveau européen (notamment *via* les programmes Horizon Europe, Digital Europe et le prochain European Competitiveness Fund), et en exploitant l'articulation naturelle du passage de solutions « incubées nationalement » à l'échelle du continent.

Le défi de la consolidation de l'offre

Le tissu français de la cybersécurité concentre des expertises clés sur de nombreux domaines tels que la détection de menaces, l'analyse de code, la cryptologie, ou l'évaluation de sécurité. Il reste néanmoins peu structuré. Il en résulte que la filière française peine à s'imposer face à la concurrence internationale, y compris en France où des solutions étrangères plus intégrées entre elles parviennent à s'imposer. Ce morcellement a également pour effet d'exposer nos pépites à des acquisitions étrangères, potentielles entraves à notre autonomie numérique.

Le Campus Cyber est né de la volonté de développer les collaborations entre de grands groupes, des petites entreprises et des *start-ups* en les faisant cohabiter au sein d'un « lieu totem », pour contribuer à la structuration de l'écosystème. Le Campus Cyber a montré sa capacité à créer des synergies au sein de la communauté cyber nationale et à la faire rayonner à l'international, condition nécessaire à une consolidation de l'offre.

La consolidation de l'offre passe aussi par la constitution de fonds européens spécialisés en cybersécurité, capables de financer des *scale-ups* avec des tickets supérieurs à 50 M€. Ce levier, clairement identifié par la stratégie nationale de cybersécurité, ne s'est pas encore concrétisé. Il demeure un objectif des années à venir.

Conclusion

À travers le plan France 2030, le Gouvernement a mis en place plusieurs dispositifs de de soutien de l'offre en cybersécurité, en misant sur l'innovation pour faire émerger des réponses maîtrisées aux défis soulevés par les évolutions réglementaires européennes, et offrir une alternative crédible aux solutions américaines qui dominent le marché.

L'impact réel de ces mesures sur notre préparation ne sera mesurable qu'à l'issue de ces dispositifs, dont la plupart sont en cours d'exécution. On peut néanmoins prédire qu'en plus d'un soutien incessant à l'émergence d'offres au meilleur niveau mondial, remporter le match de la souveraineté demandera aussi une adaptation conjointe de la demande ; la pérennité des solutions soutenues dépendra aussi de leurs carnets de commandes. Elle suppose des stratégies d'acquisition volontaristes, tenant compte de la valeur de l'autonomie. Le poids de cette autonomie doit, le cas échéant, pouvoir l'emporter sur d'autres critères tels que l'omnipotence ou la puissance prétendues ou avérées de solutions concurrentes. C'est un passage obligé pour qu'à terme nos solutions puissent les supplanter.

Il s'agit là d'une responsabilité collective. Les États européens se doivent d'être exemplaires dans cette démarche, tout comme les grands donneurs d'ordre privés. La défense de nos savoir-faire dépend en partie de notre volonté de les exploiter. Il en va de notre indépendance, et à certains égards de la subsistance de nos modèles de sociétés et de nos valeurs.

Bibliographie

[1] ANSSI (2024), « Les parcours de cybersécurité : rapport d'activité 2024 – Volet cybersécurité de France Relance », Rapport d'activité de France Relance, https://cyber.gouv.fr/publications/rapport-dactivite-france-relance-2024

[2] WAVESTONE (2025), "French cybersecurity startup radar", https://www.wavestone.com/wp-content/uploads/2025/06/wavestone-radar-cyber-2025-vf-2.0.pdf

Cybersecurity: Is the Union Ready?

By Luigi REBUFFI
Founder, VP and Secretary General of the Women4Cyber (W4C)

Despite an immense effort, the EU is not mature enough to face modern cybersecurity challenges. Inspired by Erasmus's Praise of Folly, the author, a veteran of the EU cyber ecosystem, comments the Union's current path.

The Laus, praises the EU's diligence in building a regulatory fortress (NIS2, DORA, CRA) and institutions (ENISA, ECCC).

However, a critique (Pars Destruens) highlights deep paradoxes. This regulatory approach mistakes procedural compliance for operational security: a static, "tick-the-box" mentality. Furthermore, EU-level bodies act merely as coordinators for fragmented national "stovepipes" rather than creating a unified defence.

The proposal (Pars Construens) calls for a paradigm shift away from static security. "Resilience by Design" is advocated as a philosophy that accepts breaches will occur and focuses on maintaining critical functions during an attack. This requires a new goal of holistic "Digital Resilience" and a private-led, public-supported industrial policy.

Introduction: The Folly of Wisdom

To ask if the Union is ready in cybersecurity is to pose a very critical question. After decades of cooperation with the European Commission and a long career dedicated to European security and in particular to cybersecurity, I might be tempted to offer a simple, reassuring answer: "Yes, things are going better".

Having spent many years within the European cybersecurity ecosystem, most recently as Secretary General of the European Cyber Security Organisation, I find myself returning to Erasmus's Praise of Folly. In that work, Erasmus demonstrated that true wisdom often appears as folly to those invested in conventional consensus. Now, free from past constraints, I can offer a less comfortable view. Compliance. The blunt truth is that after so much effort, Europe may still not be mature enough to face the challenge, particularly now, in this exacerbated geopolitical and economic context. And we may be running out of time to change course before other global powers define the landscape without us and for us.

Inspired by Erasmus, I would present my view by adopting a classical rhetorical structure: a Laus to praise the Union's real ambitions; a Pars Destruens to critique the foundations of our current approach; and a Pars Construens to propose a future, built on more solid ground.

Laus: The Praise of Wisdom and Diligence

It would be both untrue and profoundly unfair to claim the Union has been idle. On the contrary, to any observer, the European institutions in the last decade have demonstrated

a "wise" and furious diligence in confronting the digital threat. The ambition has been clear: to build a secure, competitive, and sovereign digital Europe. This has manifested in a comprehensive, multi-layered architecture of laws, agencies, and strategies.

First, the Union has wielded its primary power – law – with undeniable ambition

This regulatory fortress is vast. It began, in many ways, with the GDPR, which set a global standard for data protection, establishing the "Brussels Effect" and proving the Union's willingness to legislate extraterritorially in the digital sphere. This was followed by the NIS first and then the NIS2 Directive, which dramatically expands the scope of "essential and important" entities, creating a new, higher baseline for cybersecurity risk management and reporting across the entire Single Market. For the critical financial sector, the DORA (Digital Operational Resilience Act) creates one of the world's most stringent and specific frameworks, moving beyond security to touch on the resilience and stress tests. And, of course, there is now the Cyber Resilience Act (CRA). It represents a world-first attempt to impose "security by design" obligations on the entire lifecycle of digital products. This has been complemented by other critical files, from the AI Act to data governance, all attempting to weave a fabric of digital rules, the European Certification procedure, and more.

Second, this regulatory push has been matched by an institutional one

The Union recognized that rules are useless without bodies to implement them. The EU Agency for Cybersecurity (ENISA), once a modest agency, has seen its mandate made permanent and significantly strengthened by the Cybersecurity Act (CSA). It is now positioned as the Union's core technical expert, the manager of the CSIRTs Network, and the shepherd of a new European certification framework intended to build trust.

Furthermore, to manage the operational response during crises, the EU-CyCLONe network was established to coordinate the management of large-scale cybersecurity incidents.

And in what is arguably one of the Union's most tangible successes, the law enforcement pillar has been vigorously activated. Europol, through its European Cybercrime Centre (EC3), has become a global leader in coordinating complex international operations against cybercriminals, dismantling major botnets, dark web markets, and ransomware groups. This demonstrates a clear capacity for effective, coordinated action when the mission is well-defined.

Third, the Union has addressed the strategic, industrial, and financial dimensions

Brussels understood that this is not just a technical problem, but one of industrial capacity and strategic autonomy. Back in 2013, the Commission created a first EU Cybersecurity Strategy articulating a vision. Later, to coordinate the use of money and provide a wider structure behind it, the ECCC (European Cybersecurity Competence Centre) and its network of National Coordination Centres (NCCs) were created, designed to guide research, innovation, and industrial capacity building.

These bodies are entrusted with steering major funding from the Digital Europe Programme and Horizon Europe, channelling billions into the cyber domain. This entire structure was built upon the pioneering work of the Public-Private Partnership between the Commission and ECSO, an organisation I have founded on request of the Commission in 2016. This cPPP was, in itself, a groundbreaking recognition that this battle could not

be won by the public sector alone and required a true participation and cooperation with the industrial sector.

Finally, on the geopolitical stage, the European External Action Service (EEAS) has been empowered with its Cyber Diplomacy Toolbox, allowing the Union to respond to malicious cyber activities using the full spectrum of CSDP[1] and diplomatic measures. This is complemented by capability-driven PESCO projects[2], many of which are facilitated by the European Defence Agency (EDA).

Viewed from this perspective, the Union has done everything right. It has created a comprehensive, interlocking system of regulations, agencies, funding, and industrial strategy. The "wise" men of Brussels have been busy. The intent is laudable, the work is complex, and the effort to build a common approach is essential.

As an engineer from the Politecnico di Milano, I was taught one fundamental lesson 45 years ago: you must first define the problem correctly to have any chance of finding the right solution. In cybersecurity, we have identified some problems, but I would say now that their definition was not always (or often) correct, hence, many of these activities did not help to reach the mentioned objective to build a secure, competitive, and sovereign digital Europe. And, following Erasmus, the main folly would be not to see it and continue believing that we are on the right track!

On one hand we can say that Europe did a good job, to elevate cyber security to a higher level of awareness in decision makers and citizens. The many activities performed in the last 15 years, since Europe started calling IT security with the term of cybersecurity, have forced Union's countries to mature and start coordinating (at least in the public sector). And this must be recognized and cheered.

Yet, European countries are only slowly coming out from their cybersecurity stovepipes. Maybe it is because in the word cybersecurity there is the term "security" which means that each country is sovereign on that topic, and cooperation is more difficult than in other less sensitive areas. Maybe it is because other stakeholders, from outside the Union do not have the interest of a competitive and sovereign Europe. Maybe because our decision makers still have to go beyond wise statements, understanding the challenges linked to securing the digital transformation and operationalise effective cooperation and an industrial policy which is dramatically lacking in this domain.

Pars Destruens: The Paradoxes of a System Under Strain

Again, following Erasmus, it is time now to analyse critically the situation and prepare a solid ground to build a stronger future, posing the right basis. The "folly" of our current path is not a lack of effort, but that this massive effort is colliding with deep, structural paradoxes. We are building brilliant, complex solutions, but they are often for the wrong problem or are hampered by the very system creating them.

The Legislative Paradox: The "Brussels Machinery"

The first pillar of our "wisdom", the regulatory fortress, is itself a product of a complex machine. A Commission proposal, born from a theoretical democratic consultation, must navigate the competing interests of the Council (often defending fragmented national

[1] Common security and defence policy, https://www.eeas.europa.eu/eeas/common-security-and-defence-policy_en

[2] https://www.pesco.europa.eu/about/

positions) and a Parliament (doing its best with available expertise and under intense lobbying).

The result? Regulations are often compromises that risk mistaking procedural compliance for operational security. This is not to say these regulations are without value – they establish crucial baselines and harmonize approaches across Member States. However, structural tensions emerge:

- The Compliance Challenge (NIS2, GDPR): These frameworks excel at standardizing practices and raising minimum thresholds. Yet we must acknowledge a subtle but critical risk: that demonstrating compliance can be conflated with achieving security. This fosters a "tick-the-box" mentality focused on reporting rather than functional security. The question becomes not "Are we secure?" but "Can we demonstrate compliance?"
- The Static Trap (CRA, Certification): The CRA and certification schemes aim to solve vulnerability. But this is a static concept based on knowledge at "time T". The threat landscape evolves daily. We are designing for a snapshot in time, not a dynamic, hostile reality.
- The Semantic Trap (DORA): The DORA regulation uses the word "resilience", but it is largely interpreted as "better security + backups + stress tests". It does not yet embrace the engineering concept of maintaining critical function while under active, sustained attack. This is the Ferrari with the perfect engine and flat tires: the function – to move from A to B – is not fulfilled.

The Sovereignty Paradox: The National Remit

The second pillar, our institutional architecture, runs headlong into a core truth: cybersecurity is, and will remain, a national remit. This is not a flaw: it is a fact. But it creates a paradox for EU-level ambitions.

- The "Stovepipe" Coordinators (ENISA, CyCLONe): ENISA has been strengthened, but it is not, and cannot be, truly operational. This is not a failure of the agency; it is by design, as Member States want to keep operational control. Instead, ENISA and networks like EU-CyCLONe act as "wise" coordinators of the national stovepipes, rather than a mechanism to break them down. They institutionalize coordination among sovereign bodies, which is useful, but it is not a unified operational defence. The approach is purely public – public, when main attacks in critical infrastructure, hit the private sector.
- The Diplomatic Fragmentation (EEAS): Similarly, the EEAS's Cyber Diplomacy Toolbox is a collection of CSDP and diplomatic measures. It's a vital step, but it remains a toolset for sovereign states to agree to use, often reactively, not a unified, proactive cyber-diplomatic posture.
- The Europol/EC3 Success: The success of EC3 is not because its mission is "reactive", but because it found the solution to the sovereignty paradox: trusted cooperation. Its power comes from seconded national experts working side-by-side, building the human trust needed to share information and act decisively. They are highly proactive, often anticipating threats and dismantling infrastructures after months of patient, collaborative work.

The Industrial Paradox: Central Ambition vs. Local Reality

Finally, our strategic and industrial model is a conundrum. We cannot command sovereignty « à coups de règlements »:

- The Role of the cPPP: The "groundbreaking" cPPP with ECSO, which I know well having founded it, proved the value of a model where the private sector is a core partner. That partnership continues to grow and deliver value, demonstrating that this public-private dialogue is essential.
- The Future of the ECCC/NCCs: The new ECCC structure has had a difficult and delayed start. However, to "kill" it would be a mistake. Its potential lies in the National Coordination Centres (NCCs). We must understand that a European cybersecurity cannot be "driven from Brussels". Cybersecurity is a local, regional, and national issue. The NCCs, if empowered, can be the key tool for this, together with national cybersecurity agencies. They are the links in a chain, allowing a truly decentralized but coordinated European ecosystem to thrive, where all parties play their part.

But what does "empowerment" mean in practice? First, it means trusting the national level to develop solutions appropriate to their industrial fabric, threat landscape, and cultural context – with Brussels providing strategic coordination, not operational prescription. Second, it means recognizing that cybersecurity cannot be purely public-sector. The NCCs' true potential lies in becoming genuine public-private coordination bodies at the national level, where industry, government, and research can work in trusted partnership – much like the successful EC3 model but adapted to each nation's reality. Third, it means that the ECCC's role should evolve into becoming a real facilitator of peer-to-peer cooperation among these empowered national nodes. The current machinery, despite good intentions, risks replicating Brussels-centric models that don't reflect the distributed, private-sector nature of the assets we're trying to protect. We need a network of strong, trusted national partnerships that cooperate horizontally, not a hub-and-spoke system where all roads lead to Brussels.

Pars Construens: Building a Future on Digital Resilience

If the old foundation is flawed, what is the new one? The Pars Construens must be built not on the shifting sands of the obsolete security definition, but on the bedrock of resilience.

The New Goal: From Cyber-Resilience to Digital Resilience

The concept of resilience has been existing and discussed in Brussels for years. It appears also in the first Cybersecurity Strategy. But was it understood and interpreted as an engineer could do or as a politician? Today, even "cyber-resilience" is not enough. A system is more than its code. It is an environment that includes technology, processes, and, crucially, the human factor.

Our new objective must be "Digital Resilience". This is a holistic concept: the ability of our critical systems and, by extension, our society to continue their essential functions, even while under persistent, sophisticated attack. Implementation of this concept, which includes of course Cybersecurity and Cyber-defence, could provide the needed contribution to our digital transformation and increased sovereignty.

The New Philosophy: "Resilience by Design"

As "Security by Design" is static, we must replace it with "Resilience by Design". This philosophy accepts that breaches will happen. It designs systems not to be impregnable, but to be functional while compromised. It prioritizes continuity, graceful degradation, and rapid recovery. It asks not "Can this be breached?" but "What happens when it is breached (because it will be breached one day or the other – and this could be dramatic in critical infrastructures), and how do we ensure the mission continues?".

The New Model: A Private-Led, Public-Supported Strategy

Finally, we must adopt a European Digital Resilience industrial policy. The public sector (the Commission and Member States) should act as a strategic partner, an enabler, and a major customer, defining the high-level objectives together with industry, but the policy should be led by the private sector, which has the innovation, agility, and market knowledge, or we will fail reaching the expected results for competitiveness and sovereignty. And resilience – digital resilience – must be the fundamental, non-negotiable component of this new, shared industrial vision, within a strategic framework and for objectives set by the public authorities. If the conditions for this are not met at 27, it is probably possible to progress with projects based on reinforced cooperation between a hard core of members of the Union.

Conclusion: A Call for Wise Folly

This assessment may appear severe, particularly when we usually celebrate the Union's achievements in raising cybersecurity awareness and establishing common frameworks. These achievements are real and should not be dismissed. Yet precisely because so much has been accomplished, we must ask: is our current trajectory sufficient for what lies ahead? My answer, uncomfortable as it may be, is that we are not yet ready – not because we lack effort or ambition, but because we may still be solving yesterday's problems with yesterday's conceptual frameworks. The threat landscape is evolving faster than our regulatory and institutional responses. We are building a magnificent, rigid wall of regulations when we need a flexible, resilient ecosystem.

To say this is not an act of cynicism but one of profound, if "foolish", optimism. We have the resources, the talent, and the ambition. We now need the courage to pivot. We must shift our entire paradigm: from security to resilience, from static design to dynamic function, and from public-led regulation to private-led, public-supported industrial strategy (of course, we still need the public driver in many activities, as enforcement, education, etc).

Where usually others may emphasize progress – and there has been real progress – I would emphasize here the distance yet to travel. Both perspectives are necessary. The achievements of the past decade have created the foundation: now we must ensure we're building the right structure upon it.

This is the only way we will find the room to "move" and thrive against the other global powers that are already building for this new reality. Union will be ready, eventually.

Approche luxembourgeoise en matière de cybersécurité et PME

Par François THILL
Directeur de la cybersécurité au ministère de l'Économie au Luxembourg

Pour le Luxembourg, la cybersécurité constitue un pilier stratégique de l'attractivité et de la résilience économique. Elle doit être accessible à toutes les entreprises, en particulier les PME, qui jouent un rôle central dans les chaînes de valeur européennes.

Le Luxembourg s'engage à soutenir l'innovation en cybersécurité par les PME et pour les PME, en valorisant l'*open source*, le partage de données et l'intégration de l'intelligence artificielle. Cette stratégie vise à favoriser la diversité des solutions et à renforcer l'autonomie technologique européenne.

En agissant collectivement, dans le cadre offert par la législation européenne et en s'appuyant sur un écosystème dynamique, le Luxembourg et ses partenaires européens peuvent bâtir une cybersécurité inclusive, innovante et résiliente, véritable moteur de compétitivité et de confiance pour l'économie numérique de demain.

Cybersécurité et PME : un marché à rééquilibrer

Le nombre croissant d'incidents de cybersécurité touchant les petites et moyennes entreprises (PME) met en lumière des fragilités structurelles persistantes dans ce secteur affectant aussi les chaînes de valeur auxquelles elles contribuent. Ces entreprises, souvent peu familières avec les cadres réglementaires comme le règlement DORA ou la directive NIS2, peinent à naviguer dans un environnement technique complexe et en constante évolution.

Cette situation reflète une asymétrie d'information[1] marquée : les fournisseurs de solutions de cybersécurité détiennent une expertise difficilement accessible pour les utilisateurs finaux, notamment les PME. À cela s'ajoutent plusieurs obstacles majeurs : un manque d'incitations à investir dans la sécurité, des barrières à l'entrée élevées, une offre parfois mal calibrée pour les besoins spécifiques de certains segments, et un accès inégal aux ressources nécessaires.

Ces facteurs combinés freinent l'adoption généralisée de bonnes pratiques en cybersécurité, laissant de nombreuses entreprises vulnérables face aux menaces numériques. Ce constat appelle à une réflexion stratégique sur le rôle que peuvent jouer les politiques

[1] Défaillance de marché | Dictionnaire bilingue du Droit de la Régulation et de la Compliance mafr, https://mafr.fr/fr/article/defaillance-de-marche/

publiques et les mécanismes de coordination pour rééquilibrer le marché et favoriser une cybersécurité plus inclusive et efficace.

Des solutions accessibles aux PME

L'un des leviers prioritaires identifiés par le gouvernement luxembourgeois concerne l'accès des PME à des solutions de cybersécurité adaptées. Pour cela, il est essentiel de réduire la complexité et les coûts des produits et services cyber, afin de les rendre accessibles aux petites structures souvent dépourvues de moyens et de compétences spécialisées.

Cette nécessité est renforcée par les exigences de gestion des sous-traitants introduites par les règlements NIS2 et DORA, qui risquent d'exclure de nombreux petits acteurs européens au profit de grands groupes, parfois non européens. Une telle évolution compromettrait les efforts visant à renforcer l'autonomie stratégique de l'Europe.

La résilience de l'économie luxembourgeoise et européenne dépend donc de la disponibilité de solutions souveraines, accessibles et fiables, à même de protéger toutes les entités impliquées dans les chaînes de valeur – en particulier les PME.

Pour répondre à ce besoin, le Luxembourg prévoit la mise en place d'une « Cybersecurity Factory » au sein de la Luxembourg House of Cybersecurity (LHC)[2]. Cette initiative vise à stimuler l'innovation en cybersécurité en mettant à disposition de toute personne morale ayant un intérêt légitime : des données issues d'un espace de données cyber ouvert ; des solutions *open source* ; du savoir-faire spécialisé en intelligence sur les menaces et gestion des risques ; des modèles d'intelligence artificielle entraînés ; et un accès facile, en mode service, vers des infrastructures CPU/GPU telles que les *clouds* souverains luxembourgeois et européens, ainsi que le supercalculateur MeluXina.

Soutenir l'innovation cyber des PME : un enjeu stratégique pour l'Europe

Le ministère de l'Économie, en tant que ministère de tutelle de la LHC et dans le cadre du règlement européen sur les aides d'État[3], joue un rôle de catalyseur en proposant des cofinancements pour les projets innovants portés par des entreprises commerciales développant des solutions de cybersécurité.

Parallèlement, il soutient la demande en cybersécurité au sein des PME en imposant une analyse des écarts entre les mesures de sécurité requises et celles effectivement mises en œuvre. Cette démarche vise à faciliter leur mise en sécurité tout en stimulant le marché : en renforçant la demande, elle encourage le développement de solutions adaptées aux besoins réels des PME, à des prix qu'elles peuvent assumer durablement.

Toutefois, cette stratégie ne peut être déployée efficacement à court terme ni de manière isolée. L'Europe dispose d'un écosystème PME cyber dynamique et innovant. Il revient au Luxembourg ainsi qu'aux autres États membres d'identifier ces acteurs, de les soutenir *via* les dispositifs d'aides d'État et les budgets européens existants, et de favoriser l'adoption de leurs solutions.

[2] Luxembourg House of Cybersecurity: The gateway to cyber resilience, https://lhc.lu/

[3] General Block Exemption Regulation | EUR-Lex, https://eur-lex.europa.eu/EN/legal-content/summary/general-block-exemption-regulation.html#:~:text=Commission%20Regulation%20%28EU%29%20No%20651%2F2014%2C%20known%20as%20the,to%20request%20prior%20permission%20from%20the%20European%20Commission

La création de nouveaux oligopoles ou de monocultures technologiques irait à l'encontre de l'objectif d'autonomie stratégique européenne. Comme l'a souligné Bruce Schneier avec le concept de "class break"[4], une homogénéisation excessive accroît les vulnérabilités systémiques. Une approche fondée sur la cybersécurité par les PME, pour les PME apparaît donc plus pertinente pour renforcer la résilience de notre économie.

L'importance de l'*Open Source Software* (OSS)

Dès la création de la LHC en 2010, le Luxembourg a reconnu l'importance de la collaboration et du partage d'informations en cybersécurité et donc le rôle que l'OSS[5] joue dans la création de communautés. En rendant tous ses outils disponibles en *open source*, la LHC encourage non seulement le partage de connaissances, mais aussi l'innovation collective. Cela permet à la fois d'améliorer les outils existants et de renforcer la résilience globale de l'écosystème de la cybersécurité. Pour accélérer la création de communautés inclusives, la LHC va mettre en place un OSPO[6].

Partager les données cyber pour renforcer la souveraineté numérique européenne

Les outils de cybersécurité *open source*, bien qu'essentiels pour la protection des systèmes, ne suffisent pas à eux seuls. Ils dépendent d'un facteur clé : les données. Ces données portent sur les menaces et leur mode de fonctionnement, les vulnérabilités qu'elles exploitent et les impacts qu'elles peuvent engendrer. Elles sont cruciales pour pouvoir identifier des menaces, prioriser des mesures de sécurité et développer des outils et services de cybersécurité. En ce sens, ces données ne sont pas uniquement essentielles au bon développement de l'écosystème de la cybersécurité, mais elles forment véritablement une « économie de données », qui en constitue la pierre angulaire.

Or, ces informations sont aujourd'hui majoritairement disponibles *via* des flux propriétaires, coûteux et souvent liés à des outils complexes, développés hors d'Europe. Ces solutions peuvent être soumises à des sanctions, à des lois extraterritoriales ou à des décisions commerciales arbitraires, et leur contenu peut être biaisé, limitant leur pertinence pour les besoins européens.

C'est pour cette raison que la LHC, plus précisément le CIRCL[7], opère depuis plus de 10 ans[8] plusieurs plateformes d'échange d'information *open source* pour promouvoir la création et contextualisation d'intelligence sur les menaces. Par exemple, la plateforme Malware Information Sharing Platform (MISP) attire plus de 2 600 entités internationales qui échangent quotidiennement des informations sur les menaces, enrichissant le contexte nécessaire à leur identification et à leur traitement.

---

[4] Class Breaks - Schneier on Security, https://www.schneier.com/blog/archives/2017/01/class_breaks.html

[5] Plus de 18 projets de la LHC sont disponibles sur github : CIRCL - Computer Incident Response Center Luxembourg GitHub), https://github.com/CIRCL, NC3 - Luxembourg GitHub, https://github.com/NC3-LU, et Monarch Documentation, https://monarch-initiative.github.io/monarch-documentation/

[6] EU OSPO Network, https://static-page-bdf202.usercontent.opencode.de/

[7] CIRCL - Computer Incident Response Center Luxembourg -- CSIRT – CERT, https://circl.lu/

[8] Service MISP – Malware Information Sharing Platform - CIRCL MISP - Open Source Threat Intelligence Platform, https://circl.lu/services/misp-malware-information-sharing-platform/

Parallèlement à la mise à disposition de la plateforme MISP, le CIRCL opère aussi des outils et plateformes pour acquérir et générer des données primaires par rapport aux menaces. Un des outils les plus prometteurs est AIL[9] qui consiste en la collecte et l'analyse des données provenant du *deepnet* et du *dark net*.

La volonté du Luxembourg de faire de la cybersécurité une économie des données a déjà été décrite dans l'étude stratégique de la troisième révolution industrielle[10] en 2016 et se manifeste depuis 2019 dans sa "data driven innovation stratégy"[11] et a été réitérée dans la stratégie sur les données[12] ainsi que dans sa stratégie IA[13] publiées en 2025.

Le Luxembourg mise sur l'infrastructure *cloud-edge*

En janvier 2021, le Luxembourg a décidé de participer au Projet Important d'Intérêt Européen Commun Next Generation Cloud Infrastructure and Services[14] (IPCEI-CIS) renommé 8ra depuis 2024[15]. Coordonné par la France et l'Allemagne, et soutenu par la DG Connect de la Commission européenne, ce projet vise à créer un *cloud-edge-continuum* : une infrastructure fluide et interopérable entre le *cloud* et les nœuds de bord du réseau.

Le Luxembourg prévoit d'y développer des services de cybersécurité spécifiquement conçus pour les PME, en accord avec l'initiative européenne Digital Decade[16], qui ambitionne d'intégrer 80 % des PME au *cloud* d'ici 2030. C'est sur cette infrastructure que le pays souhaite mettre en place le premier espace de données ouvert dédié à la cybersécurité, avec un fort potentiel de coopération internationale.

La LHC, ainsi que deux autres entreprises luxembourgeoises, participent indirectement à ce projet *via* CLAUSEN, une initiative visant à créer cet espace de données et à développer des technologies pour la collecte d'indicateurs de compromission. Ce futur espace fournira aux entités publiques et privées disposant d'un intérêt légitime un accès à des informations contextualisées sur les menaces, vulnérabilités et scénarios de risques provenant de différentes sources et de différents acteurs.

[9] ail-framework/README.md at master ail-project/ail-framework GitHub, https://github.com/ail-project/ail-framework/blob/master/README.md

[10] Étude stratégique de la 3e révolution industrielle pour le Luxembourg, https://gouvernement.lu/dam-assets/documents/actualites/2021/07-juillet/30-revolution-industrielle/TIR-complet-FR-bat2.pdf

[11] The-Data-driven-Innovation-Strategy, https://gouvernement.lu/dam-assets/fr/publications/rapport-etude-analyse/minist-economie/The-Data-driven-Innovation-Strategy.pdf

[12] Stratégie luxembourgeoise en matière de données – Accélérer la souveraineté numérique à l'horizon 2030 – Digital Skills and Jobs Coalition Luxembourg, https://digitalskills.lu/fr/strategy/strategie-luxembourgeoise-en-matiere-de-donnees-accelerer-la-souverainete-numerique-a-lhorizon-2030/

[13] La stratégie du Luxembourg en matière d'intelligence artificielle - Le gouvernement luxembourgeois, https://gouvernement.lu/fr/publications/rapport-etude-analyse/minist-digitalisation/2025-luxembourg-ai-strategy-fr.html

[14] https://commission.europa.eu/projects/ipcei-next-generation-cloud-infrastructure-and-services-ipcei-cis-abb-ag-rox_en

[15] IPCEI-CIS – 8ra, https://www.8ra.com/ipcei-cis/

[16] Europe's digital decade: 2030 targets | European Commission, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

Ce dispositif constitue une pierre angulaire pour bâtir une économie ouverte des données en cybersécurité. Son objectif principal : stimuler, grâce aux régimes d'aides d'État, la création de solutions cyber par les PME et pour les PME, afin de renforcer la souveraineté et la résilience européenne face aux risques numériques.

L'AI Factory luxembourgeoise : catalyseur d'innovation en cybersécurité

En 2024, le Luxembourg a été sélectionné parmi sept sites européens pour accueillir une AI Factory, dans le cadre du programme EuroHPC. Cette initiative vise, dans le cas du Luxembourg, à développer l'intelligence artificielle dans quatre secteurs clés : cybersécurité, finance, économie verte et spatial.

Plusieurs facteurs convergent vers une utilisation ciblée de l'intelligence artificielle dans les domaines techniques et organisationnels de la cybersécurité : pénurie d'experts, manque d'outils autonomes pour les PME, nécessité de renforcer l'autonomie stratégique européenne, et impératif d'inclure les PME dans la protection des chaînes de valeur et le traitement de volumes énormes de données.

La Luxembourg House of Cybersecurity (LHC) opérera le AI Hub dédié à la cybersécurité, avec pour mission de fournir aux entités européennes des données cyber, des experts qualifiés, des outils *open source* et un accès à des infrastructures comme MeluXina-AI, le futur superordinateur luxembourgeois qui sera dédié à l'entraînement et à l'inférence de solutions d'IA. L'objectif : permettre aux PME de concevoir des solutions souveraines et innovantes.

Le ministère de l'Économie soutiendra ces projets *via* des aides d'État, y compris des financements en cascade en collaboration avec l'European Cybersecurity Comptence Centre (ECCC). Le nouveau cadre européen favorise les projets transfrontaliers, une opportunité stratégique pour encourager la collaboration européenne et renforcer l'autonomie stratégique numérique de l'Europe.

Un projet phare IA dans le domaine de la cybersécurité

C'est dans cette optique que le Luxembourg prévoit de lancer un projet d'envergure : le « Projet phare IA Cyber » (*flagship* AI Cyber), porté par la LHC. Ce projet poursuit plusieurs objectifs complémentaires :

- renforcer les capacités de la LHC à intégrer de nouvelles sources de données dans l'espace cyber et à simplifier leur exploitation par des non-experts ;
- réduire l'effort individuel nécessaire à la gestion récurrente des risques et à la mise en œuvre de mesures organisationnelles de sécurité ;
- préparer les entreprises luxembourgeoises à la transition vers la cryptographie post-quantique dès 2026, *via* des campagnes de sensibilisation et des outils dédiés ;
- développer, dans un sens large, des services liés à la sécurité des modèles et applications IA ;
- générer un effet d'entraînement ("spillover effect") en mettant à disposition des modèles IA *open source* et *open data* et/ou *open weight*, utilisables par le secteur privé pour développer des produits et services.

Pour soutenir cette dynamique, la LHC mettra en place une infrastructure IA interne capable d'entraîner de nouveaux modèles et de maintenir ceux existants *via* des processus semi-automatisés. Le *flagship* AI Cyber ne constitue donc pas une initiative ponctuelle,

mais bien une plateforme pérenne de production et de mise à jour de modèles IA, en phase avec l'évolution des données[17]. Pour les modèles complexes de type LLM, la LHC s'appuiera sur des infrastructures plus puissantes, telles que le supercalculateur MeluXina-AI ou les *clouds* souverains luxembourgeois.

Enfin, le ministère de l'Économie accompagnera la valorisation de l'effet d'entraînement généré par le *flagship* AI Cyber à travers :

- des appels à projets nationaux et transfrontaliers dans le cadre du règlement GBER[18] ;
- des financements en cascade pour le développement d'outils et services par les PME[19] ;
- et la proposition d'«actions conjointes » au niveau du European Cybersecurity Competence Centre (ECCC)[20] en collaboration étroite avec d'autres États membres.

[17] Huggingface.io : CIRCL (Computer Incident Response Center Luxembourg), https://huggingface.co/CIRCL

[18] Règlement 2023/1315 modifiant l'article 25 (6) a) et b) du règlement 651/2014 (GBER).

[19] New call for projects: Cybersecurity Innovation and Development – Luxinnovation, https://luxinnovation.lu/news/new-call-for-projects-cybersecurity-innovation-and-development

[20] Article 13 (3) f) du règlement (EU) 2021/887 (ECCC).

Conclusion

Par Anne LE HENANFF
Ministre déléguée chargée de l'Intelligence artificielle et du Numérique

Le cyberespace possède une dynamique qui lui est propre : instantanéité des échanges, diffusion en réseau, massivité des données accessibles à tous, effacement des frontières. L'actualité démontre chaque jour la réalité de la menace cyber et l'impérieuse nécessité de s'en prémunir. À l'heure où nos vies se tissent à travers les réseaux sociaux et les algorithmes, où la frontière entre la souveraineté et la dépendance peut se jouer à une ligne de code, où les cyberattaques sont toujours plus sophistiquées, la cybersécurité constitue un impératif vital. Aux affrontements dans le monde physique, s'ajoutent les affrontements dans l'espace numérique, dont ils sont d'ailleurs, souvent, le prolongement. Cet espace est désormais le théâtre de la rivalité des puissances, où s'intriquent les intérêts et les idéologies, et où se déroulent, souvent à bas bruit, des batailles décisives.

Disons-le donc sans ambages : la cybersécurité est devenue une condition *sine qua non* de notre liberté et de notre souveraineté. Pourtant, ce domaine est encore trop perçu comme un domaine exclusivement technique, complexe, réservé aux experts et apolitique. Le niveau d'insouciance, voire d'ignorance, quant au risque cyber reste malheureusement encore trop élevé dans notre société ; si bien qu'il constitue rarement une priorité.

Face à ce constat, la France ne saurait rester spectatrice. Elle s'est d'ailleurs pleinement investie depuis 2008 pour renforcer sa cybersécurité, avec la publication du *Livre blanc sur la défense et la sécurité nationale*, puis en 2018 avec l'adoption de la *Revue stratégique de cyberdéfense*, et cette année enfin avec la *Revue nationale stratégique*, qui érige, à raison, la cyber-résilience de la Nation au rang d'objectif stratégique. Ces stratégies ont été déclinées par la prise de mesures opérationnelles concrètes qui ont permis à la France de rehausser significativement son niveau de cybersécurité. La prochaine étape sera celle de l'entrée en vigueur de la loi relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité, qui transpose les directives européennes REC, NIS2 et DORA. Cette loi, dont la mise en œuvre nécessitera un accompagnement spécifique, décliné dans chaque territoire, renforcera significativement le niveau de cybersécurité de la Nation.

Ces défis, nous ne les relèverons pas seuls. Chaque service de l'État, chaque entreprise, chaque collectivité territoriale et, *in fine*, chaque citoyen devra prendre sa part. Ce combat, c'est celui de la Nation tout entière, dont seule l'unité permettra de faire face efficacement aux menaces cyber. Cela implique de développer dès le plus jeune âge une culture de la cybersécurité, inclusive et ouverte. Outre sa technicité supposée, la cybersécurité pâtit encore de préjugés tenaces, contre lesquels nous devrons résolument lutter : un domaine masculin, solitaire, technique et réservé à une élite.

C'est aussi le combat de l'Europe, qui impliquera de mettre en place des coopérations accrues avec nos partenaires européens, une mutualisation des savoir-faire et un agenda industriel ambitieux pour que nous construisions ensemble un cyberespace sûr, ouvert et démocratique. Cela impliquera de promouvoir un cadre et une gouvernance garantissant la sécurité et la stabilité du cyberespace et d'agir en allié et partenaire fiable au sein d'une communauté d'intérêt cyber internationale.

Mais nous devons également dès à présent anticiper les futures menaces pour gagner les combats de demain. À ce titre, nous devons nous préparer à la révolution que constitue l'émergence de l'intelligence artificielle (IA). En plus des vulnérabilités de cybersécurité usuelles, les systèmes d'IA sont exposés à des vulnérabilités spécifiques liées aux modèles

d'IA. L'impact de ces vulnérabilités et les moyens d'y remédier doivent être considérés non seulement à l'échelle des composants individuels, mais également du point de vue de l'architecture du système d'IA et de son intégration au sein d'un système d'information. Nous devons impérativement accompagner le développement indispensable de l'IA par l'élaboration d'un cadre permettant d'évaluer la cybersécurité des systèmes d'IA. À cet égard, la création de l'Institut national pour l'évaluation et la sécurité de l'IA (INESIA), qui a fait suite à la Déclaration de Séoul pour une IA sûre, novatrice et inclusive de mai 2024, matérialise l'engagement de la France en faveur d'un développement maîtrisé de l'IA dans un cadre de confiance et de sécurité. C'est aussi un enjeu majeur de souveraineté nationale : l'IA générative apporte des capacités décuplées aux cyberattaquants en mettant à leur disposition des outils plus rapides et plus sophistiqués qui leur permettent d'automatiser et de massifier les cyberattaques, y compris dans le champ informationnel.

À un horizon plus prospectif, nous devrons relever le défi de l'émergence des technologies quantiques. La France dispose d'atouts formidables. Elle fait partie des États les plus en pointe dans la compétition mondiale que se livrent à bas bruit les États pour la maîtrise de cette technologie qui promet de révolutionner de très nombreux domaines tels que la défense, la santé ou encore la finance. Dans le domaine de la cybersécurité, le défi majeur sera celui de l'émergence de la cryptographie post-quantique. La France est engagée depuis plusieurs années dans les travaux internationaux du National Institute of Standards and Technology (NIST) pour développer de nouveaux algorithmes de cryptographie post-quantiques résistants aux capacités de calcul de l'ordinateur quantique. En parallèle, les services de l'État développent leurs propres travaux d'élaboration d'algorithmes de cryptographie post-quantiques dans les domaines les plus sensibles pour la souveraineté nationale. Surtout, la France est pleinement engagée dans le programme PROQCIMA, qui soutient la montée en maturité du volet matériel de l'ordinateur quantique dans le cadre de France 2030 et de la Stratégie nationale quantique.

Enfin, plus encore que la cybersécurité, c'est notre cyber-résilience que nous devons collectivement renforcer. Déjouer une cyberattaque, s'en prémunir, est évidemment essentiel. Mais lorsque celle-ci nous frappe, nous devons être en mesure de résister et de réagir. Cela impliquera de rehausser le niveau de conscience de la menace cyber dans la population et de préparer efficacement la Nation aux crises systémiques qui pourraient résulter d'une cyberattaque.

Tous ces défis, la France et l'Europe, qui ont fait face à d'innombrables défis dans leur histoire, sauront, à n'en point douter, les relever avec brio. Nous avons tous les atouts nécessaires pour y parvenir. Allons-y !

Cybersecurity: Are we ready?

bilities and rapid adoption in non-critical applications, integrating AI into high-risk systems remains problematic because it raises new challenges related to trust, particularly cybersecurity. The specific life cycle of machine learning-based applications and the intrinsic vulnerabilities associated with them require a rethinking of traditional approaches to risk analysis. Among the most significant threats are attacks aimed at altering the functioning of the model. Added to this is the issue of securing AI learning, trained on sensitive data, against information leaks and protecting copyright in a complex context. Pending regulations, professionals are seeking countermeasures that would combine protection with performance.

31 Threats related to software dependencies
Vincent GIRAUD

When developing digital products, the dependencies exhibited by the software created are a major source of vigilance for publishers and designers. While they have the advantage of massively accelerating and simplifying work, and while they allow to benefit from robust and well-tested executables and content, they also bring many threats.

These threats are present both in dependencies that apply during development and in those that appear during software use. Moreover, assuming that they are necessarily the result of malicious intent or of an explicit attack would be a mistake: many simply arise from the very characteristics of the process based on reusing or exploiting external content. The associated threats and risks are thus particularly multifaceted.

36 Post-quantum transition: the state of play 10 years after the NSA's shocking announcement
Simon ABELARD and Ludovic PERRET

Although it has been well-known since 1994 that a sufficiently large quantum computer poses a threat to the current standards of cryptography, this threat did not become blatant until 2015, thanks to American administrations such as the NIST and the NSA. Ten years later, the time has come to assess the urgency of the quantum threat, the efforts implemented from both sides of the Atlantic Ocean and the challenges to come. At first glance, it seems that Europe may be lagging behind but a deeper dive in the subject allows us to highlight both the strengths and weaknesses of the Old Continent.

44 Cyber issues related to victims
Jérôme MOREAU

In a world increasingly dominated by the use of digital tools, it is clear that our society faces numerous sources of insecurity and criminal offences. The scale of the phenomenon, in economic, psychological, human, societal and social terms, requires the promotion of multidisciplinary, personalised and tailored support for victims. Cyberattacks have several aims: to steal identities and personal data, to obtain money illegally, or to commit sexual offences.

The France Victimes network, made up of 130 associations in mainland France and overseas, has adapted to ensure that no victim is ever left alone. The expertise gained over almost a decade of welcoming and supporting victims suggests that it is important to accurately understand the consequences of the trauma suffered by our fellow citizens in order to better help them through these violations of criminal law.

Evolution of cyber governance

from vital data, or erode donor trust. To address this, Hack4Values, an association founded in France in 2021, created the first free humanitarian Bug Bounty program for NGOs. By mobilizing a community of ethical hackers, it protects those who protect. Through this testimony, we share the challenges, results, and urgency of recognizing the role of ethical hackers in building sustainable humanitarian cybersecurity.

71 Integrating cybersecurity into industrial professions

Fabrice BRU

Long focused on operational safety and physical security, industry has been slow to recognize the digital threat, revealed by Stuxnet (2010), WannaCry/NotPetya (2017), and then the waves of attacks of 2021-2022. In a geopolitical context marked by the actions of state proxy groups carrying out disinformation and cyberattacks to weaken economies and institutions, industrial cybersecurity is becoming a major strategic issue. However, the specific nature of industrial information systems makes protection more complex.

This article highlights three levers: integrating cyber risk into industrial processes, developing hybrid IT/OT technologies (digital twins, IoT, protocol convergence), and investing in mixed skills through continuing education, academic programs, and peer-to-peer sharing. Integrating cybersecurity thus appears not as a constraint, but as a factor of resilience, performance, and competitiveness.

The French strategy – HR challenges

77 National Strategic Review, OS12 – Towards a National Cybersecurity Strategy 2025-2030

Jonathan COLLAS

The 2025 National Strategic Review set the ambition of achieving first-rank cyber resilience in a world marked by the hybridization of threats and growing dependence on digital infrastructures. The 2025-2030 National Cybersecurity Strategy is its operational implementation. It is built on consolidation: capitalizing on more than fifteen years of experience – from the creation of ansSI to successive strategies, from the 2018 Cyber Defense Strategic Review to the France 2030 plan – in order to take a decisive step forward.

Five pillars structure this ambition: developing talent, strengthening national resilience, countering threats, securing digital foundations, and acting at the European and international levels. Proportionate obligations, tailored support, open governance, and the mobilization of the French cyber industry combine to provide France and Europe with the confidence needed to face the challenges of cyberspace.

84 Cybersecurity and digital professions: a strategic challenge for the State

Stéphanie SCHAER

At a time when digital transformation is accelerating within government agencies, cybersecurity is becoming a strategic challenge that directly affects the quality of public services and depends heavily on dedicated human resources. Cyberattacks targeting institutions highlight an obvious fact: the security of systems depends as much on the technologies as on the women and men who use them. Attracting talent, training and raising awareness among all employees, and developing a shared culture: these are the conditions that the Interministerial Digital Directorate (DINUM) works on every day to strengthen the resilience of the State and assert its digital sovereignty.

the emergence of startups to the consolidation of the ecosystem, including the challenges of maturation and scaling up, this article reviews the measures taken by the French government, within the framework of France 2030, to align the national cybersecurity offering with the challenges of European regulation and the impacts of world geopolitics.

Despite an immense effort, the EU is not mature enough to face modern cybersecurity challenges. Inspired by Erasmus's Praise of Folly, the author, a veteran of the EU cyber ecosystem, comments the Union's current path.

The Laus, praises the EU's diligence in building a regulatory fortress (NIS 2, DORA, CRA) and institutions (ENISA, ECCC).

However, a critique (Pars Destruens) highlights deep paradoxes. This regulatory approach mistakes procedural compliance for operational security: a static, "tick-the-box" mentality. Furthermore, EU-level bodies act merely as coordinators for fragmented national « "stovepipes"» rather than creating a unified defence.

The proposal (Pars Construens) calls for a paradigm shift away from static security. « "Resilience by Design"» is advocated as a philosophy that accepts breaches will occur and focuses on maintaining critical functions during an attack. This requires a new goal of holistic « "Digital Resilience"» and a private-led, public-supported industrial policy.

For Luxembourg, cybersecurity is a strategic pillar of economic attractiveness and resilience. It must be accessible to all businesses, especially SMEs, which play a central role in European value chains.

Luxembourg is committed to supporting cybersecurity innovation by SMEs and for SMEs, promoting open source, data sharing, and the integration of artificial intelligence. This strategy aims to encourage diversity in solutions and strengthen European technological autonomy.

By acting collectively, within the framework provided by European legislation and relying on a dynamic ecosystem, Luxembourg and its European partners can build inclusive, innovative, and resilient cybersecurity, a true driver of competitiveness and trust for the digital economy of tomorrow.

Issue editor
General Éric Freyssinet

Ont contribué à ce numéro

Simon ABELARD est enseignant-chercheur à l'EPITA (École pour l'Informatique et les Techniques avancées). Agrégé de mathématiques et titulaire d'un doctorat en informatique soutenu en 2018, il possède une expertise aussi bien dans les aspects les plus théoriques de la cryptanalyse que dans la cryptographie appliquée. Son parcours reflète cette dualité puisqu'il a d'abord été chercheur postdoctoral à l'Université de Waterloo (Canada) puis à l'École Polytechnique avant d'exercer pendant 4 ans en tant qu'ingénieur au sein du groupe Thales, ce qui l'a amené à participer activement au déploiement de la cryptographie post-quantique aussi bien à travers des études amont qu'au sein de projets d'ampleur liés au spatial et à la défense. Il a co-signé plus d'une dizaine de publications et de brevets.

→ ***Transition post-quantique : état des lieux 10 ans après l'annonce choc de la NSA***

Boussad ADDAD est expert en intelligence artificielle et travaille au sein de cortAIx Labs, Thales. Il a obtenu son doctorat à l'École Normale Supérieure de Paris-Saclay en 2011. Il est l'auteur de plusieurs articles publiés dans des revues et conférences, ainsi que des brevets. Après 2 ans en tant que chef de projet en robotique, il travaille actuellement chez Thales sur l'application de l'IA à différents domaines comme la cybersécurité ou le traitement du signal. Étant donné les vulnérabilités des modèles basés sur l'apprentissage automatique et la criticité des produits Thales, il travaille également sur la robustesse de l'IA face aux attaques spécifiques à l'IA. Enfin, il est l'auteur de plusieurs ouvrages liés aux technologies numériques, à la souveraineté et à l'intelligence artificielle.

→ ***Les défis de la cybersécurité de l'IA***

Fabrice BRU a une formation universitaire en mathématiques de l'Université Pierre et Marie Curie (Paris VI). Il a débuté sa carrière dans le domaine de la cybersécurité au sein du cabinet de conseil ERCOM. En 2003, il rejoint le groupe Danone, où il contribue à la structuration progressive des pratiques de cybersécurité. En 2008, il intègre la maison Louis Vuitton, au sein de laquelle il développe des approches adaptées aux enjeux spécifiques du secteur du luxe et de la distribution internationale.
En 2018, il prend la direction de la cybersécurité de la STIME, la DSI du groupement Les Mousquetaires. À ce poste, il supervise la stratégie de protection des systèmes d'information d'un écosystème industriel et commercial intégrant plus de 4 000 points de vente et 60 usines. Cette expérience lui permet de consolider une expertise singulière à l'interface entre exigences métiers, innovation numérique et résilience opérationnelle. Souhaitant élargir sa réflexion aux dimensions stratégiques et économiques de la cybersécurité, depuis décembre 2025, il dirige la direction Cybersecurité et Architecture de la STIME.
Fabrice Bru obtient en 2024 un Executive MBA en stratégie et intelligence économique à l'École de Guerre Économique (EGE). Cette formation lui permet d'articuler enjeux techniques, gouvernance et analyse géopolitique dans une perspective intégrée. Parallèlement à ses responsabilités professionnelles, il s'investit dans la structuration de la communauté cyber française. Membre du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) depuis sa création, il en devient administrateur en 2018. En 2025, il est élu président du club, qu'il contribue à développer comme un espace d'échanges, de retours d'expérience et de réflexion stratégique pour les responsables cybersécurité.

→ ***Intégration de la cybersécurité dans les métiers industriels***

Jonathan COLLAS est conseiller industrie et numérique au Secrétariat général de la défense et de la sécurité nationale (SGDSN), au cabinet du Secrétaire général.
Il assure le secrétariat de trois stratégies nationales majeures : la Stratégie nationale de cybersécurité 2025-2030, la Stratégie nationale de lutte contre les manipulations de l'information 2025-2030 et la Stratégie nationale spatiale 2040.
Il est par ailleurs représentant du Premier ministre au conseil d'administration du Centre national d'Études spatiales (CNES).
Ingénieur diplômé de Polytech Montpellier (FR) et de l'Université de Sherbrooke (CA) en microélectronique, il a débuté sa carrière en entreprise de services numériques, à Paris puis à Shanghai, avant de rejoindre le ministère des Armées, où il a occupé plusieurs postes de responsabilité sur les questions numériques et cyber.
Passionné par les questions européennes, il est également ancien auditeur du Cycle des Hautes études européennes de l'INSP (promotion 2023).
→ ***Revue nationale stratégique, OS12 – vers une stratégie nationale de cybersécurité 2025-2030***

Yann DIEULANGARD est chargé d'études et responsable de l'Observatoire du numérique au sein de l'agence Bretagne Next, l'agence de développement économique de la Région Bretagne. Son activité l'amène à suivre les écosystèmes des *pure players* de la filière et de ses satellites depuis plus de 10 ans : cybersécurité, spatial, photonique, électronique, télécom, *data science*, tous traversés par l'axe du numérique durable.
Il est titulaire d'un doctorat en mathématiques, sciences de l'informatique réalisé avec Airbus Defence & Space dans le cadre d'une thèse CIFRE.
→ ***Comment NIS 2 impacte un territoire : le cas de la Bretagne***

Odile DUTHIL est diplômée de l'ENSEA (École Nationale Supérieure de l'Électronique et de ses Applications), ingénieure en télécommunications. Elle débute sa carrière en 1995 au sein du groupe France Télécom, en tant qu'ingénieure en télécommunications.
Après avoir construit une solide expertise dans les réseaux, plateformes de services et systèmes d'information au sein du groupe Orange, elle rejoint en 2018, la direction de la Sécurité du groupe. En 2020, elle intègre le groupe Caisse des Dépôts en tant qu'adjointe du directeur cybersécurité, avant de devenir directrice cybersécurité du groupe CDC.
Odile Duthil est administratrice du Clusif (Club de la sécurité de l'information français) et membre du CESIN (Club des Experts de la Sécurité de l'information et du numérique). Elle est également co-présidente du salon « Les Assises de la cybersécurité » pour l'édition 2025.
→ ***Témoignage d'un recruteur de profils cyber sur l'évolution des besoins***

Éric FREYSSINET est général de gendarmerie, conseiller sénior cybersécurité & cybercriminalité au commandement du ministère de l'Intérieur dans le cyberespace. Il accumule 27 ans d'expérience opérationnelle, technique et stratégique dans le champ de la lutte contre la cybercriminalité en France mais aussi dans des contextes de coopération internationale.
Polytechnicien (X92), il a ensuite suivi un mastère en sécurité des systèmes d'information et des réseaux à Télécom Paris (2000) et accompli un doctorat en informatique sur la lutte contre les *botnets* (2015, Université Paris 6).
Il est aussi impliqué dans la gouvernance d'associations qui contribuent à la cybersécurité et la lutte contre la cybercriminalité (OSSIR, Signal Spam, CECyF, Botconf) et il préside le conseil scientifique de la chaire de Souveraineté numérique et cybersécurité de l'IHEDN.
→ ***Introduction***
→ ***Évolution des menaces de cybersécurité en 2025***

Vincent GIRAUD est chercheur à la chaire cyber et souveraineté numérique de l'Institut des Hautes Études de Défense Nationale (IHEDN). Docteur en sécurité informatique

diplômé à l'École Normale Supérieure (ENS) de Paris, il travaille particulièrement sur les systèmes grand public et dits « sur étagère » lors de sa thèse. Il a également développé son expérience au sein de l'industrie du paiement et de la monétique.
Ses recherches mènent à des travaux en informatique, abordés sous un angle technique, social, légal et géopolitique.
→ ***Les menaces liées aux dépendances des logiciels***

Karolina GORNA est doctorante en cybersécurité et *blockchain* à Télécom Paris et au Ledger Donjon, l'équipe de recherche en sécurité de Ledger. Ses recherches portent sur la sécurité du langage Go appliquée aux couches 2 des *blockchains* publiques.
Diplômée de Télécom SudParis, elle est également titulaire de la certification « Expert en sécurité des systèmes d'information » de l'ANSSI. Elle a été présidente de l'association KRYPTOSPHERE, encadrant plus de 500 étudiants à travers la France.
Par ailleurs, elle a co-organisé l'International Space Apps Challenge de la NASA à Paris et a été primée pour ses travaux sur le climat, la *blockchain* et les chaînes d'approvisionnement. Elle a mené de nombreuses formations pour le MIT Professional Education, l'AFORP et Télécom Paris. Elle participe actuellement aux travaux du Campus Cyber sur la sécurité des cryptoactifs et rédige des analyses techniques sur ces sujets.
→ ***La menace dans le champ des cryptoactifs***

Sylvain GOUSSOT est diplômé de l'École Polytechnique et de Télécom Paris.Il dirige l'EPITA depuis bientôt 2 ans et a un riche parcours dans les entreprises de la Tech. Il a notamment été directeur de l'innovation de Bouygues Telecom et directeur *data* de TF1.
→ ***Face au défi Cyber : entreprises et écoles, un duo essentiel***

Katarzyna KAPUSTA est experte en cybersécurité et travaille depuis 2020 au sein du laboratoire cortAIx Labs de Thales. Elle pilote l'équipe transverse "AI Friendly Hackers" dont l'objectif est de faciliter l'évaluation de la robustesse des systèmes intégrant de l'IA contre les attaques exploitant les vulnérabilités intrinsèques des modèles d'apprentissage automatique.
Elle intervient en tant qu'experte technique sur le sujet de la cybersécurité de l'IA dans les projets de recherches collaboratifs et dans les groupes de standardisation européens, tels que ETSI TC Securing Artificial Intelligence. Elle a obtenu un doctorat en informatique à Télécom Paris en 2018 où elle continue d'enseigner. Elle est l'autrice de plusieurs articles publiés dans des revues et conférences, ainsi que des brevets.
→ ***Les défis de la cybersécurité de l'IA***

Florent KIRCHNER est le directeur du pôle « Souveraineté Numérique » du Secrétariat général pour l'Investissement. Normalien, titulaire d'une thèse en informatique de l'École Polytechnique, il a travaillé au SRI International à Menlo Park, à l'Inria de Rennes, avant de rejoindre le CEA où il a dirigé le Laboratoire Sûreté et Sécurité du Logiciel puis le département Ingénierie Logicielle et Système.
Devenu auditeur de l'IHEDN au sein de la 3e session nationale souveraineté numérique et cybersécurité, il s'engage au SGPI en 2022 comme coordinateur de la stratégie nationale pour la cybersécurité. Il siège au conseil d'administration de l'European Cybersecurity Competence Centre (ECCC) depuis 2023.
→ ***Adaptation de l'offre aux enjeux de la réglementation européenne***

Tiphaine LEDUC est, depuis 2024, la coordinatrice générale de Bretagne Cyber Alliance, le campus cyber breton. Après un parcours d'ingénieur et de chef de projet Europe au sein de PME innovantes, elle a piloté le secteur Numérique et Cybersécurité de l'Agence régionale de développement économique de la Région Bretagne pendant une dizaine d'années.
Elle est actuellement « expert du collège numérique » pour France 2030. C'est une ancienne auditrice de l'IHEDN, Institut des hautes études de défense nationale, session

nationale « Souveraineté numérique et cybersécurité » dédiée aux réflexions stratégiques sur les enjeux de cybersécurité.

→ ***Comment NIS 2 impacte un territoire : le cas de la Bretagne***

Fabien LEMARCHAND est président de Hack4Values, une association qu'il a fondée en 2021 pour protéger les ONG des cybermenaces grâce à un programme unique de *Bug Bounty* solidaire. Ancien Chief Information Security Officer (CISO) chez Cdiscount puis ManoMano, il a plus de 15 ans d'expérience dans la cybersécurité offensive et la protection des plateformes numériques à grande échelle.

Passionné par l'impact social des technologies, il met aujourd'hui son expertise au service du monde associatif et humanitaire. Sous sa direction, Hack4Values a mobilisé une communauté de plus de 50 *hackers* éthiques bénévoles et accompagné plus de 20 ONG internationales (Médecins Sans Frontières, SOS Méditerranée, Action Contre la Faim, etc.).

Fabien Lemarchand intervient régulièrement dans les écoles et des conférences (FIC Lille, Les Assises de la sécurité Monaco, Sthack Bordeaux, Risk Intel TV) et auprès d'institutions publiques pour promouvoir la reconnaissance juridique des *hackers* éthiques. Il est convaincu qu'une cybersécurité durable doit être inclusive, collaborative et alignée avec les 17 Objectifs de Développement Durable de l'Onu.

→ ***Témoignage d'une association humanitaire***

Olivier LIGNEUL est diplômé l'ESIEA en 1994 et débute son parcours professionnel dans le secteur des télécoms avant de rejoindre celui, plus généraliste, des systèmes d'information.

Après avoir intégré les équipes d'architecture d'AT&T, piloté la direction technique hébergement de Colt Telecom, il occupe la fonction de DSI d'un groupe international de 2005 à 2009. Il rejoint l'ANSSI lors de sa création, à la tête des activités assistance et conseil axées principalement autour de l'accompagnement de maîtrises d'ouvrage des ministères et des opérateurs d'importance vitale. Ses équipes se consacreront à l'édition de la méthode EBIOS, l'évaluation des risques critiques, la conduite d'homologation de programmes européennes et de systèmes interconnectés avec l'OTAN.

En 2012, il intègre le Secrétariat général des ministères économiques et financiers et prend en charge la dimension technique du système d'information, assurant la définition des orientations technologiques et des référentiels associés, la mutualisation de l'expertise entre les directions, afin d'accompagner le déploiement des programmes de simplification et de transformation numérique.

En 2015, Olivier Ligneul rejoint le Groupe EDF dont il devient le Directeur Cybersécurité du groupe. Il est également, expert judiciaire rattaché à la Cour d'Appel de Versailles, évaluateur PASSI, en charge de la Communauté des grandes entreprises et administrations (CGEA) du CESIN, président du Club EBIOS et membre du conseil d'administration du Campus Cyber.

→ ***L'adaptation de la gouvernance de la cybersécurité dans un grand groupe***

Juliette MATTIOLI, avec 10 ans dans l'enseignement des mathématiques au niveau secondaire, valide en 1993 un doctorat en mathématiques appliquées à l'intelligence artificielle (IA), abordant l'IA hybride combinant morphologie mathématique et réseaux de neurones. En 1996, elle prend en charge l'activité de recherche en optimisation combinatoire, puis de 2001 à 2016, elle dirige des laboratoires de recherche en IA pour la décision. Considérée comme une référence en IA non seulement chez Thales mais aussi en France, elle est en 2017 l'un des cinq représentants de la France à la conférence des innovateurs du G7.

Depuis 2019, elle est présidente du *hub* « Data sciences & IA » du pôle de Systematic. Reconnue pour sa connaissance des enjeux industriels de l'IA, elle promeut l'IA hybride et contribue au développement d'une nouvelle discipline : « L'ingénierie de l'IA », afin d'accélérer le déploiement industriel et responsable de solutions à base d'IA. Enfin, dès

2020, consciente de la pénurie des talents mais aussi de la transformation des métiers, elle a concouru à la mise en place dans Thales d'un cycle de formation continue sur l'IA, allant de l'acculturation à l'expertise.

→ ***Les défis de la cybersécurité de l'IA***

Marie MOIN, après 20 ans d'enseignement à l'EPITA, dirige depuis 10 ans son centre de formation continue, qu'elle a développé en s'appuyant sur l'expertise de l'école pour accompagner les entreprises sur les enjeux numériques et la cybersécurité.

→ ***Face au défi Cyber : entreprises et écoles, un duo essentiel***

Jérôme MOREAU est aujourd'hui, vice-président et porte-parole de la Fédération France Victimes, premier opérateur associatif d'aide aux victimes en France, vice-président de Victim Support Europe, fédération des associations d'aide aux victimes au niveau de l'Union européenne.

Débutant ses études de droit en 1995, il s'oriente vers une spécialité en droit public à l'Université de Bourgogne où il sera attaché temporaire d'enseignement et de recherches. Il devient, très vite, en 2002, collaborateur d'élus parlementaires et locaux. À partir de 2015, il s'oriente vers la gestion d'établissements pour adultes en situation de handicap. Aujourd'hui, il dirige 8 structures d'accueil et d'accompagnement pour personnes en situation de handicap et pour personnes âgées dans la Nièvre.

Après ses études de droit, il réalise bénévolement des permanences juridiques au sein de l'association France Victimes 58 pendant une dizaine d'années, s'investit en parallèle dans le bureau pour en devenir président au cours des années 2000. Il déploie de nombreux dispositifs, renforce l'équipe pluridisciplinaire, travaille en partenariat pour créer une unité de médecine légale et solidifie l'association dans la Nièvre. Il s'engage dans le conseil d'administration de la fédération France Victimes en 2016, pour devenir trésorier adjoint, trésorier puis vice-président en 2021.

Il est promu Chevalier de l'Ordre national du Mérite en 2021. Il est aussi porte-parole pour promouvoir une vision universaliste, partenariale et égalitaire pour un accompagnement de toutes les victimes.

→ ***Les enjeux cyber liés aux victimes***

Benjamin MORIN a rejoint le Secrétariat général pour l'Investissement (SGPI) en février 2025, en qualité de coordinateur de la Stratégie nationale pour la cybersécurité. Son parcours, long de 25 années dans le secteur de la cybersécurité, est jalonné d'expériences dans les domaines de la recherche, de l'expertise, du management et de la cyberdéfense.

Il a notamment travaillé durant 14 années à l'ANSSI en tant que chef adjoint de la division scientifique et technique, puis en tant que chef de la division détection du CERT-FR. Avant de rejoindre le SGPI, il occupait le poste de fonctionnaire de sécurité des systèmes d'information du ministère de l'Intérieur.

→ ***Adaptation de l'offre aux enjeux de la réglementation européenne***

Ludovic PERRET est professeur à l'EPITA (France), membre associé du LIP6 à Sorbonne Université et chercheur associé au sein de la Chaire Cyber et Souveraineté Numérique – IHEDN, dans laquelle il pilote un groupe de travail sur l'impact du quantique en cybersécurité depuis 2023.

Avec plus de 100 publications académiques, il est spécialisé dans la conception et la standardisation de la cryptographie post-quantique, l'analyse de sécurité des primitives post-quantiques, leur déploiement pratique, ainsi que les enjeux industriels et géopolitiques liés à cette technologie. Il a reçu le premier Prix Atos & Joseph Fourier dans le domaine des technologies quantiques en 2018 pour ses travaux, et a été classé parmi les 100 innovateurs français les plus influents par le magazine *Le Point* en 2022. Il est

également auditeur de la 5e session nationale « Souveraineté Numérique et Cybersécurité » (SNC) de l'IHEDN (2022-2023).

→ ***Transition post-quantique : état des lieux 10 ans après l'annonce choc de la NSA***

Jérôme POGGI occupe le poste de Responsable de la Sécurité des Systèmes d'Information (RSSI) de la municipalité de Marseille. Son parcours combine une formation technique solide et une expérience diversifiée : BTS en Informatique industrielle avec spécialisation en robotique, suivi d'études d'ingénierie informatique.

Il commence son parcours professionnel chez Dassault Aviation, puis passe 7 ans en tant que consultant en sécurité informatique chez Hervé Schauer Consultants, avant de rejoindre la mairie de Marseille en 2008 et d'être nommé RSSI en 2017.

Jérôme Poggi est régulièrement cité dans les médias spécialisés pour son témoignage sur la cyberattaque qui a paralysé la ville en 2020, soulignant les enjeux humains et techniques auxquels les RSSI sont confrontés.

→ ***Témoignage d'un RSSI de collectivité locale : le cas de Marseille***

Luigi REBUFFI est fondateur et vice-président et secrétaire général de la fondation Women4Cyber (W4C) depuis sa création en 2019.

Il est ancien secrétaire général et fondateur de l'ECSO (European Cyber Security Organisation) (2016-2025).

Diplômé en génie nucléaire à l'École polytechnique de Milan en 1983, il a ensuite travaillé en Allemagne sur le projet ITER pour la fusion thermonucléaire. À partir de 1991, il a travaillé chez Thales, où il a assumé des responsabilités croissantes dans le domaine de la R&D européenne, avant de devenir directeur des affaires européennes en 2003. Il a créé l'EOS (European Organisation for Security) en 2007, qui regroupe les plus importantes entreprises et centres de recherche européens, afin de soutenir le développement du marché de la cybersécurité. En 2016, il a fondé l'ECSO pour le PPP avec la Commission européenne sur la cybersécurité. En 2020, il a été nommé dans la liste des "IFSEC Global Influencers in security - Executives".

Parmi ses autres activités actuelles, il est auteur d'articles sur le numérique, la cybersécurité, l'IA et la physique (quantique, relativité...) à des fins de sensibilisation et de vulgarisation.

→ ***Cybersecurity: Is the Union Ready?***

Stéphanie SCHAER, ingénieure générale des Mines, est, depuis septembre 2022, la directrice interministérielle du Numérique (DINUM).

Ancienne élève de l'École polytechnique (1997), elle est également diplômée de l'École nationale supérieure des télécommunications/Télécom Paris.

Son parcours professionnel est notamment marqué par des passages à la direction centrale de la Sécurité des systèmes d'information (DCSSI devenue ANSSI) de 2002 à 2006 puis au ministère de l'Économie, de l'Industrie et de l'Emploi où elle est chargée de mission sur l'électronique embarquée puis chef du bureau de l'Industrie du logiciel de la direction générale de la Compétitivité, de l'Industrie et des Services en 2008.

Elle devient plus tard directrice régionale adjointe des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi (Direccte) de Bourgogne, puis de Bourgogne-Franche-Comté. En parallèle, en 2015, elle lance en tant qu'intrapreneuse la *start-up* d'État, Signaux Faibles, qui permet de détecter précocement, pour mieux les accompagner, les entreprises en difficultés grâce à des données détenues par les administrations. Ce service, aujourd'hui déployé dans l'ensemble de la France, a bénéficié de programmes d'accompagnement de la DINUM : les entrepreneurs d'intérêt général (EIG) et le programme d'incubation des *start-ups* d'État, Beta.gouv.

Stéphanie Schaer devient en 2019 directrice adjointe du cabinet d'Élisabeth Borne, au ministère de la Transition écologique et solidaire puis au ministère du Travail où elle sera

ensuite nommée à la tête du cabinet. Lorsqu'Élisabeth Borne est nommée à Matignon en mai 2022, elle devient conseillère auprès de la Première ministre.
Le 26 septembre 2022, elle est nommée à la tête de la direction interministérielle du Numérique.
Depuis août 2025, elle est également membre du conseil d'administration de Bpifrance.

→ ***Cybersécurité et métiers du numérique : un enjeu stratégique pour l'État***

Edvardas ŠILERIS est directeur du Centre européen de Lutte contre la cybercriminalité (EC3) depuis 2020. Sous sa direction, le Centre s'efforce de prévenir et de soutenir les enquêtes sur les crimes liés à la cybercriminalité, tels que les *ransomwares*, ainsi que les crimes facilités par la cybercriminalité, notamment la fraude en ligne, l'exploitation sexuelle des enfants en ligne et la production ou la diffusion de matériel pédopornographique. Ces efforts sont menés en étroite collaboration avec le groupe de travail conjoint sur la cybercriminalité (J-CAT).
L'EC3 fournit une assistance avancée en matière de criminalistique numérique, de décryptage, de renseignements sur les cybermenaces et de traçage des cryptomonnaies, ainsi qu'une analyse stratégique des cybermenaces et des initiatives relatives à l'accès légal aux données. Le Centre sert également de liaison entre les forces de l'ordre, l'industrie et le monde universitaire par l'intermédiaire des groupes consultatifs de l'EC3 et soutient les campagnes de prévention cybernétique afin de renforcer les actions opérationnelles contre les groupes criminels organisés.
Avant de devenir directeur de l'EC3, Edvardas Šileris a occupé le poste de commissaire général adjoint de la police lituanienne, où il était également chargé de superviser l'innovation. Il a consacré 30 ans à la lutte contre la criminalité.

→ ***Voler, négocier et répéter : les menaces convergentes de la cybercriminalité et du crime organisé en 2025***

Vincent STRUBEL est Ingénieur général des Mines, ancien élève de l'École Polytechnique et de Télécom ParisTech.
Il intègre dès 2005 la direction centrale de la Sécurité des systèmes d'information (DCSSI) devenue, en 2009, l'Agence nationale de la Sécurité des systèmes d'information (ANSSI), autorité nationale de cybersécurité. Il y a successivement occupé les postes de chef de laboratoire, de chef de division et de sous-directeur Expertise.
En juillet 2020, le secrétariat général de la Défense et de la Sécurité nationale (SGDSN) décide de la fusion du centre de transmissions gouvernemental et de la sous-direction numérique de l'ANSSI pour créer l'Opérateur des systèmes d'information interministériels classifiés (OSIIC). Il prend la direction de ce nouveau service à compétence nationale.
Vincent Strubel est nommé directeur général de l'ANSSI le 4 janvier 2023.

→ ***Préface - Un collectif prêt à rehausser massivement les digues de cyberprotection de la Nation***

Arnaud TANGUY est le directeur de la Sécurité du groupe AXA, il dirige l'ensemble des activités de sécurité couvrant la cybersécurité, la sécurité physique, ainsi que la résilience opérationnelle de l'organisation. Il était précédemment Chief Information Security Officer au sein d'AXA Investment Managers où il a piloté la transformation de la sécurité de l'information.
Ancien officier de la Marine nationale française, en charge de l'informatique, des télécommunications et de la sécurité de la base navale de Brest, il a également travaillé dans les secteurs de l'audit et du conseil pour les cabinets EY et PwC, spécialisé en sécurité de l'information et stratégie IT.
Arnaud Tanguy est également président du *think tank* « Le Cercle de la Donnée » et membre du conseil d'administration de « Campus Cyber » en France. Ces organisations à but non lucratif offrent une plateforme permettant aux professionnels de divers secteurs de partager leurs connaissances et leurs idées, dans le but de sensibiliser et de

mieux comprendre les enjeux liés au numérique et à la sécurité dans la société. Par son engagement dans ces organisations, il s'emploie à promouvoir le partage des connaissances, non seulement entre professionnels de la sécurité, mais aussi envers d'autres familles professionnelles et la société.

→ ***Cybersécurité et sécurité physique : une réponse unifiée face aux menaces hybrides***

François THILL est directeur de la Cybersécurité au ministère de l'Économie au Luxembourg.

Après 10 ans d'expérience en informatique dans le secteur bancaire, il a rejoint le ministère de l'Économie du Luxembourg en 2001.

Il a joué un rôle clé dans la création du système d'accréditation luxembourgeois pour les infrastructures à clé publique (PKI), ainsi que dans plusieurs initiatives telles que CASES (Cyberworld Awareness and Security Enhancement Services) en 2003 ; le premier CERT luxembourgeois en 2007 ; ou encore la Luxembourg House of Cybersecurity en 2010, qui héberge le Centre national de compétence en cybersécurité (NC3) ainsi que CIRCL, l'un des CERT nationaux. Il est également co-auteur des stratégies nationales de cybersécurité du Luxembourg.

Par ailleurs, François Thill a représenté le Luxembourg au sein du conseil d'administration de l'Agence européenne pour la Sécurité des réseaux et de l'information (ENISA) de sa création en 2004 jusqu'en 2022. Il est président du conseil d'administration de la Luxembourg House of Cybersecurity, membre du comité interministériel chargé d'assurer la coordination nationale en matière de cyber prévention et de cybersécurité (CIC-CPCS), membre suppléant de la Commission nationale pour la protection des données (CNPD) au Luxembourg, et depuis 2023, membre du conseil d'administration d'une banque systémique luxembourgeoise.

→ ***Approche luxembourgeoise en matière de cybersécurité et PME***