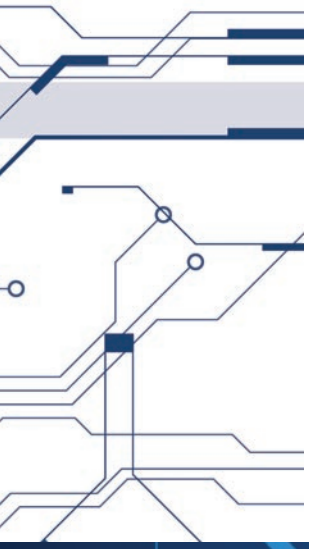
CYBER CERCLE collection



PAROLES D'EXPERTS

2025

PAROLES D'EXPERTS

Ce livre est édité sous la direction de
Bénédicte PILLIET, Présidente du CyberCercle

Préface

BENEDICTE PILLIET
Présidente
CyberCercle

A l'heure où le numérique irrigue l'ensemble de la société, la sécurité et la confiance numériques s'imposent comme des fondamentaux. A la fois enjeux et vecteurs de résilience, de souveraineté et de lien sociétal, elles s'inscrivent désormais au cœur des politiques publiques : elles engagent l'Etat dans ses responsabilités de sécurité et de défense, mais également dans les champs du développement économique et du bon fonctionnement de notre démocratie. Elles engagent également les collectivités et les entreprises, appelées à se protéger dans un contexte de risques accrus, tout en tirant pleinement parti des opportunités que porte intrinsèquement la transformation numérique.

Les contributions réunies dans cet opus 2025 des Paroles d'Experts apportent des éclairages précieux sur les défis d'une transformation numérique de confiance et mettent en lumière plusieurs convictions fondatrices du CyberCercle : le développement d'un numérique de confiance ne peut se concevoir sans une démarche structurée de sécurité numérique ; la sécurité et la confiance numériques ne sauraient être appréhendées sous le seul prisme technique ; elles recouvrent une diversité de plus en plus large de champs et d'enjeux ; enfin, elles ne peuvent être pensées de manière isolée : elles appellent une vision collective, structurée, durable et résolument positive.

Ce nouveau recueil s'inscrit pleinement dans la mission du CyberCercle : offrir un espace de valorisation des idées en associant élus, institutions, acteurs économiques et experts, en dépassant les logiques de silos ; éclairer la décision publique avec des visions complémentaires et diversifiées ; nourrir la réflexion afin de favoriser l'élaboration de politiques publiques efficaces, cohérentes et pragmatiques ; apporter des clés de compréhension aux décideurs dans un

contexte de complexité croissante des enjeux numériques, d'intensification du cadre réglementaire, de développement des risques et d'accélération des technologies.

Je remercie très sincèrement l'ensemble des personnalités qui ont accepté de contribuer à nos Paroles d'Experts tout au long de l'année, nous permettant de publier cet ouvrage. Par la diversité de leurs profils et la qualité de leurs tribunes, elles illustrent pleinement la vocation du CyberCercle : faire dialoguer les points de vue, les analyses, les visions de la sécurité et la confiance numériques, au service de l'intérêt général et d'une transformation numérique pérenne.

Hacker éthique et cybersécurité, est-ce possible ?

MYRIAM QUEMENER
Magistrat honoraire
Docteur en droit
&
AMELIE KOCKE
Consultante en criminalité financière

Hacker éthique et cybersécurité, est-ce possible ?

Face à une actualité particulièrement riche relative à des hackers majoritairement dépourvus d'éthique[1] , il apparaît important de cerner ces personnages de façon plus précise. En effet, les hackers sont encore dans l'ensemble souvent perçus comme des pirates informatiques qui à la fois fascinent et angoissent. Il faut relever que la plupart des hackers dont on parle dans les médias sont en fait des cybercriminels ou « black hat » qui ont attaqué des systèmes d'information ou exploité des failles de sécurité pour récupérer des milliers de données numériques revendues ensuite, y compris dans le Darkweb. Tel est le cas par exemple du mineur de 17 ans récemment interpelé et mis en examen pour avoir piraté de façon massive la base de données de Free, portant sur 19,2 millions de clients français dont 5,11 millions incluant un numéro d'IBAN. Cette base avait été mise en vente aux enchères sur un forum cybercriminel et le mineur, déjà connu pour des faits similaires avait perçu la somme de 10 000 euros pour cette action illicite.

Cependant, tous les hackers ne sont pas tous des cybercriminels[2] qui devraient d'ailleurs être dénommés plutôt crackers que hackers

En effet, certains agissent pour le bien commun et la protection des systèmes d'information d'entreprises ou d'organisations par exemple et sont appelés « white hat » ou hackers éthiques[3]. Parfois, la frontière entre ces deux catégories de hackers peut être faible, certains d'entre eux apparaissant même « borderline », comme par exemple celui qui indique après avoir été cybercriminel être un hacker repenti[4] et avoir retrouvé le brouteur[5] c'est-à-dire l'auteur de l'arnaque au faux Brad Pitt[6] qui a dépouillé une Française d'une somme de 830 000 euros.

L'analyse juridique de ces hackers éthiques qui vient d'être publiée[7] tombe à point nommé en permettant de distinguer ces deux types de hackers et de décrypter l'éthique des hackers afin de comprendre le rôle qu'ils peuvent avoir pour contribuer à la cybersécurité des entreprises et des organisations. Il convient d'aborder en premier lieu le profil des hackers qui sont en fait des cybercriminels, puis le régime juridique des hackers éthiques.

Les hackers cybercriminels

Les hackers qui sont identifiés au terme d'une enquête peuvent faire l'objet de poursuites, notamment sur le fondement des infractions d'atteinte au fonctionnement et aux données contenues dans un système de traitement automatisé de données (STAD). L'entreprise victime de l'acte malveillant pourrait également se prévaloir, selon les circonstances, d'un abus de confiance commis à son préjudice. Selon l'article 323-1 du Code pénal « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 100 000 euros d'amende. Lorsqu'il en résulte soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 euros d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000€ d'amende. »

Ainsi, le simple fait d'accéder ou de se maintenir frauduleusement dans un système de traitement automatique de données peut être sanctionné par la loi pénale. Or, l'activité du hacker éthique consiste à s'introduire dans un système informatique sans droit d'accès afin de découvrir les éventuelles failles du système. En revanche, tous les hackers éthiques n'agissent pas forcément dans le cadre d'un bug bounty ou d'un audit de sécurité.

Aux termes de l'article 323-3-1 du Code pénal « le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ». Les hackers éthiques ne sont pas toujours à l'abri de poursuites sur cette base juridique, par exemple s'ils diffusent des failles de sécurité sans respecter une procédure bien définie avec le client afin d'éviter de nuire à sa réputation[8] numérique.

L'infraction de collecte frauduleuse des données personnelles, punie par l'article 226-18 du Code pénal, a parfois été retenue cumulativement soit avec l'accès frauduleux dans un système de traitement automatisé de données, soit avec l'extraction de données visée par l'article 323-3 du Code pénal. Il est aussi retenu les infractions d'association de malfaiteurs et complicité de tentative d'extorsion. En outre, par exemple dans la procédure Florent Curtet, ce dernier a été condamné à la peine complémentaire d'interdiction d'exercer dans le domaine de la cybersécurité pendant cinq ans, dont quatre avec sursis et des peines d'amende[9]

Les hackers éthiques

Les hackers éthiques dénommés également chercheurs ou hunters par des entreprises craignant les confusions peuvent avoir une place de choix à prendre en matière de cybersécurité, à la condition de s'inscrire dans un dispositif contractuel bien défini pour rassurer les organisations et inspirer la confiance. En effet, l'activité des hackers éthiques consistant à signaler les vulnérabilités des systèmes informatiques afin de les corriger, renforce la cybersécurité. L'intérêt croissant de l'activité des hackers éthiques se reflète notamment avec le développement considérable des programmes de bug bounty.

Face à la complexification technique des cybermenaces, se passer des hackers éthiques semble être un risque pour la protection des systèmes d'information. Il n'est donc pas dans l'intérêt public de restreindre l'activité de ces véritables lanceurs d'alerte informatique.

En France, la signalisation spontanée de vulnérabilités à l'Autorité Nationale de la Sécurité des Système d'Information (ANSSI) par les hackers éthiques est encadrée par l'article L.2321-4 du code de la défense. Cet article réserve l'appréciation de la bonne foi du hacker ayant effectué une signalisation aux collaborateurs du CERT de l'ANSSI (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) sans toutefois en connaître précisément les critères.

Plusieurs propositions législatives ont été réalisées sans avoir été retenues, ce qui démontre la difficulté à concilier d'un côté la défense face aux risques d'abus des hackers d'un cadre juridique trop protecteur et de l'autre côté le manque de garantie d'une absence de sanction pour les hackers en cas de signalement.

Face aux cybermenaces grandissantes visant aussi bien les entreprises, les collectivités territoriales et même les hôpitaux, rechercher et opter pour des solutions efficaces est aujourd'hui une priorité pour l'ensemble des organisations.

Les bonnes pratiques du hacking éthique

Des solutions juridiques existent pour garantir un minimum d'encadrement pour les hackers éthiques. Il s'agit par exemple des contrats de pentests (tests d'intrusion) et des bug bounty. Il s'agit en cybersécurité d'un programme organisé par une entreprise ou une organisation invitant des hackers éthiques à identifier et signaler des vulnérabilités (ou bugs) dans leurs systèmes informatiques, applications, ou sites web. En échange, ces chercheurs reçoivent des récompenses financières ou autres avantages en fonction de la gravité des failles découvertes suite à des pentests[10]. Ces solutions ne couvrent cependant pas le signalement spontané de vulnérabilités qui devrait être davantage sécurisé juridiquement, dans l'intérêt à la fois du hacker et du destinataire de cette transmission qui peut être précise.

Actuellement, les hackers éthiques se font connaître aussi au niveau réputationnel par le biais de ce qu'on appelle des Hackathons[11] des concours de hacking encore peu connus des juristes[12] .

Les préconisations proposées dans l'ouvrage qui vient d'être présenté dans le cadre du CyberCercle résultent d'idées de différents professionnels de la cybersécurité interrogés et de l'analyse de réglementations étrangères comme par exemple la Belgique[13] et la Suisse qui encouragent le recours à ces sentinelles du numérique et qui a élaboré un guide de bonnes pratiques pour clarifier la mission des hackers éthiques. Le but est de préciser les conditions de signalement de vulnérabilités afin d'assurer une protection des hackers éthiques face à un risque de sanction.

Il est donc essentiel désormais, ainsi que l'a fait la Belgique, de définir une véritable doctrine de cybersécurité[14] pour les hackers éthiques qui ont toute leur place dans la protection des systèmes d'information des organisations, des entreprises et des collectivités territoriales. Ils peuvent en effet apporter des solutions pour faire face aux risques toujours croissants de cyberattaques.

Parution le 31 janvier 2025

[1] Le hacker Florent Curtet a été condamné à 2 ans de prison avec sursis pour association de malfaiteurs et complicité de tentative d'extorsion. https://www.lemonde.fr/pixels/article/2024/12/16/le-hackeur-florent-curtet-condamne-a-deux-ans-de-prison-avec-sursis_6452291_4408996.html
[2] Ou « Black Hat »
[3] G.Goubin, L.Janaszewicz « le hacker éthique, votre meilleur ennemi ? », Dalloz IP/IT 2021, p.505
[4] https://www.lalsace.fr/faits-divers-justice/2025/01/18/faux-brad-pitt-cette-campagne-de-cyberharcelement-est-en-train-de-detruire-anne
[5] Escroc opérant sur Internet, notamment sur les réseaux sociaux. Le phénomène d'escroquerie en ligne ou « broutage » est apparu dans les années 2000
[6] On évoque le terme de brouteur.
[7] M.Quéméner , A.Köcke , « Hacker éthique et cybersécurité, opportunités et défis » , Lextenso 2024
[8] https://www.7mag.re/Un-ex-hacker-a-la-rescousse-de-la-victime-du-faux-Brad-Pitt_a19695.htm
[9] Florent Curtet doit aussi s'acquitter d'une amende de 13 000 euros et verser, au total, 39 000 euros de préjudice aux différentes parties civiles.
[10] Test d'intrusion, contraction de l'anglais « penetration test » est une méthode d'évaluation de la sécurité d'un système informatique par la démonstration, par simulation des actions d'attaquants.
[11] Évènement au cours duquel des spécialistes se réunissent pendant plusieurs jours autour d'un projet collaboratif de programmation informatique ou de création numérique
[12] F.Meuris – Guerrero, Les réunions nocturnes des hackers éthiques, Communication Commerce électronique n°9, septembre 2018, alerte 67
[13] https://www.lemonde.fr/economie/article/2024/12/05/en-belgique-l-essor-du-hacking-ethique_6431562_3234.html
[14] M.Quéméner, A.Köcke, Hacker éthique et cybersécurité , opportunités et défis, Lextenso 2024

La Cyber Verte : un Manifeste pour un Numérique Durable

ELISE BRUILLON
Directeur Général
STRAAD.A
&
EL YAMANI HAMEDI
Directeur Général Associé
STRAAD.A

Introduction

Les entreprises et les institutions publiques, engagées dans leur transformation numérique, évoluent dans un monde toujours plus ouvert et plus connecté. Si l'économie numérique offre de nouvelles opportunités, elle s'accompagne également de risques et de menaces de plus en plus sophistiqués.

Dans ce contexte, les activités de protection et de sécurisation génèrent une dette écologique croissante : la sécurisation des infrastructures critiques, notamment énergétiques, repose sur l'ajout de protections physiques et numériques, entraînant une augmentation des équipements, du traitement des données et par conséquent de la consommation énergétique.

Paradoxalement, cette nécessité s'oppose à la dynamique actuelle d'optimisation énergétique, où l'objectif est de consommer moins et mieux. Ce paradigme soulève un défi majeur : comment renforcer la cybersécurité sans compromettre l'efficacité énergétique, comment renforcer la cyber sécurité en prenant en compte une nécessaire frugalité dans la consommation de ressources par essence énergivore ?

L'enjeu réside dans l'équilibre entre résilience aux cyberattaques et sobriété dans la consommation, notamment en développant des solutions innovantes et éco-efficaces capables de protéger les infrastructures tout en minimisant leur impact environnemental. Il s'agit ici du concept de la dette "Cyber".

Ce paradigme est particulièrement pertinent dans le contexte des villes intelligentes (Smart Cities), où la convergence entre cybersécurité et efficacité énergétique devient un enjeu majeur. Si ces villes optimisent la gestion urbaine, elles n'en demeurent pas moins vulnérables aux cyberattaques :

la prolifération des objets connectés et des systèmes automatisés élargit la surface d'attaque, exigeant des protections renforcées. Il est donc crucial d'adopter une approche équilibrée, intégrant l'analyse des risques cybersécurité dans une démarche éco-responsable pour aligner de concert sécurité et durabilité.

Mais comment garantir la résilience numérique des villes intelligentes tout en respectant les impératifs de sobriété énergétique ?

Les défis et les opportunités de la convergence entre cybersécurité et efficacité énergétique dans le contexte des villes intelligentes

La convergence entre cybersécurité et efficacité énergétique représente à la fois un défi et une opportunité pour les villes intelligentes. D'un côté, la sécurisation des infrastructures urbaines connectées nécessite une puissance de calcul accrue, entraînant une consommation énergétique plus importante. De l'autre, une approche intelligente permet d'intégrer l'efficacité énergétique dans l'évaluation des risques cyber, en identifiant des solutions moins énergivores sans compromettre la sécurité.

Par exemple, dans une ville intelligente, la gestion du trafic en temps réel repose sur un réseau d'objets connectés et de capteurs. Sécuriser ces flux de données tout en réduisant leur empreinte carbone implique de développer

des stratégies de protection adaptées, privilégiant des algorithmes d'optimisation énergétique et des infrastructures résilientes mais sobres. L'implémentation d'une gestion des données économe est également cruciale : limiter la redondance des traitements, favoriser le stockage décentralisé et adopter des technologies plus vertes permettent de réduire l'impact écologique des opérations cybersécurité. Enfin, la sensibilisation joue un rôle clé : éduquer les citoyens et décideurs sur les bonnes pratiques d'une cybersécurité verte encourage l'adoption de solutions responsables et durables. En alignant cybersécurité et sobriété énergétique, les Smart Cities peuvent ainsi allier innovation, résilience et respect de l'environnement.

Un Nouveau Paradigme de Protection Durable

Face aux défis et opportunités qu'offre la convergence entre cybersécurité et efficacité énergétique dans les villes intelligentes, un nouveau paradigme de protection durable doit émerger. Ce modèle repose sur trois piliers essentiels.

D'abord, l'autonomie locale, en développant une cybersécurité décentralisée, mieux adaptée aux réalités régionales et plus résiliente face aux menaces globales. Cela passe par l'éco-conception des systèmes de sécurité, intégrant des architectures plus sobres en énergie et optimisées dès leur conception pour limiter leur impact environnemental.

Les politiques publiques ont un rôle clé à jouer dans cette transition vers des infrastructures numériques plus durables. La mise en place de datacenters verts par exemple doit répondre à des exigences de durabilité claires, mesurables et auditées, en intégrant des solutions comme la récupération des eaux de pluie et l'utilisation d'énergies renouvelables. Par ailleurs, les stratégies de sauvegarde des données ne doivent pas être uniquement centrées sur l'Île-de-France : il est essentiel de repenser l'aménagement du territoire en valorisant les expertises et les infrastructures régionales, afin de renforcer la résilience nationale face aux défis numériques et environnementaux.

Ensuite, la diversité des profils en cybersécurité ; il s'agit, tout d'abord, de favoriser les entreprises et institutions locales, en adoptant une approche de circuit court, permettant de répondre plus efficacement aux besoins des utilisateurs tout en limitant l'empreinte carbone des infrastructures numériques, en encourageant une plus grande mixité, notamment par la présence féminine dans la cybersécurité, et en facilitant l'accès à la formation et à la montée en compétences. Cette diversité est une réponse essentielle au manque de ressources en cybersécurité, en apportant des perspectives nouvelles et en comblant les besoins en expertise.

Enfin, l'innovation responsable, en promouvant des solutions créatives et durables, comme les mises à jour intelligentes qui réduisent la fréquence des patchs de sécurité sans compromettre la protection des infrastructures. Cela fait écho à l'adoption du Security by Design, qui intègre la cybersécurité dès la conception des infrastructures et des systèmes évitant ainsi les corrections coûteuses et énergivores a posteriori. En repensant la sécurité en amont, cette approche permet de réduire la fréquence des mises à jour, de limiter la consommation de ressources et de favoriser des solutions plus légères et plus efficientes. Elle encourage également la créativité en incitant les entreprises à développer des architectures numériques plus résilientes et moins énergivores. En combinant anticipation des risques et efficacité énergétique, le Security by Design s'impose comme un modèle durable, conciliant protection des infrastructures et réduction de l'empreinte environnementale.

Par ailleurs, au-delà des entreprises et des institutions, chaque individu peut jouer un rôle dans cette démarche en adoptant de simples gestes militants pour une cybersécurité plus durable. Une action accessible à tous consiste à supprimer régulièrement les données en doublon ou obsolètes, réduisant ainsi l'infobésité et l'empreinte énergétique liée au stockage inutile. Ce geste, appliqué à grande échelle, contribue à alléger la charge des serveurs, à optimiser les ressources numériques et à favoriser une utilisation plus responsable des infrastructures informatiques.

En adoptant cette approche, les villes intelligentes pourront concilier protection numérique et sobriété énergétique, garantissant un avenir à la fois sécurisé, inclusif et respectueux de l'environnement.

Vers une Cybersécurité Éthique et Durable

Les règles déontologiques professionnelles occupent une place centrale pour aligner cybersécurité et préservation de l'environnement. Les sociétés spécialisées en cybersécurité doivent s'engager à repenser leurs pratiques en intégrant des principes de sobriété numérique et d'optimisation énergétique. Il ne s'agit plus de bâtir des forteresses numériques imprenables, exigeant des infrastructures massives et énergivores, mais d'adopter une cybersécurité flexible et adaptative, inspirée de stratégies de résilience plutôt que d'une logique d'éradication totale du risque.

Cette approche repose sur une distinction essentielle entre prévention et résilience. Plutôt que de poursuivre un idéal de sécurisation absolue, synonyme de surconsommation de ressources, il s'agit de protéger l'actif vital en intégrant une réflexion plus réaliste sur la gestion des risques et la priorisation des ressources essentielles. Là où la cybersécurité traditionnelle se focalisait sur une vision défensive massive, exigeant des capacités et une énergie quasi illimitée, cette nouvelle approche prône une gestion intelligente et ciblée du risque, optimisant ainsi l'impact environnemental. Enfin, cette transition vers une cybersécurité durable implique un changement de mentalité : il ne s'agit plus de contrôler à tout prix, mais d'accepter une part de risque maîtrisé dans une logique d'adaptation continue. Cette philosophie, ancrée dans une vision éthique et responsable, redéfinit les engagements des entreprises du secteur, leur imposant d'intégrer les enjeux environnementaux au cœur de leurs stratégies de protection.

Ce nouveau paradigme de protection durable nous conduit donc inévitablement vers une cybersécurité éthique, durable et responsable, où plusieurs principes clés doivent être intégrés pour assurer un avenir à la fois sécurisé et respectueux de l'environnement.

La première étape exige avant tout le courage, de la part des professionnels du secteur, de prendre une certaine distanciation vis-à-vis des approches traditionnelles. Trop souvent, la cybersécurité a été pensée dans une logique d'accumulation de défenses, avec des infrastructures de plus en plus complexes, énergivores et coûteuses. Il ne s'agit plus de tout

verrouiller, mais d'optimiser les protections en fonction des enjeux réels, en réduisant les surconsommations inutiles et en favorisant des solutions plus sobres et intelligentes. Accepter cette évolution, c'est faire preuve de lucidité et de responsabilité, en intégrant dès aujourd'hui la nécessité d'une protection numérique alignée avec les défis environnementaux.

Cela consiste aussi à penser hors du cadre, penser autrement, à sortir des schémas classiques pour développer des approches plus ingénieuses et audacieuses Cela implique d'oser remettre en question nos partis pris, de dépasser nos biais cognitifs et d'explorer de nouvelles manières d'aborder la cybersécurité et l'efficacité énergétique. Il ne s'agit pas simplement d'innover pour innover, mais d'inventer un modèle repensé en profondeur. Si cette transformation aboutit à une innovation, alors le pari sera véritablement gagné. Concrètement, cela passe par le développement de solutions disruptives comme les smart grids, ainsi que par une refonte de la gouvernance énergétique, en encourageant une gestion intelligente, décentralisée et optimisée des ressources, tout en intégrant des mécanismes de sécurité robustes. Ensuite, il est essentiel de mettre en place une gestion responsable, qui assure une utilisation durable et sécurisée des ressources communes, notamment face aux cybermenaces.

Cette approche doit garantir une distribution équitable de l'énergie, en conciliant protection des infrastructures et sobriété énergétique, pour un monde connecté, résilient et respectueux de l'environnement.

Une autre dimension essentielle est d'adopter une logique du vivant, en reconnaissant que la cybersécurité n'est ni figée ni immuable, mais qu'elle doit évoluer en permanence pour s'adapter aux nouvelles menaces et aux transformations technologiques. Redevenir agile, c'est accepter que la protection numérique ne repose pas sur des forteresses imprenables, mais sur des mécanismes adaptatifs capables de résister, de se transformer et de se renforcer face aux attaques. Nous pouvons ainsi établir un parallèle avec la méthode agile dans le développement informatique, qui privilégie une approche itérative, l'amélioration continue et l'adaptation rapide aux imprévus. Appliquer cette philosophie à la cybersécurité, c'est favoriser des stratégies évolutives, basées sur l'anticipation, l'apprentissage en temps réel, plutôt qu'une vision rigide et centralisée

Cela implique aussi de travailler sur la résilience des écosystèmes et des infrastructures, en intégrant des technologies et des stratégies qui permettent aux systèmes de se régénérer et de s'adapter aux évolutions technologiques et environnementales. Enfin, il est indispensable de développer une approche humaine, en plaçant l'humain au cœur des stratégies de cybersécurité et d'efficacité énergétique. Cela inclut la protection des individus et de leurs données, mais aussi l'accès à une énergie propre et sécurisée, en s'assurant que tous puissent bénéficier de ces technologies de manière responsable et équitable.

Une dernière dimension essentielle repose sur la coopération globale, un levier fondamental pour bâtir une cybersécurité durable et efficace à l'échelle internationale. Face à des menaces qui ne connaissent pas de frontières, s'appuyer sur les initiatives existantes menées par les entreprises, les institutions et les acteurs de la cybersécurité est indispensable. Mutualiser les connaissances, partager les meilleures pratiques et renforcer les synergies permettent de construire des modèles de sécurité alignés avec les impératifs environnementaux. Dans cette dynamique, contribuer à un manifeste étendu au niveau de l'Union européenne offrirait un cadre structurant pour encourager des politiques de cybersécurité responsables, intégrant sobriété énergétique, innovation durable et résilience numérique. En fédérant les acteurs autour d'une vision commune, cette coopération renforcerait non seulement la protection des infrastructures critiques, mais aussi la souveraineté numérique européenne, tout en inscrivant la cybersécurité dans un modèle plus éthique et respectueux de l'environnement.

Ce paradigme que nous pouvons qualifier de cyberfrugalité nous invite donc à concevoir un avenir où la cybersécurité et l'efficacité énergétique ne sont pas seulement des outils techniques, mais des leviers éthiques et responsables pour une société plus résiliente et respectueuse de son environnement.

Conclusion

La convergence entre cybersécurité et efficacité énergétique dans le cadre des villes intelligentes offre de nombreux défis mais aussi des opportunités

considérables. Il est essentiel de développer des solutions novatrices qui permettent de renforcer la sécurité tout en minimisant l'impact environnemental, en intégrant des pratiques éco-responsables et en adoptant des stratégies adaptées aux enjeux locaux. Ce nouveau paradigme de protection durable invite à repenser la manière dont nous concevons la cybersécurité, en la plaçant au cœur de la transition énergétique et en veillant à ce que la résilience numérique soit synonyme de durabilité. En favorisant l'innovation responsable, la diversité des compétences et l'autonomie locale, nous pouvons bâtir des villes plus sûres, plus intelligentes et plus respectueuses de l'environnement. Ce modèle de cybersécurité éthique et durable représente un véritable levier pour construire un avenir équilibré, où la technologie et l'écologie se nourrissent mutuellement, assurant ainsi un développement harmonieux et inclusif pour les générations futures.

Manifeste pour une Cybersécurité Verte :

5 Engagements Clés pour les Entreprises

❶ Intégration de la Cybersécurité dans les politiques de durabilité
- Les entreprises doivent prendre l'engagement d'intégrer la cybersécurité dès la conception des systèmes pour garantir une protection durable et efficace.

❷ Promotion de la Recherche et du Développement dans les Technologies Vertes et Sécurisées
- Les entreprises doivent investir activement dans des technologies innovantes qui optimisent l'efficacité énergétique tout en assurant une protection robuste contre les cyberattaques.

❸ Sensibilisation aux Risques Cybersécurité dans les Initiatives de Développement Durable
- Les entreprises doivent s'engager dans l'éducation et la sensibilisation des employés et des parties prenantes aux enjeux de la cybersécurité et à son rôle dans la durabilité.

❹ Collaboration entre les Secteurs Public et Privé pour Renforcer la Cybersécurité
- Les entreprises doivent encourager les partenariats entre les secteurs public et privé pour partager les meilleures pratiques et renforcer la résilience des systèmes face aux cybermenaces.

❺ Optimisation des Ressources Numériques et Réduction de l'Infobésité
- Les entreprises doivent s'engager à réduire l'empreinte écologique liée aux données et aux systèmes numériques en supprimant les données obsolètes et inutilisées.

Ce manifeste vise à guider les entreprises vers une approche plus durable et sécurisée de la gestion énergétique, en mettant l'accent sur l'importance de la cybersécurité dans la transition vers des économies plus vertes et résilientes.

Parution le 28 mars 2025

L'IA est-elle devenue la clé de tous les projets de transformation ?

HELENE BRISSET
Directrice du numérique
Ile de France Mobilités

L'intelligence artificielle est partout, de plus en plus, dans nos échanges de la vie quotidienne. L'appel à l'IA semble aujourd'hui un impératif de modernité, avec presque en miroir la crainte que s'il n'y a pas d'IA dans un projet, alors il sera définitivement « old school ».

Vraiment ?

Les progrès spectaculaires de l'IA autour de nous masquent une diversité d'usages, présentant à la fois des opportunités réelles et des gains substantiels d'efficacité ainsi que des risques tout aussi réels de fuite d'information et de perte de souveraineté.

Quelle trajectoire alors suivre dans cet environnement très complexe et évolutif ?

Suivons donc l'adage d'un ancien Premier ministre : « Plus un sujet est compliqué, plus il est important de répéter des choses simples ».
Aussi, aujourd'hui, l'usage de l'IA dans un cadre de service public ou professionnel commence par deux questions simples, outre bien sûr celle de son utilité :

- Sommes-nous spécifiques ? et si oui en quoi ?
- Les données à mobiliser sont-elles sensibles ?

Revenons sur ces deux questions.

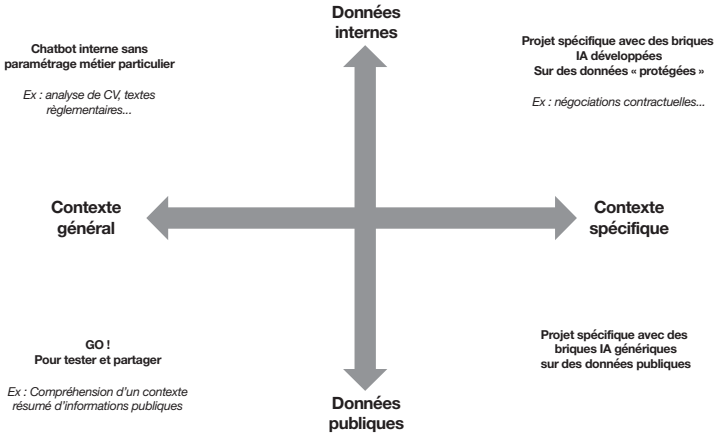
L'IA est entrainée en se nourrissant de ce qu'elle apprend, sur Internet et par les données qui lui sont transmises. L'IA grand public répond à des besoins génériques et est entrainée à grande échelle pour y répondre. Cela donne en général des résultats de très bon calibre sur des questions standard[1], pour laquelle l'IA est très entraînée.

NB : La performance apparente ne doit cependant pas nous faire oublier que l'IA générative fonctionne en mode probabiliste, en donnant la réponse qu'elle pense être la plus probable. Il faut toujours rester vigilant sur la tendance de l'IA de générer du contenu plausible même quand elle ne sait pas, ce qui peut donner des « hallucinations » dont certaines sont parfois spectaculaires. L'IA peut également amplifier des biais appris à partir des données dont elle se nourrit.

En complément, cet entrainement de masse, nourri d'Internet, ne prend pas en compte des besoins spécifiques, ou y répond de manière générique. Cela peut amplifier le risque d'erreur, d'hallucination ou de biais parce que l'IA ne prend pas suffisamment en compte votre contexte particulier qui peut parfois modifier substantiellement la teneur de la réponse souhaitée. Il est bien sûr possible de réaliser un entrainement spécifique[2], en vérifiant qu'il est suffisant et en pensant à le maintenir à jour.

Le carburant de l'IA, ce sont les données. Une question posée à une IA publique avec des données sensibles les divulgue directement en les rendant potentiellement disponibles en réponse à des requêtes futures d'autres acteurs.

La réponse à ces deux questions donne ainsi le cadran ci-contre qui permet de positionner votre contexte d'usage de l'IA :



Par exemple, dans le champ des marchés publics, l'IA peut être utilisée à plusieurs moments dans le cycle de vie d'un marché.

Il faut vérifier alors si les données concernées sont sensibles et si un entrainement générique suffit, en répondant aux deux questions ci-dessus.

- Pour la phase amont de veille et de sourcing, pour laquelle il s'agit généralement de données ouvertes et de questions standards, l'IA grand public peut être très efficace.

- Pour la phase de rédaction, il semble possible pour certains paragraphes de s'appuyer sur une IA généraliste interne, sans entrainement particulier mais en veillant à la protection des données avant publication de l'appel d'offres.

- Pour la phase d'analyse des offres reçues, l'utilisation d'une IA générative grand public est bien sûr proscrite car elle divulguerait les réponses sans tenir compte du secret industriel et de la propriété intellectuelle des candidats. L'utilisation d'une IA interne à qui on « apprend » quels sont les critères d'analyse des offres semble a contrario envisageable en aide au dépouillement.

Concernant les interactions avec les usagers, l'IA peut naturellement être un vecteur important d'amélioration du service et de simplification.

Il s'agit ici impérativement de vérifier si l'IA donne des réponses adaptées à la demande des usagers, et pas juste de jolies réponses formelles parfois déconnectées de la question initiale. Si certaines IA grand public peuvent constituer un premier socle, il y a très probablement une phase d'entraînement spécifique à prévoir pour intégrer le contexte local ainsi qu'une phase de vérification importante pour confirmer, avant l'ouverture du service, la qualité du service obtenu et la lisibilité du parcours usager. Permettez-moi de citer ici deux exemples de déploiement d'IA en appui de la relation usager.

L'application dédiée aux Jeux Olympiques et Paralympiques, Transport Public Paris 2024, a mobilisé de la traduction automatique par IA sur plusieurs langues indo-européennes[3]. Ce service s'est massivement appuyé sur des briques génériques de traduction, avec seulement quelques ajustements à la marge. Une phase de tests préalable importante a néanmoins été nécessaire pour confirmer l'adaptation au besoin.

Pour les transports franciliens, un numéro de téléphone unifié, en cours de généralisation, permet de prendre en compte l'ensemble des appels usagers, jusque-là portés par 106 numéros différents. Pour ce faire, un entrainement très spécifique a dû être réalisé et nécessite une actualisation très régulière pour conserver le niveau de qualité attendu dans les relations usager.

L'intelligence artificielle induit aujourd'hui une transformation très forte de notre environnement. Elle constitue un vrai accélérateur, une sorte d'exosquelette, dont il serait dommage, voire pénalisant, de ne pas pouvoir se servir mais qu'il faut utiliser en sachant pour quel usage et dans quel cadre. Aussi, avant de l'utiliser, demandez-vous toujours si l'IA est-elle correctement entrainée pour ce que vous souhaitez faire et quels sont les risques à la nourrir avec vos données.

Parution le 11 avril 2025

[1] Avec un prompt bien travaillé pour optimiser le retour.
[2] Avec par exemple ce qu'on appelle la technologie RAG (Retrieval-Augmented Generation), technologie qui permet de générer du contenu en s'appuyant sur des sources spécifiques, même en dehors de la phase d'apprentissage.
[3] Allemand, espagnol, italien, portugais

La force de la communauté en cybersécurité : l'exemple de l'aviation

Suite de l'ouvrage "Sécurité numérique & Aéronautique" (Collection CyberCercle – Regards Croisés, 2022)

ERIC VAUTIER
DSI adjoint - RSSI Groupe - Groupe ADP
Senior advisor - CyberCercle

Près de trois ans après la publication du Regards croisés sur la sécurité numérique de l'aéronautique, il nous a semblé intéressant de le rouvrir pour opérer une forme de « droit de suivi », en toute humilité, sur les sujets qui avaient été exposés. L'idée n'est pas de distribuer des bons ou des mauvais points, mais d'analyser ce qui a été fait, ou pas, et d'en tirer des enseignements pour l'action à venir.

Le CERT Aviation France

Considéré, dixit la conclusion de la contribution du Directeur Général de l'Aviation Civile, comme « un outil [à] coconstruire par l'aviation civile pour l'aviation civile », le CERT Aviation France a vu le jour en novembre 2022, matérialisant l'engagement pris par la DGAC un an plus tôt. Constitué autour d'un noyau dur de membres fondateurs, le CERT Aviation France a pour mission principale d'accompagner les acteurs du secteur dans leur montée en maturité en sécurité numérique, que ce soit en matière d'anticipation, de protection ou de réaction à des incidents.

Via les associations représentant les compagnies aériennes, les aéroports, les industriels et les prestataires de service de l'aviation, le CERT Aviation France possède plus de 700 « bénéficiaires » de services essentiels en matière de cybersécurité – réponse à incidents 24 heures sur 24, surveillance

continue de leurs sites Web, formations, etc. – contribuant ainsi au renforcement de la posture cyber de ces entreprises.

Mais la vraie valeur ajoutée est la capacité à faire appel à la solidarité de l'écosystème en cas de besoin. Une parfaite illustration en est le traitement en mode crise du bug Crowdstrike de juillet 2024. A peine quelques semaines plus tôt, le CERT Aviation France avait initié ses briefings quotidiens en prévision de la période des Jeux Olympiques de Paris. Même si la plupart des acteurs de l'aviation n'étaient pas directement touchés, la mise en commun des bonnes pratiques des acteurs plus rôdés a permis à ceux qui étaient directement impactés de mieux réagir – partage technique – et de mieux informer les entités qu'elles impactaient indirectement – partage d'information.

Depuis, les JOP se sont déroulés sans encombre, mais ce briefing quotidien perdure et permet à tout l'écosystème de « prendre la température » – l'état de la menace – grâce au partage des incidents recensés par les uns ou les autres.

Vers l'ISO27AERO ?

Dans sa contribution, Stéphanie Buscayret, alors CISO de Latécoère, appelait de ses vœux la création d'un référentiel de sécurité spécifique à l'aviation « de portée mondiale, auditable depuis tous les pays, reconnu par tous les organismes publics et privés ».

L'intérêt d'un tel référentiel est évident : simplification des engagements contractuels par le biais d'un questionnaire unique quel que soit le donneur d'ordre et réduction du coût de remplissage par les fournisseurs, comparaison facile entre pairs de l'aviation et constitution d'un catalogue cohérent de solutions de sécurité adaptées au secteur. Citée en exemple dans l'article, l'entité BoostAerospace, créée conjointement par Airbus, Dassault Aviation, Safran et Thales, en avait déjà constitué un, nommé AirCyber. Il y a trois ans, AirCyber était circonscrit au périmètre des fournisseurs des quatre sociétés fondatrices et comptait une centaine de membres (sur 7000 possibles).

A nouveau, le principe de communauté a joué à plein : des associations hors

de l'écosystème Airbus ont commencé à s'y intéresser, des discussions se sont engagées, incluant notamment Boeing, l'autre acteur incontournable du secteur, pour déterminer si ce référentiel pouvait passer à l'échelle et être diffusé mondialement. Un consensus a mis quelques mois à être atteint et BoostAerospace a rendu AirCyber *open source* durant l'année 2024, permettant ainsi sa reconnaissance par l'Aviation-ISAC, société américaine à but non lucratif dédiée au partage d'informations de cybersécurité, charge à leurs membres de l'intégrer à leurs contrats.

Un premier palier important avait été franchi, au moment où BoostAerospace atteignait les 300 membres. Mais certaines réticences persistaient, principalement dues au fait qu'il s'agissait de la propriété d'une société fortement liée à Airbus. Et une fois de plus, des échanges constructifs ont commencé à dégager le chemin vers un standard indépendant de toute entité commerciale : la création d'un comité de normalisation et d'un schéma d'accréditation d'auditeurs qualifiés sont en bonne voie, avec la contribution active d'Eurocontrol, dont le statut assure la neutralité idéale pour mener ces débats. Combien de temps faudra-t-il pour aboutir au résultat ? Difficile à dire, mais les acteurs de bonne volonté avancent, laissant envisager des progrès réguliers.

Je conclurai en observant le chemin parcouru et le pragmatisme de la méthode : d'un référentiel interne avec ses défauts à un standard universel, au travers d'une démarche *bottom-up* en mode intelligence collective.

Tirer les leçons de la Part-IS ?

Dans sa contribution, Patrick Ky, alors Président de l'EASA, cite l'ESCP, l'entité montée en 2019 par l'EASA pour conduire la *rulemaking task 720* [je laisse sciemment le vocabulaire anglais]. Les travaux se voulaient un modèle de concertation pour créer la réglementation en matière de cybersécurité de la sécurité aérienne : l'Agence conviait les compagnies aériennes, les aéroports, les constructeurs, les mainteneurs et les autorités nationales pour que chacun s'exprime sur cette, à l'époque, troisième réglementation européenne en matière de cybersécurité dans l'aérien, après la NIS et la règlementation sur la cybersécurité dans la sûreté. Très rapidement, les « invités », dont je faisais partie, ont compris que les travaux

ne seraient pas collaboratifs. Les demandes de cohérence avec les autres textes ? Balayées : l'EASA se considérait au-dessus des autres et la loi serait un *lex specialis* qui ferait référence. Le fait que les entités les plus matures étaient calées sur l'ISO 27001 ? Idem, l'EASA allait expliquer à tous dans un texte réglementaire, la « Part-IS », une nouvelle manière d'implémenter la cybersécurité. Les craintes que ledit texte soit trop détaillé pour être à même de tenir dans le temps ? Idem : l'EASA aller assurer la veille technologique par le biais d'*Acceptable Means of Compliance*.

La raison ? L'Agence avait un calendrier à tenir – un peu décalé par la pandémie, évidemment – et a souhaité s'y tenir coûte que coûte, au détriment de la concertation.

Le résultat ? Publiée en 2021, la Part-IS est une politique de sécurité suffisamment désalignée avec l'ISO 27001 pour compliquer la vie de tous les RSSI concernés, et six ans plus tard, à quelques mois de l'entrée en vigueur de la réglementation, l'EASA a encore publié des propositions d'amendement des AMC, compliquant à la fois la tâche des entités devant mettre en œuvre les mesures dans un délai court et celle des entités chargées de les auditer. L'histoire n'est pas encore finie, attendons la suite...

Vous devez avoir trouvé dans cette description des points communs avec le processus de transposition de la Directive NIS 2 dans notre pays. Mais, pour la NIS 2, les « AMC », ie les décrets et les arrêtés, ne sont pas encore publiés, ce qui laisse la chance à une transposition, au global, plus collaborative, pourquoi pas en confiant la responsabilité de leur rédaction aux ministères en charge des secteurs concernés. On éviterait peut-être ainsi des textes inadaptés dont l'interprétation nous détournerait finalement de la mise en place des mesures nécessaires pour assurer la sécurité numérique de nos entreprises.

Parution le 25 avril 2025

Le traitement de la cybercriminalité par deux juges d'instruction spécialisés

ELISE TREGUER
Vice-présidente chargée de l'instruction
Pôle financier, Section Criminalité financière et Cybercriminalité
JIRS – JUNALCO

BRICE HANSEMANN
Vice-président chargé de l'instruction
Pôle financier, Section Criminalité financière et Cybercriminalité
JIRS – JUNALCO

Présentation du service CFC

Le tribunal judiciaire de Paris compte plusieurs pôles spécialisés de l'instruction dont le pôle financier composé de deux services : le service économique et financier (SEF) et le service de la criminalité financière et cybercriminalité (CFC). Anciennement dénommé service de la délinquance astucieuse, celui-ci a pris sa dénomination actuelle en septembre 2020 et vu ses effectifs de magistrats portés à 10. Cette période correspond également à l'année de mise en place, au sein du tribunal judiciaire de Paris, de la Juridiction nationale de lutte contre la criminalité organisée (JUNALCO) dont le service CFC est une des composantes.

L'évolution récente du vocabulaire et l'ajout de la cybercriminalité dans la désignation du service en 2020 soulignent d'une part l'évolution de l'appréhension du phénomène de la délinquance économique et financière et d'autre part l'émergence d'un nouveau contentieux lié aux risques du numérique dans la sphère d'intervention de la justice, ces deux secteurs étant étroitement liés. En effet, le risque cyber, à savoir l'ensemble des risqués liés à l'usage des technologies numériques, et la criminalité financière se rejoignent à plusieurs titres et vont de pair avec la digitalisation de l'économie.

La crise de la Covid 19 a accéléré cette tendance.

Si le juge d'instruction est souvent présenté comme un magistrat solitaire, les dossiers dévolus au service se prêtent souvent à la pratique de la cosaisine lorsque la gravité ou la complexité de l'affaire le justifie. Par ailleurs, le pôle financier dispose de plusieurs assistants spécialisés et attachés de justice qui apportent leur soutien aux magistrats instructeurs. Toutefois, avec un seul assistant spécialisé cyber actuellement, cette notion d'équipe autour du magistrat demeure peu étoffée alors que le service CFC fait pourtant face à des dossiers de plus en plus nourris sur un plan technique, ce qui n'est pas sans soulever quelques inquiétudes.

Ce service dispose de compétences particulières d'un point de vue géographique et matériel. Il instruit les dossiers au titre :

De la juridiction interrégionale spécialisée (JIRS) créée en 2004, pour les dossiers revêtant une grande complexité ; de la JUNALCO créée en 2019, opérant au tribunal judicaire de Paris exclusivement, en charge de la lutte contre la criminalité de très grande complexité ; de la compétence concurrente nationale (CCN) qui permet de centraliser des faits de nature cyber ayant lieu sur l'ensemble du territoire. Cette spécificité offre l'avantage de favoriser la cartographie des phénomènes criminels numériques, de permettre les rapprochements et de regrouper de manière cohérente les procédures afin d'élaborer une réponse pénale adaptée.

Panorama des types de dossiers traités

La cybercriminalité recouvre les crimes et délits commis à l'encontre ou par le biais des systèmes d'information. Le service CFC n'a donc pas vocation à traiter les affaires portant sur la haine et la diffamation en ligne, le cyberharcèlement et la pédopornographie en ligne notamment qui relèvent d'autres services de l'instruction.

L'essentiel des dossiers « cyber » traités par le service porte sur des infractions qui constituent le vecteur de la commission d'infractions relevant de la criminalité organisée et financière. Ainsi, le caractère hybride mentionné dans la dénomination du service trouve toute son expression.

Au rang de ces dossiers, il est possible d'en établir une liste, non-exhaustive, qui occupe la majeure partie de nos cabinets : le déploiement de solutions de téléphonie chiffrée à des fins criminelles ; les atteintes aux systèmes de traitement automatisé de données (STAD) : rançongiciels ou faux supports informatiques ; les plateformes d'échanges de cryptoactifs (PSAN) qui contreviennent à la réglementation LBC-FT et participent à l'opacification des flux financiers illicites ; les escroqueries en bande organisée et fraudes de grande ampleur (notamment FOVI, fraude l'investissement du type pyramide de Ponzi ou pig butchering…).

Ont été traitées et sont toujours en cours des informations judiciaires portant sur le déploiement, par des organisations souvent implantées hors du territoire national (en Amérique du Nord notamment), de solutions de téléphonie chiffrée extrêmement sophistiquées par le recours à plusieurs couches de chiffrement et à une infrastructure technique robuste. A titre d'exemple, un dossier, récemment clôturé à l'instruction, a nécessité un investissement conséquent sur cinq années et s'est articulé par la mise en place de méthodes de travail et d'une synergie adaptées pour répondre aux multiples défis soulevés (en terme de ressources humaines, techniques et d'entraide internationale). La mise à jour de très nombreux phénomènes criminels de haute intensité a ainsi permis et permet encore, d'initier, voire d'alimenter, un nombre significatif de dossiers incidents conduisant au démantèlement d'infrastructures criminelles et à des interpellations sur l'ensemble du globe (atteinte à la vie, trafic international de stupéfiants, blanchiment de capitaux…).

Les milliers d'interpellations, tant en France qu'à travers le monde, ont été sources d'un contentieux juridique au volume conséquent générant des jurisprudences très fournies, souvent novatrices, compte tenu des défis et problématiques posés par l'emploi de ces nouvelles technologies (portant notamment sur l'interception de masse ainsi que sur l'admissibilité des éléments de preuves recueillis au moyen d'interception et de captation judiciaires).

La quête d'anonymat se retrouve, par ailleurs, sur Internet par l'utilisation notamment de VPN qui, si elle n'est pas interdite, peut être utilisée pour masquer des activités illégales.

Si le nombre de cyberattaques ciblant les grandes enseignes ou entreprises est constant, on remarque que les groupes de rançongiciels ciblent de plus en plus les petites et moyennes entreprises en raison, sans doute, d'un moindre investissement de ces dernier dans la cyberdéfense. En effet, une simple analyse coûts-avantages oriente les cybercriminels vers les organisations disposant d'infrastructures moins sécurisées. La plupart des opérateurs de rançongiciels choisissent leurs cibles en fonction de la taille, de la probabilité d'un paiement et de l'effort requis pour compromettre les systèmes de la cible.

Le dark web, accessible principalement par le réseau Tor, constitue un catalyseur clé de la cybercriminalité, permettant aux délinquants de partager leurs connaissances, leurs outils et leurs services de manière plus dissimulée.

Les défis quotidiens auxquels nous sommes confrontés s'agissant du recueil de la preuve numérique dans le traitement des dossiers concernent principalement :

L'indisponibilité des données, en particulier lorsqu'elles sont supprimées, en raison de règles incohérentes et inadaptées en matière de durée de conservation des données à des fins répressives ; l'impossibilité de récupération des données, en particulier en cas d'échec de l'extraction à partir d'un support numérique ; le caractère illisible / inintelligible des données, en raison du chiffrement ; l'impossibilité matérielle d'analyser les données dans toutes les situations ; la difficulté à obtenir les données, en raison de système juridiques différents.

La criminalité financière, principalement la fraude à l'investissement et le blanchiment d'argent, reste le domaine dans lequel les cryptomonnaies sont le plus souvent rencontrées. Plusieurs dossiers portent sur des plateformes de cryptoactifs, peu regardantes sur l'origine des fonds, parfois criminels, qui sont transférés par le biais de leur service.

Cette opacification des fonds douteux est accentuée par l'absence de procédure de connaissance du client (KYC) ou le défaut de réponse aux autorités judiciaires ou policières lorsqu'elles sont légalement requises. Les

principales difficultés auxquelles nous sommes confrontés dans ce type de dossier portent sur le traçage des flux de cryptos et l'identification des auteurs des transactions et détentrices des wallets.

Le phishing, sous toutes ses formes (le smishing : SMS/text phishing, le quishing : QR code phishing ou le vishing : hameçonnage vocal), constitue le vecteur le plus répandu d'attaque. La disponibilité du phishing-as-a-service ne cesse d'augmenter. Les kits d'hameçonnage sont largement disponibles, ce qui réduit le niveau d'organisation et d'expertise technique requis pour perpétrer des fraudes.

Services et techniques employés

Dans le cadre des informations judiciaires que nous traitons, nous sommes amenés à déléguer certains actes d'investigation (par commission rogatoire) dont nous conservons la direction des orientations judiciaires. Pour ce faire, dans le domaine de la cybercriminalité, nous avons principalement recours à des services d'enquête spécialisés relevant tant de la police nationale (OFAC), de la gendarmerie nationale (UN Cyber) ou de la Préfecture de Police (BL2C) ou encore DGSI.

En appui, sur les compétences rares notamment (concernant les cryptoactifs), le COMCYBER-MI peut également être mobilisé. En raison de la thématique ou de la spécificité des dossiers, ces services ou offices peuvent être cosaisis avec d'autres offices centraux ou services territoriaux ou SR / BR…

De plus, le ministère de l'Intérieur a mis en place trois plateformes de signalement d'infraction en ligne qui peuvent apporter des éléments de nature à enrichir les investigations en cybercriminalité : PERCEVAL (cartes bancaires), PHAROS (contenu illicite en ligne) et THESEE (escroqueries).

En réponse aux problématiques relevées dans les développements précédents et concernant notamment le chiffrement, il peut être recouru à des techniques d'enquête numériques spéciales telles que l'interception, la captation, la géolocalisation, l'enquête sous pseudonyme, la perquisition

numérique…). Afin d'exploiter les supports numériques, nous faisons également appel à des experts publics ou privés, notamment en cas de chiffrement des supports. Les recherches en sources ouvertes ou OSINT pour Open Source Intelligence constituent également un apport de plus en plus important pour les enquêtes.

Une entraide pénale intense

Le recours à la preuve numérique s'est développé avec la massification et la diversification de l'usage des appareils des outils de cette nature.

Le caractère transfrontalier de la criminalité organisée rend indispensable le développement d'outils permettant l'accès aux données contenues d'une part dans les supports numériques (téléphones, ordinateurs, clés cryptos… dont l'exploitation se fait généralement au cours d'une perquisition) et d'autre part dans les systèmes à distance (accès aux correspondances stockées qui est opérées à l'insu de la personne concernée).

Ainsi, les magistrats instructeurs peuvent être amenés à se déplacer à l'étranger. Ils sont en effet les plus à même d'identifier les matériels nécessaires à la manifestation de la vérité dans le cadre de leur dossier. Leur présence, aux côtés des enquêteurs et/ou magistrats est décisive dans la mesure où ils sont en mesure d'identifier les supports numériques recherchés.

Le volet coopération, indispensable dans les dossiers « cyber », entre autorités judiciaires et policières, est amplement facilité enfin par la participation, à la demande des magistrats instructeurs, des agences européennes que sont Eurojust et Europol. A ce titre, Europol constitue un acteur incontournable compte tenu des moyens humains, logistiques et techniques à sa disposition : plateforme de déchiffrement, task force entre services d'enquête (OTF), plateforme d'Experts Europol (EPE), messagerie sécurisée…

Enjeux et perspectives : les défis sont nombreux, dont :

- l'Intelligence Artificielle dont les technologies dérivées élargissent les possibilités pour les fraudeurs d'atteindre plus de victimes à la fois et rendent l'ingénierie sociale encore plus efficace
- la 6G (prévue pour 2030)
- l'Internet des objets (IOC)
- la communication par satellites
- le développement de l'informatique quantique.

Parution le 16 mai 2025

Un clausier de conformité numérique co-construit : une réponse collective aux enjeux de cybersécurité

BEATRICE BERARD
Présidente - Club des RSSI en Santé
Officier de sécurité - DSII - Hospices Civils de Lyon

Un besoin partagé face à la complexité croissante des exigences

Dans un contexte de montée en puissance des exigences réglementaires en cybersécurité et de multiplication des référentiels (PGSSI-S, NIS2, ISO 27001, HDS, etc.), les établissements, notamment du secteur de la santé, peinent parfois à homogénéiser leurs pratiques contractuelles. La rédaction de clauses de sécurité adaptées, précises et juridiquement solides devient un exercice technique et chronophage.

C'est dans ce contexte qu'est née l'idée d'un clausier de conformité numérique mutualisé[1], conçu par un collectif d'experts réunissant 3 organisations professionnelles : le Club des RSSI en Santé, le Réseau des DPO hospitaliers et l'Association Française des Ingénieurs Biomédicaux. Leur ambition : mettre en commun leurs expériences et besoins pour créer un outil opérationnel, réutilisable et évolutif, au service de tous.

Une démarche collaborative et structurée

Le projet de clausier a vu le jour grâce à l'initiative d'un groupe de travail composé de RSSI inter-établissements, alimenté par le modèle de clausier utilisé à l'Assistance Publique des Hôpitaux de Marseille (APHM) et appuyé par le soutien de la Centrale d'Achat de l'informatique

Hospitalière (CAIH). Il s'inscrit dans une logique de travail en commun, animée par les principes suivants :

- Transparence : toutes les propositions sont discutées en groupe, puis arbitrées collectivement.
- Pragmatisme : les clauses sont conçues pour être applicables sur le terrain, adaptées à différents contextes (prestations de services, fourniture de logiciels, maintenance, infogérance, etc.).
- Interopérabilité : le clausier s'appuie sur des référentiels reconnus et facilite leur intégration dans les documents contractuels.
- Accessibilité : le contenu est rédigé dans un langage clair, structuré par thématique.

Contenu et structure du clausier

Le clausier final se présente comme un document modulaire, organisé en plusieurs sections thématiques :

- Clauses générales de sécurité : référentiels applicables, responsabilités des parties.
- Gestion des identités et des accès : cycle de vie des identités numériques, droits d'accès, authentification, traçabilité.
- Protection des données : conformité RGPD, mesures de pseudonymisation et de chiffrement.
- Exigences techniques : sécurité des systèmes, des flux, des postes de travail, des réseaux.
- Exigences spécifiques : télémaintenance, cloud, sous-traitance, Dispositif médicaux, Intelligence artificielle.

Chaque clause est accompagnée de commentaires explicatifs et de recommandations d'usage, permettant à l'utilisateur de mieux en comprendre les enjeux, les modalités d'application et les points de vigilance.

Un outil vivant, mis à jour collectivement

Conscients de l'évolution rapide des menaces et des normes, les membres du collectif ont voulu inscrire le clausier dans une logique d'amélioration

continue. Un comité de suivi est chargé d'actualiser le contenu annuellement au fil des évolutions juridiques, technologiques et réglementaires.
Le site web du Club des RSSI en santé ICI permet à chacun d'accéder au clausier. Chacun peut proposer des modifications, signaler des cas d'usage en écrivant à contact@listes.rssi-sante.fr, afin de mutualiser les bonnes pratiques.

Cette gouvernance ouverte garantit que le clausier reste pertinent, opérationnel et conforme aux exigences du terrain.

Des bénéfices concrets pour les établissements et leur partenaires

L'utilisation de ce clausier présente de nombreux avantages :

- Gain de temps : les équipes juridiques et techniques partent d'une base solide, validée collectivement.
- Harmonisation : les exigences de sécurité sont alignées entre les établissements, ce qui facilite les échanges avec les prestataires.
- Sécurisation juridique : les clauses sont rédigées dans une logique contractuelle robuste, limitant les zones d'ambiguïté.
- Dialogue constructif avec les fournisseurs : les clauses sont expliquées et contextualisées, favorisant une meilleure compréhension et adhésion des partenaires.

Un modèle reproductible dans d'autres domaines

Au-delà du domaine de la cybersécurité, cette expérience de co-construction d'un clausier ouvre la voie à des formes nouvelles de collaboration entre acteurs publics, fondées sur l'entraide, la mutualisation et la transparence.

Le clausier Conformité Numérique n'est pas seulement un outil technique : c'est le reflet d'une culture de la résilience collective, où chaque acteur, quelle que soit sa taille ou sa maturité, peut contribuer à élever le niveau global de sécurité.

Conclusion

Ce clausier Conformité Numérique n'est pas figé. Il vit, s'adapte, se partage. Il incarne une réponse concrète, humaine et pragmatique à un défi technologique complexe. En misant sur la coopération, le collectif a transformé une contrainte en levier de transformation positive.

Parution le 6 juin 2025

[1] https://www.rssi-sante.fr/clausier-securite-ssi

L'accélération de la résilience numérique du secteur protéiforme de la santé en France

RODOLPHE BACA
Responsable région AURA
ATOS Cybersécurité Services

Introduction

Ensemble nous développerons la thématique de la cybersécurité dans le secteur de la santé en France. Comme à notre accoutumée nous allons rester purement factuel, dans l'analyse rigoureuse des chiffres, des situations dans leur globalité, mais aussi dans leur spécificité. Personne ne peut se targuer de tout connaitre, et s'auto-proclamer expert est souvent gage du contraire. Nous resterons le plus humble possible, sans moralisation, sans critique facile, sans leçon à donner, et surtout, en évitant le sensationnalisme.

Le ton étant donné, commençons par notre ambition dans cet essai. Volontairement destiné à un large public, nous ferons essentiellement une description de l'actuel, en expliquant les situations passées et présentes, et en projetant le futur. Cela fait déjà 2 ans que les premiers exercices de crise d'origine cybersécurité, financés par le ministère de la santé via l'INSTRUCTION N° SHFDS/FSSI/2023/15 du 30 janvier 2023 ont eu lieu. Par ce dispositif, les ARS (Agences Régionales de Santé) et pour certaines via leur GraDeS (Groupement Régional au Développement de la e-Santé) ont pu suivre l'évolution grandissante de la prise en compte du sujet cyber au sein des directions des structures.

Notre retour d'expérience est le suivant. Nous avons pu effectuer à ce jour avec mon équipe, un petit peu plus de 100 exercices, qu'ils aient été du kit débutant, intermédiaire, confirmé ou encore intégralement adapté.

Nous avons pratiqué ceci en sanitaire et médico-social dans le secteur public, établissements supports de GHT ou CH et autres, dans le secteur privé lucratif et non lucratif. Par ailleurs, nous réalisons quotidiennement des analyses de risques, des audits de maturité, des pentests, des mises en conformité, des évolutions d'architectures, des intégrations de logiciels, du SOC, de la réponse à incident, mais également au plus proche des services de santé, avec des évolutions des dispositifs de crise, notamment les fameux « PCRA ».

C'est grâce à cette palette et cette vision à 360° que nous pouvons aujourd'hui vous expliquer ce que sont les SI de santé, expliquer la réglementation en vigueur, retranscrire les réels impacts des cyberattaques récentes, expliquer l'écosystème actuel, enfin, faire une projection des attendus et des incertitudes actuelles. Ceci tendra à argumenter notre optimisme quant à l'accélération de la résilience numérique du secteur protéiforme de la santé en France.

Existe-t-il un SI de santé, ou bien des SI de santé ? Comment inclure la cybersécurité dans un secteur où sa place parait logique, mais en pratique complexe à mettre en œuvre ?

Encore une fois, conservons à l'esprit que nous n'estimons pas tout savoir de tous les établissements de santé en France. Nous donnons notre vision, qui comme tout sujet, est libre d'interprétation et d'amélioration continue. Nous avons rencontré les architectures de SI de santé suivante :

- La première correspond aux structures disposant de serveurs physiques hébergés en interne des bâtiments de la structure de santé, sur lesquels repose une forte virtualisation de serveurs. Les sauvegardes sont fréquemment internalisées mais cloisonnées dans des VLAN isolées, ou encore complètement externalisées. L'administration des réseaux et des systèmes est effectuée en interne par les équipes d'une Direction du Numérique, ou une Direction des SI. L'équipe dispose de professionnels de la cybersécurité notamment d'un RSSI et d'adjoints selon la nécessité, et surtout le

budget dédié. Le recours à de l'hébergement externe existe mais assez peu sur des fonctions critiques telles que le Dossier Patient Informatisé (DPI), ou le logiciel de Gestion Administrative du Patient (GAP). Ceci s'explique par la confiance, justifiée, en l'architecture et la sécurité de cette partie du SI pour maintenir les besoins de continuité et d'urgence de l'établissement. Pour faire simple, un prestataire externe ne ferait pas forcément mieux en termes de capacité, et surtout pas au même tarif… D'autres parties du SI, notamment dans les fonctions supports, tels que des logiciels Sage ou Bluekango se retrouvent plus fréquemment hébergés par leurs éditeurs. Dans la majeure partie des cas, cette situation décrit les SI des établissements supports de Groupements Hospitaliers Territoriaux (GHT), c'est-à-dire les établissements publics les plus importants des métropoles / départements.

- La seconde correspond à des établissements avec peu ou prou la même architecture, mais cette fois des budgets plus faibles et des tensions de disponibilités de personnels IT élevées. Il s'agit également d'établissements, disons « périphériques » aux plus gros établissements régionaux publics, dont les budgets sont liés directement à l'activité et donc à la PMSI (Programme de Médicalisation des SI). Pour faire simple, plus l'établissement a d'activité, plus son budget est élevé. Assez logique … Mais intrinsèquement pour les structures disons secondaires, les capacités de défense et de résilience y sont donc plus faibles. Est-ce une explication au fait que les structures de santé cyber-attaquées récemment, correspondent pleinement à ceci (Dax, Villefranche, Versailles, Sud Francilien, Brest, Armentières…), lorsque des structures telles que l'AP-HP, les HCL sur Lyon, l'AP-HM à Marseille n'ont jusqu'alors pas été frappées par des blocages de leur SI via rançongiciel …

- La troisième correspond à des établissements privés à but lucratif, disposant d'un gigantesque SI centralisé dans un/des datacenters en France, et où les structures de santé ne disposent physiquement chez elles, que de serveurs de « rebond » pour accéder aux ressources centralisées. Cette structure permet ainsi de centraliser

l'administration, les dépenses, les compétences, les trajectoires et stratégies. Fréquemment, leur robustesse et leur résilience sont plus élevées que la moyenne du secteur de la santé. Les cliniques, EHPAD ou autres structures fréquemment « rachetées » et donc intégrées au Groupe, viennent ainsi rejoindre ce SI afin d'y bénéficier de la maturité cyber. Volontairement nous simplifions les difficultés d'intégration et la gestion des changements de ce type de projet de migration car ce n'est pas le sujet ici …

- La quatrième correspond aux structures privées lucratives ou non-lucratives, à taille plus modérée, disposant d'infogéreurs, et qui parfois doivent jongler entre plusieurs infogéreurs en parallèles car les établissements de santé sont géographiquement éloignés. Ceci amène à une disparité de la maturité des établissements de ces groupements ou associations du fait de leur dépendance à leurs infogéreurs.

Une fois que l'on a décrit la grande majorité des architectures des SI de santé en France, il convient d'expliquer que malgré ces différences, au final quand nous ouvrons le capot, le contenu de ces SI est très similaire, lié directement aux métiers de la santé : admettre et soigner les patients, organiser les moyens techniques de soin, disposer de services supports RH et financiers pour effectuer les activités. Ainsi, nous retrouverons quasi-obligatoirement les artefacts suivants :

- Un Dossier Patient Informatisé (DPI), contenant, selon la solution éditeur retenue, le plan de soin, l'historique des prescriptions, les soins et injections effectuées, les relevés divers …

- Une Gestion Administrative du Patient (GAP), débutant à l'admission du patient permettant de suivre son parcours au sein de la structure, de son entrée à sa sortie, fréquemment l'outil contient ou est directement interconnecté avec la PMSI afin de disposer et centraliser l'activité de l'établissement avant transfert vers notamment l'ARS et la CPAM. C'est via l'étape de la GAP qu'est, normalement, réglée la problématique de l'identitovigilance.

- Un outil d'imagerie/radiologie/scanner venant alimenter ou non le DPI, et outil de PACS (archivage et transmission d'image).
- Un outil lié aux résultats de laboratoires s'il est internalisé.
- Un outil de gestion de la pharmacie, commande, stock et gestion du parcours du médicament.
- …

« Les Hospices civils de Lyon (HCL) comptent plus de 500 applications sur 14 sites différents et l'Assistance publique-Hôpitaux de Paris (AP-HP) utilise près d'un millier d'applications sur 40 sites », *La sécurité informatique des établissements de santé, Cour des Comptes, S2024-1456*.

A retenir, on voit déjà que pour soigner un patient, une suite de logiciels est interconnectée en permanence pour assurer à chaque étape, une gestion numérique du soin. La situation serait idyllique si un seul outil pouvait effectuer l'ensemble. Aussi, il serait utopique de penser que ces outils communiquent « facilement » entre eux. Selon leur mode de communication, leur écriture, leur versioning, ils pourront ou non s'interconnecter, et transmettre des informations vers les autres outils. Mais tout de même on peut concéder que leur développement est dans la majeure partie des cas, orientée vers leur interopérabilité. Mais, pas forcément l'interopérabilité avec des outils de cybersécurité … Nous avons ainsi rencontré des structures, où les RSI nous ont confié qu'ils avaient dû déconnecter leur antivirus sur le serveur de DPI car cela l'empêchait de « fonctionner » correctement. Cela peut nous paraitre insensé car nous sommes des acteurs de la cybersécurité. Mais c'est oublier que la priorité des structures est de soigner leurs patients. Si un élément se met sur cette route, il doit logiquement s'adapter ou être « retiré ». La cybersécurité doit s'adapter à son contexte, jamais l'inverse. Ainsi on peut trouver aberrant que des ordinateurs dans les services contenant des données personnelles sensibles sur la santé des patients, soient laissés ouverts et accessibles à tous. Mais d'une part, quel est le risque réel ? De savoir que la personne dans la chambre 102 s'est cassée la jambe, ou est atteinte d'Alzheimer ?

Personne n'a jamais vu d'attaquants venir physiquement voler des données de cette façon, de plus, un éventuel curieux serait vite interrompu par le personnel soignant. Ces PC ne sont jamais verrouillés car le besoin métier est de pouvoir accéder aisément à l'information de traitement, quid du nombre de fois où les soignants devraient taper leur code sinon. Ou bien, quid du personnel soignant devant se connecter via une carte d'authentification, et qui malencontreusement oublie cette carte dans la veste qu'il portait hier, il ne va donc pas soigner pour la journée ? Le sujet est sérieux, il convient d'aller plus loin dans la réflexion pour apporter une vraie valeur ajoutée.

A partir de ceci, comment alors améliorer la résilience ?

Afin de répondre aux précédents programmes et à la certification HAS, les établissements ont dû mettre en place des modes dégradés. Fréquemment, il s'agit d'un PC de secours, contenant une extraction automatique du DPI en version PDF, mis à jour à des temporalités différentes (toutes les 30mn, toutes les heures, 3 fois par jour …). Il permet en cas de panne informatique, ou d'électricité, d'accéder de manière secondaire à l'information sur son patient. C'est une réponse intéressante à ces risques, mais à l'époque de leur mise en place, les attaques cyber via ransomware n'étaient pas autant présentes et puissantes. Aujourd'hui, c'est certes une réponse intéressante, mais uniquement si leur configuration est effectuée pour prévenir ce risque cyber. Lorsque l'informatique tombe du fait d'une cyber attaque, c'est le retour au mode papier. Lequel est illustré par des caisses complètes de documents vierges, permettant de noter la prise de température, les injections effectuées, les prescriptions, les observations… qui ne peuvent plus s'effectuer sur les ordinateurs ou tablettes. On pourrait ainsi penser que ces PC de secours, du fait de leur importance, sont plus robustes, mieux sécurisés. Malheureusement ce n'est pas forcément le cas. Dans le meilleur des mondes, ils devraient être isolés dans un pan du réseau différent ayant toutes ses communications filtrées afin d'empêcher la propagation d'un ransomware à leur espace. Leur moyen de communication avec le reste du SI devrait également diverger, on parle de rupture protocolaire (le même principe, en parallèle, s'appliquant au durcissement d'Active

Directory …). Pour faire simple, lors d'accompagnement sur un audit du dispositif de crise, il est nécessaire d'auditer l'architecture, ainsi que fréquemment réaliser un Pentest, afin de se placer dans la peau d'un attaquant et trouver les failles de sécurité du dispositif nominal, et du dispositif de secours.

Aussi, outre les logiciels critiques et secondaires, les SI de santé voient de plus en plus s'intégrer des logiciels tiers nécessaires aux soins, mais source majeure de vulnérabilité. Ainsi on voit se multiplier les objets connectés (frigo connectés, dispositifs anti-fugue, appels malades, robots X ou Y …) ainsi que l'ouverture du SI à de multiples parties prenantes. Pour simplifier, au quotidien, pour le besoin des soins, on multiplie des sources potentielles de vulnérabilités et donc de risques réels pour l'ensemble de la structure de santé. On ne répètera jamais assez la nécessité de disposer d'excellents architectes afin de construire des réseaux cloisonnés.

Si l'on prend un exemple médiatique récent, il est apparu que les appareils Contec CMS8000, transmettaient des flux d'informations sur l'identité de patients et leurs constantes vitales, vers des IP localisées dans une université chinoise. Ceci étant codé en dur dans le logiciel de l'équipement. Pour beaucoup, adepte du sensationnalisme médiatique ou « Linkedinique », on y a vu un espionnage chinois dans la santé des patients français. C'est certes vrai, mais c'est extrêmement naïf de penser que d'une part c'est un exemple isolé, et que d'autre part cela aurait fonctionné. Pour régler le sujet et empêcher tout transfert d'information d'un SI vers une IP externe, on passe par des équipements de filtrage appelés Firewall et Proxy. Dans une configuration de base, les firewalls filtrent les communications de chaque machine, ou type de machines, à accéder ou à n'être accessible qu'à des adresses, ou groupe d'adresses, autorisées. C'est-à-dire qu'il ne rentre et ne sort, que des IP validées en amont. C'est ce que l'on appelle maitriser sa matrice de flux.

Ainsi, dans 99% des cas, aucune donnée de patient français n'a été transmise directement vers la Chine, car tous les firewalls empêchent par défaut ce type de communication. C'est la différence entre la cybersécurité sur Linkedin avec un titre tapageur, et la réelle cybersécurité de ceux qui travaillent au quotidien.

Pour conclure cette thématique, on pourra parler de la hausse récente de la maturité des structures de santé grâce au domaine 1 du programme CaRE que l'on développera après. Il convient de noter que 3 sujets étaient ambitionnés :

- Le durcissement de l'Active Directory des établissements,
- Le renforcement de l'exposition sur internet,
- La prise de conscience du Top management par la réalisation des exercices de crise cybersécurité.

Suite à la réalisation des actions, soit directement en interne soit via des prestataires industriels, les structures peuvent obtenir le financement des travaux selon leur éligibilité et le montant maximal qui leur est alloué. Très clairement, cette année 2024, et début 2025, a confirmé que cette première étape a considérablement amélioré la résilience des établissements de santé.

Finalement, nous espérons avoir pu démontrer que derrière la pensée d'un secteur de santé homogène, il y a vraiment des SI totalement différents et sujets à des risques plus ou moins élevés.

Un accroissement réglementaire, une organisation institutionnelle en constante évolution, des financements fluctuants : signe d'une stratégie par à-coup plus que par planification à long terme

Depuis 10 ans on observe une augmentation du nombre d'établissements de santé avec l'obligation légale d'intégrer les risques et des objectifs en termes de cybersécurité.

Cela a commencé par la première loi de programmation militaire (LPM), faisant entrer une grosse dizaine d'établissements publics sous le champ d'application des opérateurs d'importances vitales (OIV). Bien que la liste des OIV ne soit pas communicable (Article R1332-3 du code de la Défense) il est très simple de trouver les établissements de santé qualifiés :

ils disposent obligatoirement d'un Officier de Sécurité, information malheureusement trop souvent partagée sur Linkedin (pour booster son égo) ou autres réseaux professionnels. Pour rappel, si cette liste est confidentielle, il convient de maintenir le même degré de confidentialité concernant son appartenance au procédé… Le décret Décret 2015-351 du 17 mars 2015 précise les moyens de contrôle de ces OIV une fois par an, par l'Etat, l'ANSSI ou un industriel qualifié PASSI LPM.

Ensuite, par le biais de la loi de transposition de NIS1, les Opérateurs de Services Essentiels (OSE) ont été identifiés et ils avaient l'obligation, sous contrôle de l'ANSSI, d'identifier et désigner leur Système d'Information Essentiel (SIE). Bien que la quasi-totalité l'ait fait, nous avons reçu récemment d'un établissement support de GHT une demande d'accompagnement pour l'identification de ses SIE. Preuve qu'en 2025, 7 ans après l'obligation initiale, il y a toujours un retard conséquent, indicateur soit de la méconnaissance, soit de l'incapacité budgétaire de la structure à prendre en charge le sujet. L'Etat estimant sûrement, que vu leur activité, et donc logiquement leur budget, il n'était pas nécessaire de prévoir un financement pour répondre à cette obligation légale. On est ainsi passé d'environ 10 structures, à environ 130 structures à devoir intégrer une conformité légale sur la cybersécurité. Sachant que les obligations entre LPM et NIS 1 ne sont bien sûr pas les mêmes, même si les 23 objectifs de NIS1 n'étaient pas franchement complexes…

Aujourd'hui, début mars 2025, les travaux sur la transposition de NIS2 se poursuivent. Sans entrer dans les détails, deux terminologies feront leur apparition : les entités essentielles (EE) et les entités importantes (EI). Dans la santé, il y aura environ 800 futures EE, et 1200 futures EI. Ajoutant le fait que, cette fois, les objectifs de sécurité seront bien plus précis et complexes. On change d'échelle. L'ANSSI avait déjà les plus grands maux à contrôler avant NIS2, avec un budget rapiécé en 2025, bon courage … Ceci expliquant d'ailleurs, la sous-traitance grandissante vers des opérateurs privés entre l'évolution de la qualification PASSI et la création de PACS. A l'heure où les menaces de guerre hybride via la cybersécurité sont à un niveau jamais égalé, nul doute que cette trajectoire devra faire l'objet d'analyse de la part de nos Parlementaires, et il vaudrait mieux que cela soit en amont, et non en aval d'une crise majeure…

Outre NIS2, on parle également du Cyber Resilience Act (CRA) dont l'objectif est de contraindre les fournisseurs par le renforcement de la sécurité des produits qu'ils commercialisent. Cependant, les outils connectés liés au secteur de la santé sont exclus de CRA, car ils sont déjà « couverts » par le RÈGLEMENT (UE) 2017/745 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 5 avril 2017 relatif aux dispositifs médicaux. On parle du marquage « CE ». Or pour les professionnels de la cybersécurité, nous savons très bien que ce marquage n'a aucune valeur réelle et n'est pas un gage de résilience cyber du dispositif. Voilà ainsi une opportunité gâchée d'obliger les fournisseurs de dispositifs médicaux, à mettre en place un haut niveau de cybersécurité. Enfin sur ce sujet, à l'heure où NIS2 pense la cybersécurité dans toute la chaine de sous-traitance, nous savons d'ores et déjà, que les établissements de santé ne pourront jamais être « pleinement » conformes, car ils hébergent en leur sein, des dispositifs médicaux non-conformes. Il n'est pas certain qu'une justification technique, de type « cloisonnement » dans des VLAN spécifiques soit suffisante … On verra donc.

Concernant l'organisation de l'Etat sur la cybersécurité dans la santé, on voit depuis 10 ans que des initiatives sont prises, puis qu'à la faveur du positionnement du sujet numérique dans les gouvernements successifs, des évolutions ont lieu.

Aujourd'hui, le sujet est sous pilotage de la Délégation du Numérique en Santé (DNS), structure tutelle de l'Agence du Numérique en Santé (ANS), et du Fonctionnaire de sécurité des SI (FSSI) auprès du Haut Fonctionnaire de Défense et de Sécurité (HFDS) du ministère de la Santé. Vous me suivez toujours ?… Je vous assure que ça s'est pourtant simplifié.

Cette gouvernance est en charge de la planification à l'échelle nationale de la stratégie numérique des établissements sanitaires et médico-sociaux. Pour cela, le Ségur du numérique a vu le jour, financé par l'Union Européenne à hauteur de 2 milliards d'euros à sa présentation en 2021. L'ambition était « de généraliser le partage fluide et sécurisé des données de santé entre professionnels de santé, du social et du médico-social et avec l'usager pour mieux prévenir, mieux soigner et mieux accompagner ». Difficile aujourd'hui de retrouver l'information, mais à l'origine la somme destinée

à la cybersécurité des établissements de santé, était chiffrée à… 0 €. Dans le détail, on peut encore trouver sur internet des publications de 2022, notamment ici, la répartition originelle : 1,4 milliard sur le partage de données de santé, et 600 millions dédiés au secteur médico-social. Depuis, la communication a étonnamment changé, et on trouve en 2024 sur le site du Ségur du numérique, un volet sur la cybersécurité notamment via le programme CaRE. Quelle est la raison de cette évolution ? La volonté de l'Etat au sortir des cyberattaques de 2021 et 2022 d'améliorer la résilience des structures. Ainsi, des sommes initialement prévues ailleurs, ont été déplacées vers la création du programme CaRE, et ce, uniquement car comme le dit la Cour des Comptes, il y a eu « une sous-consommation de crédits prévus pour le développement des usages numériques en santé par les médecins de ville. » Merci donc aux médecins de ne pas aimer le numérique, ceci a permis de financer CaRE sur 2023 et 2024. Or, sur 2025, la Cour indique textuellement que « les modalités du financement du programme CaRE entre 2025 et 2027 devront être précisées. » Nous sommes en fin mai 2025, le domaine 2 du programme CaRE n'est toujours pas paru. Des indices nous avaient pourtant été laissés, notamment par le biais de la Cour des Comptes.

C'est donc l'opportunité de crédit qui a permis la construction d'un financement ponctuel du domaine 1 de CaRE, et non une stratégie coordonnée et planifiée dans le temps.

Au sein des régions, et sous pilotage des ARS, les Groupements Régionaux au Développement de la e-Santé (GRADeS) disposent eux-aussi de financements afin d'accompagner sur leur territoire l'amélioration de la maturité cyber de tous les établissements de santé. En Auvergne-Rhône Alpes il s'agit du GCS SARA. On parle des Centres Régionaux de Ressources Cyber (CRRC). Leurs objectifs et financements sont prévus sur cette INSTRUCTION N° DNS/2024/54 du 2 juillet 2024 relative aux missions des centres régionaux de ressources cybersécurité (CRRC) et à leur financement.

Au final, tant qu'une ligne de financement précise sur le programme CaRE n'aura pas été inscrite, il y a fort à parier que la cybersécurité ne sera financée que grâce au hasard des budgets et crédits.

Dans cette optique, et prenant en considération que la cybersécurité dans le domaine de la santé ne s'est améliorée qu'avec des financements de l'Etat, peut-on raisonnablement penser que la conformité à NIS 2 soit envisageable sur les 3 prochaines années ? Pas si sûr. Laissons donc le hasard décider de la résilience des établissements de santé face aux futures cyberattaques dans un monde toujours plus numérique et belliqueux.

Parution le 20 juin 2025

Le processus de Pall Mall : un effort diplomatique pour encadrer l'essor commercial des outils de hacking

LEONARD ROLLAND
Sous-directeur de la cybersécurité
Ministère de l'Europe et des Affaires étrangères

Face à la prolifération et l'usage irresponsable des capacités de cyber-intrusion disponibles sur le marché, la diplomatie française est à la manœuvre pour faire émerger un consensus international sur un dossier complexe, où volontarisme politique et sens de la nuance sont invités à faire bon ménage.

Une « bombe à retardement »

C'est sur ce signal d'alarme adressé par Vincent Strubel, le Directeur général de l'ANSSI, que s'est ouverte la deuxième conférence internationale du Processus de Pall Mall le 3 avril dernier, à l'initiative du Ministère de l'Europe et des Affaires étrangères et en partenariat avec le Foreign Office britannique.

L'objet de cette inquiétude : la prolifération de capacités de cyber-intrusion disponibles sur le marché, ou CCIC (commercial cyber intrusion capabilities) dans le jargon diplomatique international. Cette catégorie recouvre des produits « clés-en-main », comme les logiciels espions de type Pegasus, Predator, ou plus récemment Graphite, pour ne citer que les plus connus. Les CCIC peuvent également être commercialisées sous la forme de prestation de services, on parle alors de « hackers-for-hire », à l'instar de l'entreprise I-SOON dont l'ampleur des activités cyber-offensives ont été révélées l'année dernière. Enfin, certaines entreprises sont spécialisées dans la vente de composants critiques au développement de capacités de cyber-

intrusion, à l'instar des failles « zéro day », ces vulnérabilités informatiques dont le coût – jusqu'à plusieurs millions d'euros l'unité – est proportionnel à la rareté.

Utilisés de manière responsable, les capacités commerciales de cyber-intrusion jouent un rôle crucial au service de notre sécurité nationale, par exemple en matière de lutte contre le terrorisme ou contre la criminalité organisée. Mais leur usage abusif, régulièrement documenté à travers le monde, porte un triple risque pour :

- les libertés fondamentales, les CCIC étant régulièrement utilisés à des fins de surveillance arbitraire d'opposants politiques, de journalistes ou de défenseurs des droits de l'Homme,
- la sécurité nationale des États, ces capacités venant accroître la menace de cyber-espionnage voire de sabotage pesant sur nos intérêts,
- la paix et la stabilité internationale du cyberespace, car la prolifération des CCIC abaisse d'une part le seuil d'accès aux capacités cyber-offensives et rend d'autre part le travail d'attribution encore plus ardu.

Identifier des solutions à ce phénomène inquiétant, c'est tout l'objet du Processus de Pall Mall, une initiative diplomatique lancée en 2024 par la France et le Royaume-Uni, qui vise d'une part à lutter contre la prolifération de telles capacités, mais également d'autre part à en établir un cadre d'emploi responsable par les États.

Le Processus de Pall Mall, c'est tout d'abord une méthode innovante.

Lancé en février 2024 à Londres, ce processus a donné lieu quelques mois plus tard au lancement par la France et le Royaume-Uni d'une grande consultation auprès des États, de l'industrie, de la société civile et de la recherche. Le but ? Identifier quelles pourraient être les meilleures pratiques en matière de régulation, mais aussi les défis en la matière.

A l'image de l'Appel de Paris pour la sécurité et la confiance dans le cyberespace lancé par le Président de République en 2018, dont il est une déclinaison « sectorielle » sur les enjeux de prolifération cyber, le Processus

de Pall Mall se caractérise en effet par une forte dimension « multi-acteurs ». Lors de ses réunions, s'y côtoient des diplomates, des représentants des services de renseignement et d'agences de cybersécurité, des ONG de défense des droits de l'Homme, des acteurs industriels de la cyber-intrusion…et d'autres acteurs industriels en charge de lutter contre les outils de cyber-intrusion. Ce format permet d'une part d'avoir accès à une expertise la plus large possible ; il permet d'autre part de créer des ponts entre communautés afin de mieux comprendre les points de vue et les contraintes de chacun, voire parfois de favoriser la coopération entre parties prenantes lorsque les intérêts sont partagés.

Ce format inclusif, de même qu'un calendrier soutenu des travaux, font du Processus de Pall Mall un véritable « accélérateur de discussions », pour reprendre les termes d'un participant à la conférence d'avril. Tant au niveau national, où les États ont dû faire émerger en quelques mois une position consolidée sur le sujet (en France c'est le fruit d'une étroite concertation interservices), qu'au niveau international, où le sujet est désormais bien identifié à l'ordre du jour diplomatique, y compris au sein de l'Organisation des Nations Unies.

25 états s'engagent à Paris

La conférence d'avril à Paris a permis l'adoption d'un Code de bonnes pratiques à destination des États pour lutter contre la prolifération et l'usage irresponsable des CCIC. Ce document rappelle le cadre normatif international applicable à l'action des États, détaille quatre grands principes d'action (redevabilité, précision, transparence et contrôle) et recense un grand nombre de bonnes pratiques dans différents domaines, du contrôle export au contrôle des techniques de renseignement, en passant par la transparence en matière de gestion des vulnérabilités ou l'accès au recours juridictionnel par les victimes de cyber-intrusion.

Compte-tenu du caractère extrêmement régalien et sensible du sujet, s'accorder sur un tel document – même si celui-ci est de portée volontaire – représente une avancée importante, a fortiori dans le contexte actuel de polarisation de l'environnement géopolitique et de désagrégation du cadre international de stabilité stratégique. Pour autant, c'est bien la phase de

mise en œuvre des engagements qui s'ouvre qui s'avère la plus cruciale. Le processus de Pall Mall aura ainsi vocation à servir de plateforme d'échange entre ses membres pour l'échange de bonnes pratiques, tandis que la société civile s'organise déjà pour assurer un suivi des engagements pris par les États à Paris. En parallèle, le processus de Pall Mall sert de catalyseur pour la mise en place d'initiatives dédiées au soutien aux victimes.

A moyen terme, l'objectif est de négocier un nouveau Code de bonnes pratiques, cette fois à destination des entreprises. Ce document aura vocation à établir un cadre d'action responsable pour le secteur de la cyber-intrusion aussi bien que pour les entreprises de cybersécurité en charge de lutter contre cette menace.

Cybersécurité et cyberdiplomatie

A l'heure où le numérique rebat les cartes de la puissance, entre Etats, mais également avec certains acteurs privés, la diplomatie a plus que jamais un rôle à jouer dans l'organisation de ces nouveaux rapports de force. Le processus de Pall Mall, s'il ne constitue qu'une partie de l'exercice de désamorçage de la « bombe à retardement » évoquée par Vincent Strubel, a déjà démontré sa capacité à briser les silos qui freinent l'identification de solution : silos entre États, secteur privé et société civile, entre acteurs offensifs et défensifs, ainsi qu'entre les différents leviers dont disposent les États pour lutter contre la menace issue de la commercialisation des outils de hacking.

Parution le 4 juillet 2025

Face à la complexité du monde adoptons l'intelligence du risque et de la menace

JULIEN LOPIZZO
Président Directeur Général
Semkel

Pandémie mondiale, tensions géopolitiques accrues, crises énergétiques et climatiques à répétition, cyberattaques massives et désinformation généralisée : les entreprises et institutions évoluent aujourd'hui dans un contexte de crises multiples, parfois interdépendantes et d'une intensité rarement observée auparavant.

Dans ce contexte crisogène inédit, aucune organisation ne peut plus se permettre de subir passivement les événements : l'anticipation doit devenir une composante centrale et proactive de toute stratégie durable. Pour ce faire, il ne s'agit plus seulement d'évaluer la probabilité d'un risque, mais de prévenir et d'agir très rapidement dès l'apparition des premières menaces en adoptant ce qu'il est convenu d'appeler une intelligence du risque et de la menace. Car, pour les entreprises, passer de la vigilance à la pro-action, c'est non seulement rendre résiliente leur stratégie, mais aussi renforcer leur agilité, optimiser leurs décisions, protéger leur réputation et saisir plus rapidement de nouvelles opportunités.

Cette intelligence du risque et de la menace peut notamment se fonder sur trois piliers.

Premier levier : les signaux faibles

Nous savons aujourd'hui que si un homme tousse à l'autre bout du monde, cela peut impacter nos vies et nos entreprises. C'est dire tout

l'enjeu qu'il y a à mieux détecter les signaux faibles qui annoncent des évolutions ou des ruptures majeures. Comment ? En cartographiant méthodiquement ses propres dépendances et en installant une veille proactive de son écosystème. Vous êtes tributaire des micropuces de Taïwan ? Mettre une surveillance sur la météo de la zone indo-pacifique paraît judicieux pour anticiper, comme à l'été 2021, une intense sécheresse qui ralentit la production ; vous pourrez ainsi changer vos propres plans de production ou vos fournisseurs le temps que la crise soit passée.

Détecter les signaux faibles permet ainsi d'être en avance de phase et d'élaborer des réponses adaptées avant même que la menace ne prenne forme.

Deuxième levier : la préparation

Anticiper implique d'être en permanence prêt à parer toute crise. Cela suppose une véritable "culture de crise" intégrée à tous les niveaux de l'organisation. Si, malgré une bonne cyberdéfense ou une surveillance de votre écosystème numérique (pour contrer le risque systémique lié à la compromission de votre supply chain), vous étiez touché par une cyberattaque (ransomware, exfiltration de données…) comme c'est arrivé récemment à Harvest, Mark & Spencer ou Disneyland Paris, alors vous devez vous poser la bonne question : où était la faille ? Plans de continuité d'activité régulièrement actualisés, entraînements périodiques des équipes, dispositifs d'alerte et processus de prise de décision clairement définis, notamment, doivent ainsi être des réflexes. La préparation devient ainsi une capacité stratégique à part entière, permettant aux entreprises de réagir instantanément et efficacement dès les signes avant-coureurs d'une crise.

Troisième levier : la contextualisation

Pour agir efficacement, il ne suffit pas de détecter les signaux faibles, il faut également être en mesure de les replacer dans leur contexte global. Comprendre les dynamiques économiques, sociales, géopolitiques ou technologiques à l'œuvre permet justement d'interpréter correctement

la portée réelle d'une menace naissante. Même s'il est parfois difficile de distinguer une simple posture politique d'une menace réelle, le programme du président Trump indiquait dès le départ son intention d'utiliser la hausse des droits de douane comme levier de négociation. Surtout qu'en l'occurrence, le premier mandat du président Trump avait permis de confirmer qu'une telle menace pouvait être mise à exécution… Un tel travail de mise en contexte mobilise une expertise transversale, une connaissance fine de l'environnement dans lequel évolue l'organisation et une capacité à croiser différents domaines de compétence pour obtenir une vision globale des risques émergents.

Ne nous y trompons pas, cette intelligence du risque et de la menace constitue, pour les organisations, un changement radical dans leurs méthodes traditionnelles de gestion des risques et de prise de décision. Elle suppose d'abord d'être équipé pour collecter, trier et analyser en temps réel des flux d'informations complexes et multidimensionnels. Elle requiert aussi la capacité de connecter les points, c'est-à-dire de comprendre comment des événements apparemment disparates peuvent s'agréger en crises majeures. Le renseignement économique, la cybersurveillance, l'analyse géopolitique et la veille réputationnelle et informationnelle deviennent, dans ces circonstances, des éléments fondamentaux. Autant de compétences qui ne peuvent plus être pensées isolément : leur efficacité dépend désormais de leur capacité à s'intégrer au sein d'une démarche globale, où ces disciplines dialoguent constamment entre elles, facilitant une compréhension systémique et multidimensionnelle des risques émergents. Ce décloisonnement stratégique s'accompagne d'un changement organisationnel : les entreprises devront soit transformer leur direction du risque actuelle en une véritable direction de l'intelligence du risque et de la menace, soit la créer ex nihilo. Cette nouvelle direction stratégique devra porter, diffuser et ancrer cette doctrine stratégique que ce soit auprès de la direction qu'au sein de chaque branche opérationnelle, facilitant ainsi la prise de conscience collective des enjeux globaux auxquels l'entreprise est confrontée. Une nouvelle organisation qui conciliera vision stratégique, rationalité opérationnelle et mission fondamentale de l'organisation, en intégrant pleinement sa capacité d'anticipation.

Il ne s'agit là rien de moins que d'une véritable révolution culturelle et organisationnelle. Mais elle s'impose aujourd'hui à tous les acteurs, tant une anticipation systémique et décloisonnée est aujourd'hui indispensable pour ne plus subir la complexité et l'incertitude. Loin de constituer une contrainte pour l'organisation, elle en devient, au contraire, un véritable levier stratégique.

Parution le 25 juillet 2025

IA : la supervision comme impératif de gouvernance

GENERAL DE BRIGADE PATRICK PERROT
Docteur en IA
Chargé de mission - Inspection Générale de la Gendarmerie Nationale

Emancipée de son statut de curiosité expérimentale, l'intelligence artificielle (IA) essaime aujourd'hui ses applications dans tous les secteurs d'activité, marquant ainsi sa transition définitive du laboratoire vers le théâtre opérationnel. Les utilisations se multiplient que ce soit dans le domaine industriel ou celui du particulier. Dans le même temps, les nations comme les instances internationales peinent à mettre en œuvre une régulation qui fait consensus. Les exploitations de l'IA se développent trop souvent de manière anarchique sans réelle gouvernance alors que celle-ci demeure le socle d'une utilisation responsable. En sécurité intérieure, l'enjeu de la responsabilité est majeur tant le risque de mésusage peut être à l'origine d'impacts considérables sur les droits fondamentaux : biais non contrôlés, opacité des modèles et des données, détournements d'usage, manque de robustesse cyber. Face à ces enjeux, la nécessité de superviser les systèmes d'intelligence artificielle par l'évaluation et l'audit est devenue à la fois nécessaire et indispensable.

L'IA ne pourra s'imposer en sécurité intérieure qu'à la condition de la confiance du citoyen. Il s'agit alors d'assurer une intégration de l'IA en veillant à une gouvernance placée au bon niveau, à un cadre d'usage qui correspond au juste besoin, à une convergence de compétences, garante de la singularité de l'IA. La facilité croissante de développement des applications d'IA, y compris par des acteurs non spécialisés, renforce encore la nécessité d'une supervision capable d'auditer les systèmes. C'est tout l'objet de mettre en place au sein des organisations sans attendre que cela ne vienne de l'extérieur une instance de supervision, de contrôle

et d'audit des systèmes d'IA. L'objectif est d'assurer à la fois une exploitation légitime et de confiance, et une protection de l'institution face aux dérives et mésusages.

Confiance et légitimité : un double impératif

L'IA suscite de nombreuses inquiétudes quant à une exploitation débridée, notamment au sein des entreprises et des institutions. Alors que le citoyen l'utilise sans réelle exigence dans sa vie quotidienne, il demeure beaucoup plus défiant lorsque cette IA est exploitée par les institutions étatiques ou au sein de l'entreprise. Ce paradoxe oblige les organisations privées comme publiques à mettre en place des mesures assurant une légitimité aux usages. Et ces derniers, pour être durables, doivent répondre à l'exigence de la confiance comme préalable à la légitimité. En effet, confiance et légitimité sont les deux faces d'une même pièce. Alors que la première permet l'adhésion du citoyen, la seconde assure le cadre d'usage dans le respect des valeurs sociétales choisies. Ne pas envisager ces deux volets, c'est prendre le risque d'une désapprobation de l'usage, d'une crise de confiance du citoyen et in fine d'une dépendance aux sirènes venues de l'extérieur.

La célérité de développement de l'IA et de son adoption dans la vie quotidienne a fait oublier que le socle nécessaire à l'adoption est la confiance. Celle-ci ne se décrète pas, elle se gagne et s'entretient. Elle repose sur la connaissance qui permet la compréhension des méthodes trop souvent considérées comme opaques. La connaissance, c'est la capacité à développer et utiliser des systèmes plus fiables, plus robustes et donc plus responsables. Les systèmes sont conçus pour des tâches spécialisées et ne peuvent être généralisés sans impact sur la performance et la sécurité. Il s'agit de s'assurer qu'ils fonctionnent dans des environnements maîtrisés, notamment aux niveaux des biais et des risques cyber. En d'autres termes, connaître les méthodes mathématiques sous jacentes aux systèmes constitue le meilleur moyen pour lutter contre les discriminations et prévenir le détournement des systèmes, tant au niveau des phases d'apprentissage que de décision.

L'impératif de confiance et de légitimité prévient les usages anarchiques et ne doit pas être considéré comme un frein au développement de l'IA. Mettre en place les garanties de supervision est une condition stratégique à une exploitation opérationnelle, efficace, responsable et durable.

Vers une approche intégrée de la supervision de l'IA en sécurité intérieure

La supervision des systèmes d'IA répond à une exigence légale, même si la mise en oeuvre pratique est encore assez peu précise ou tout au moins laisse une liberté de manœuvre dont il faut savoir se saisir. En sécurité intérieure, l'enjeu est double : il s'agit de permettre d'exploiter des systèmes d'IA, protecteur de notre modèle de société, tout en demeurant très vigilant sur l'impact en terme de droits fondamentaux et de libertés individuelles. A cette fin, une approche intégrée qui rassemble les aspects organisationnels, scientifiques et techniques, opérationnels, éthiques et réglementaires apparaît la plus responsable. Chaque aspect couvre un champ d'audit qui apporte confiance et légitimité.

L'audit organisationnel : s'engager en responsabilité

L'adoption de l'IA au sein d'une organisation répond à une exigence de responsabilité en prévenant le développement d'applications anarchiques dénuées de gouvernance comme de réels cadres d'usage. L'objectif de l'audit organisationnel est de s'assurer de la présence d'une gouvernance engagée et de contrôler les garanties de responsabilité dans la chaîne de subsidiarité. Il s'agit d'examiner le niveau de la structure de gouvernance, la répartition des rôles, les mécanismes de priorisation comme de réponse aux incidents mais aussi l'ensemble de la cohérence structurelle. Alors qu'il est souvent clamé que la technologie est neutre, il ne peut en être dit autant des instances de gouvernance mettant en œuvre une technologie. L'audit organisationnel prévient le risque d'une adoption techno-centrée et replace l'humain au sein de l'enjeu de responsabilité.

L'audit scientifique et technique : comprendre pour une meilleure maîtrise

L'objectif de l'audit scientifique et technique est de garantir le niveau de performance des systèmes de la phase de conception à celle de production. Mais l'examen du seul niveau de performance ne peut suffire : il s'agit aussi d'examiner la robustesse des systèmes à des environnements diversifiés en s'assurant de leur résilience en cas de généralisation comme d'attaques cyber. Les systèmes d'IA peuvent très vite devenir des vecteurs de vulnérabilité. Il est essentiel de contrôler que les systèmes fonctionnent dans les limites définies et conformément aux exigences de performance comme de résilience. A titre d'illustration, dans le cadre d'un outil de classification d'images, il s'agira de vérifier la qualité des données d'apprentissage, de validation et de test, le niveau de faux positifs et de faux négatifs en phase de généralisation, la performance requise au point de fonctionnement choisi et de s'assurer de la robustesse face aux manipulations potentielles des données (empoisonnement, deepfakes, attaques adversariales…).

L'audit opérationnel : garantir une action efficace

L'usage opérationnel pour être efficace doit respecter un besoin réel et non s'inscrire dans un usage artificiel. Il est essentiel en IA de s'assurer que le système respecte les limites du cadre d'usage envisagé, est utilisé conformément aux prescriptions requises et prévient toute baisse de compétence professionnelle ou toute perte de responsabilité humaine. En sécurité intérieure, la garantie d'un usage en connaissance est essentiel, c'est une exigence de redevabilité vis à vis du citoyen. Tout utile que soit une application d'IA, celle-ci ne doit pas entraîner une perte de compétence à court, moyen ou long terme. L'IA en milieu professionnel se conçoit comme un outil d'assistance et non d'assistanat.

Il s'agit par exemple en ordre public de conserver la main sur la conception de manœuvre, comme en police judiciaire sur la capacité à qualifier une infraction. Même si elle est efficace, ce n'est pas à la machine de le faire. La performance d'un système d'IA ne signifie pas nécessairement l'efficacité de son usage. Il s'agit aussi de vérifier le niveau

de compétence à l'exploitation des utilisateurs et de contrôler l'évolution du système au fur et à mesure de son utilisation.

L'audit éthique et réglementaire : transformer le risque de dérive en protection stratégique

Les dérives éthiques comme réglementaires sont inévitables si elles ne sont pas appréhendées au plus tôt et en connaissance. Trop d'organisations enferment l'IA au sein des DSI (Direction des Systèmes d'Information) en négligeant la pluralité des exigences de l'IA, notamment éthique et réglementaire. Ce type d'audit doit garantir au citoyen un usage de l'IA qui contrôle les biais, qui prévient la discrimination, qui respecte les libertés individuelles tout en garantissant une protection collective de l'individu. L'efficacité opérationnelle ne doit pas se faire sans contrôle au détriment des droits fondamentaux. Un système d'IA mal configuré, mal utilisé, voire mal conçu, peut influencer directement des décisions impactant illégitimement le citoyen. L'automatisation peut en outre généraliser le mésusage et accroître considérablement l'étendue de l'impact. Cet audit a donc pour objectif de garantir le respect des principes éthiques fondamentaux et de s'assurer de l'application du règlement européen sur l'IA.

Ainsi, en sécurité intérieure, l'IA représente une rupture profonde qui ouvre des perspectives inédites d'efficacité et d'anticipation. Mais elle exige dans le même temps une responsabilité accrue. Dans un contexte où la défiance peut fragiliser l'action publique, seule une gouvernance éclairée, reposant sur une supervision fondée sur des audits rigoureux, permettra de profiter de la puissance de l'IA comme atout stratégique plutôt que la voir constituer une menace.

Loin d'être un frein, l'audit constitue le levier d'une innovation durable offrant la transparence nécessaire à la confiance, la robustesse indispensable à la résilience, et la légitimité sans laquelle aucune technologie ne peut s'ancrer dans le temps. L'avenir de l'IA en sécurité intérieure ne réside donc pas uniquement dans la performance technique, mais bien dans la capacité des institutions à l'intégrer en responsabilité, en prenant en compte sa singularité.

Superviser l'IA, c'est donc faire le choix stratégique de ne pas subir, de protéger sans aliéner, de renforcer sans affaiblir, et de placer la confiance citoyenne au cœur de la puissance publique. C'est à cette condition que l'IA deviendra non seulement un outil opérationnel, mais aussi et avant tout un véritable levier stratégique de sécurité et de souveraineté.

Parution le 26 septembre 2025

Une cyber-souveraineté pour une cybersécurité de confiance

PIERRE-YVES HENTZEN
Président & CEO
Stormshield

La souveraineté numérique s'impose comme un enjeu stratégique majeur pour l'Europe. Et pourtant, les organisations publiques et privées s'appuient bien souvent sur des technologies, des services cloud et des infrastructures développés hors du continent. Or cette dépendance croissante fragilise la maîtrise des données, la sécurité des systèmes critiques et la résilience des chaînes de valeur.

Pour pallier cette problématique, la création d'un nouvel outil d'évaluation, l'Indice de Résilience Numérique (IRN), a été annoncée[1] par un collectif d'acteurs économiques et d'experts. Sa première évaluation, prévue à l'automne 2025, offrira aux organisations un point de référence pour orienter leurs décisions stratégiques. Et si cette démarche marquait une étape vers une prise en compte plus systématique et sérieuse de la souveraineté numérique ?

La cybersécurité au service de la souveraineté numérique

Au cœur de la souveraineté numérique réside la capacité à maîtriser pleinement ses données et ses infrastructures. Cette maîtrise est essentielle pour garantir l'autonomie décisionnelle et la libre disposition de ses ressources numériques. Et dans un contexte mondial marqué par une prolifération constante d'attaques informatiques, qu'elles soient d'origines étatiques, criminelles, à but lucratif ou liées à l'intelligence économique, faire le choix de solutions de cybersécurité européennes s'impose comme un pilier fondamental de cette souveraineté. Ceci, afin

de conserver le contrôle sur les actifs numériques et de protéger les données et les infrastructures contre tout accès non autorisé par des tiers. Ce choix contribue ainsi directement à la construction et à la préservation de l'indépendance stratégique d'une entité.

L'instabilité géopolitique, marquée par un déplacement des conflits sur le terrain cyber, et donc l'intensification des cybermenaces accentuent ces enjeux et appellent à une autonomie stratégique renforcée, fondée sur la confiance et la transparence. Ces tensions peuvent en effet amplifier le risque d'attaques ciblées, soulignant l'urgence de renforcer les capacités de prévention et de réaction des organisations.

Il est donc crucial pour les entreprises européennes de prendre en compte ces tensions, notamment dans le choix de leurs outils. Cela leur permet non seulement de conserver la maîtrise de leurs infrastructures et de leurs données, mais aussi de se prémunir contre l'impact des réglementations extraterritoriales, et, comme cela a été observé récemment, de garantir l'accès à des ressources qui pourraient être coupées à tout moment. Le monde évolue et la dépendance aux solutions de cybersécurité non-européennes représente désormais un facteur de risque majeur.

Garantir autonomie et confiance grâce à des solutions souveraines

Au-delà de la simple évaluation, cette démarche d'indice de dépendance est un grand pas dans la bonne direction. Elle vise en effet à encourager une transition vers des écosystèmes numériques plus fiables, en mettant l'accent sur la maîtrise technologique, la capacité à auditer et à contrôler les codes sources, la proximité des acteurs en cas d'incident, ainsi que la conformité aux réglementations européennes. Une souveraineté numérique solide passe aussi par le développement de solutions conçues pour répondre aux standards locaux dès leur conception, garantissant ainsi une meilleure intégration dans les contextes réglementaires comme la directive NIS2[2] ou le Cyber Resilience Act[3].

Par ailleurs, l'équation entre souveraineté et performance n'implique pas de compromis. En s'appuyant sur des solutions de cybersécurité évaluées ou, a minima, certifiées par des autorités indépendantes comme l'ANSSI[4], il est possible de bénéficier de technologies à la fois fiables et efficaces, tout en préservant la maîtrise des données et des infrastructures. Ces solutions doivent être simples à déployer, afin de protéger efficacement sans freiner la productivité, tout en contribuant à l'indépendance stratégique.

Choisir une solution souveraine renforce la résilience face aux cybermenaces et garantit l'intégrité des données, la confiance et l'autonomie décisionnelle. Pour répondre à ces exigences, les produits doivent non seulement être certifiés, c'est-à-dire évalués selon des critères de sécurité techniques définis par des normes, mais aussi qualifiés par les agences de cybersécurité européennes. La qualification va au-delà de la certification car elle atteste que le produit répond à des besoins opérationnels identifiés par les autorités, qu'il est fiable sur le long terme et qu'il peut être utilisé dans des environnements sensibles. Et si leur code source est également soumis à des audits indépendants, cela permettra de détecter toute vulnérabilité, qu'elle soit involontaire (erreurs de programmation) ou volontaire (backdoors introduites pour des accès non autorisés). Cette démarque renforce la confiance et contribue directement aux objectifs de souveraineté numérique.

Construire ensemble un écosystème de cybersécurité souverain

La souveraineté numérique est l'affaire de tous.

Des institutions publiques aux entreprises privées de toutes tailles, toutes sont concernées par ces enjeux, que ce soit pour protéger les données des citoyens, des collaborateurs ou les informations sensibles à leurs activités. Cette exigence requiert un engagement collectif vers des solutions de cybersécurité dignes de confiance qui contribueront à garantir un écosystème numérique solide et souverain. Il faut également trouver des consensus entre des pays dont les intérêts peuvent parfois diverger, avec des systèmes politiques et des visions qui diffèrent des objectifs de l'Union Européenne.

C'est dans ce cadre que se pose la question des leviers de souveraineté numérique. Il s'agit des moyens et instruments que l'on peut mobiliser pour renforcer l'autonomie technologique et la sécurité des acteurs européens. Identifier et activer ces leviers revient à aborder un sujet vaste et complexe, qui nécessite une coordination étroite entre acteurs publics et privés. Ils concernent à la fois la capacité d'innovation technologique, le développement d'infrastructures sécurisées, le soutien à un tissu industriel local compétitif et la mise en place de normes communes au niveau européen. La première étape consiste à réduire la dépendance vis-à-vis des outils numériques, des infrastructures et des solutions de cybersécurité non européennes.

Dans un marché largement dominé par des acteurs extra-européens, privilégier des alternatives locales permet non seulement de reprendre la maîtrise des technologies et des données, mais aussi d'affirmer une véritable autonomie stratégique en matière de sécurité et de numérique. Ce choix technologique ne se limite pas à une logique de sécurité : il participe également au dynamisme économique. Développer et adopter des solutions européennes revient à soutenir l'industrie numérique et la cybersécurité à l'échelle continentale et à stimuler la création d'emplois qualifiés. À l'inverse, continuer à importer massivement des technologies américaines revient à financer indirectement l'économie numérique des États-Unis, au détriment des capacités locales.

Pour atteindre ces objectifs économiques et renforcer la souveraineté numérique, plusieurs outils sont déjà à la disposition des organisations : le financement de projets de recherche, la coopération et le partage d'informations entre acteurs, l'élaboration et l'adoption de normes communes, ainsi qu'un cadre réglementaire robuste (RGPD[5], NIS2, DORA[6], etc.). Ce sont autant d'initiatives qui visent à consolider un écosystème numérique européen résilient, capable de répondre au défi de la souveraineté, tout en favorisant l'innovation collective.

Réduire cette dépendance signifie aussi limiter l'exposition aux législations extraterritoriales. Le Cloud Act[7] américain, par exemple, autorise l'accès aux données, qu'elles soient privées ou publiques, y compris lorsqu'elles sont stockées hors du territoire américain. Cette

réalité juridique illustre le risque d'un manque de souveraineté : laisser une puissance étrangère disposer d'un droit d'accès sur des données sensibles, à l'insu même de leur propriétaire.

Alors, l'objectif ultime consiste à susciter un véritable élan collectif, capable de fédérer l'ensemble des acteurs publics et privés autour d'un objectif partagé, celui de bâtir un numérique européen autonome, sûr et durable. La souveraineté ne saurait reposer sur la seule volonté de quelques parties prenantes de l'écosystème. Elle exige une mobilisation d'ensemble, cohérente et ambitieuse. La dynamique est néanmoins en marche : les pouvoirs publics multiplient les initiatives en ce sens et, sur le terrain, les entreprises comme leurs clients expriment de plus en plus clairement cette exigence d'indépendance technologique.
C'est dans cette convergence d'actions et de volontés que réside la possibilité de transformer la souveraineté numérique en réalité tangible, au service de la sécurité, de l'économie et de l'avenir du continent.

Parution le 10 octobre 2025

[1] https://assets.rte-france.com/prod/public/2025-07/2025-07-04-cp-indice-resilence-numerique.pdf
[2] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[3] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[4] https://cyber.gouv.fr/
[5] https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[6] https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
[7] https://www.justice.gov/criminal/cloud-act-resources

Angers : les enseignements de la cyberattaque, 4 ans après

JEROME GUIHO
Directeur Général adjoint en charge de la Transition Numérique
Angers Loire Métropole

LUC DUFRESNE
RSSI
Angers Loire Métropole

Victime d'une cyberattaque par rançongiciel en janvier 2021, la ville d'Angers, dans le Maine-et-Loire, a mis deux ans pour se remettre progressivement de l'incident. La municipalité a tiré les enseignements de cette crise.

Que s'est-il passé dans la soirée du 16 janvier 2021 ?

Jérôme Guiho : La Ville et l'agglomération d'Angers ont été la cible d'une cyber attaque, par rançongiciel. C'était un vendredi soir, tout le système d'information a été totalement paralysé. Les conséquences ont été très lourdes et très impactantes pour l'organisation puisque l'ensemble des agents de la collectivité, qui sont connectés au système d'information, ne pouvaient plus travailler avec les outils bureautiques : plus de boîte mail, plus d'accès à la messagerie… Cela a duré plusieurs jours. Nous sommes revenus à la mode du papier et du crayon.

Connaissez-vous l'origine de l'attaque ?

Luc Dufresne : C'est une intrusion avec une demande de rançon pour rétablir le système d'information.

Quel était le montant ?

Jérôme Guiho : Nous ne savons pas, nous avons eu le réflexe de ne pas cliquer. Et de toute façon, et l'ANSSI et les policiers nous ont demandé de ne pas aller plus loin.

Luc Dufresne : Nous avons tout transmis au service juridique.

Combien de temps avez-vous été impactés ensuite ?

Jérôme Guiho : Nous avons passé trois à quatre jours avec l'absence totale d'outils. Petit à petit, les outils bureautiques basiques ont été rétablis puis les logiciels métiers. Nous en avions identifié près de 200 dans la collectivité. Les services se sont d'abord occupés des plus urgents, notamment tout ce qui concernait la paye, les finances, les RH. Nous étions alors en pleine période de paye pour 4000 agents, vous pouvez imaginer un peu les conséquences, donc ça c'était vraiment des sujets prioritaires.

Cela a pris plusieurs mois pour remédier et remettre en place l'ensemble des logiciels métiers. L'ANSSI nous avait dit qu'il nous fallait deux ans pour nous remettre de cet incident et reconstruire un système qui soit véritablement robuste et à l'identique en termes de Fonctionnalités, et effectivement, cela a pris deux ans.

Luc Dufresne : Le message qu'on a eu, c'était « deux semaines très difficiles ». Il nous a fallu un peu plus d'une semaine pour remonter la messagerie par exemple, deux à trois mois après pour obtenir un système d'information minimal avec vraiment les grosses fonctions régaliennes, RH, finance, etc. et puis après bien deux ans de sécurisation, de travaux de sécurisation complémentaires.

Jérôme Guiho : Ça a été très impactant pour la Direction du Système d'Information et du Numérique (DSIN). L'épisode a été assez long et assez lourd à gérer pour ses agents.

Quel a été l'impact sur les administrés d'Angers ?

Jérôme Guiho : Très limité, même si nous sommes revenus à des modes de fonctionnement un peu rudimentaires. La première décision a été d'ouvrir l'hôtel de ville aux usagers dès le lundi matin. Nous avons fonctionné en mode dégradé mais les rendez-vous se sont tenus, les actes de naissance ont été rédigés à la main, les mariages aussi.

Quelles ont été les décisions au lendemain de la cyberattaque ?

Jérôme Guiho : Du jour au lendemain, la cybersécurité, jusque là sujet technique, est devenue un sujet stratégique, un enjeu majeur impliquant toute la direction générale de la ville dans la gestion quotidienne.
En termes de gouvernance, tous les trois mois, nous avons un comité stratégique autour des questions numériques et il y a toujours un volet cybersécurité. Ensuite, C'est un point de sensibilisation permanent, que ce soit auprès des directeurs ou auprès de nos agents.

Les 3 000 collaborateurs municipaux et de l'agglomération connectés sont régulièrement formés et entrainés lors de simulations d'attaque, à l'aide de (faux) messages trompeurs par exemple, les télétravailleurs suivent une formation obligatoire avant d'être autorisés à travailler à distance. Les SI d'Angers sont surveillés 24h/24 par un SOC nantais. Ce qui permet à la collectivité de traiter plus d'une vingtaine d'incidents de cybersécurité par mois, illustrant la réalité permanente de la menace cyber.

A combien sont évalués les impacts financiers ?

Jérôme Guiho : Je ne pourrais pas vous dire mais ce sont des grosses sommes, vraiment de très grosses sommes. Je vais vous donner un exemple : sur le volet territoire intelligent, nous avons installé ce qu'on appelle un WAF, qui est un gros firewall pour ce projet de territoire intelligent. On est sur des outils à 600 000 €.

Ensuite, tous les ans, la maquette budgétaire maintenant intègre ce volet cybersécurité. C'est coûteux mais indispensable.

Luc Dufresne : Ce qui est intéressant, c'est de parler en pourcentage du budget informatique. L'ANSSI préconise qu'il faudrait être entre 5 à 10 % du budget informatique consacré à la sécurité. Nous en étions loin en 2021. Aujourd'hui, on s'en rapproche.

Comment avez-vous échelonné la mise en œuvre d'outils de cyber protection ?

Luc Dufresne : On avait commencé à travailler avant la cyberattaque. J'ai pris mes fonctions de RSSI en 2020, un an avant la crise. L'idée était de travailler de manière cohérente, faire un état des lieux de la cartographie des risques, mettre en place une politique accompagnée d'un plan d'action. On a commencé à dérouler, malheureusement on s'est fait attaquer trop tôt.

Suite à la cyberattaque, la première chose était de comprendre comment on avait été attaqué, quel avait été le chemin utilisé pour rompre notre système. Nous avons ensuite réorganisé le plan d'action pour venir corriger les grosses failles utilisées tout de suite.

Le plan d'action peut être découpé en quatre types d'actions.
Il y a les actions de gouvernance, qu'évoquait Jérôme Guiho ; des actions de protection : mettre en place des « parpaings », des barbelés, tout ce qu'on imagine derrière la sécurité informatique, les aspects vraiment techniques.

Après la défense, il y a la surveillance de ce qui se passe chez nous, on va traiter les incidents et puis après aussi préparer la crise avec la résilience, avec de la sensibilisation et de la formation.

De la même manière, nous commençons à être moins dans les conséquences de l'attaque, nous allons aussi devoir travailler à la préparation de la prochaine crise éventuelle. On va commencer à faire des exercices de gestion de crise, de procéder, formaliser notre gestion de crise.

On imagine que vos 3 000 agents connectés sont ultra-vigilants…

Jerôme Guiho : En tout cas, on fait en sorte qu'ils le soient ! Pour vous donner un exemple, les télétravailleurs sont assujettis à une formation obligatoire sur le volet cybersécurité avant de pouvoir faire du télétravail. On est très rigoureux là-dessus. Mais vous savez, on est très humbles.

Luc Dufresne : Nous avons 3000 personnes qui travaillent, peut-être qu'il y en aura 2 999 qui seront parfaits. Il suffit d'une seule personne…
On considère qu'il peut y avoir quelqu'un qui fait une erreur et c'est pour ça que nous on va parler de défense en profondeur. On sensibilise l'utilisateur mais on met aussi d'autres protections derrière. Un peu comme un mode d'aéroport.

C'est-à-dire ?

Luc Dufresne : Avant de rentrer dans un avion, on a été scanné deux ou trois fois. D'un point de vue sécurité. On a plusieurs barrières pour retarder l'attaquant, pour le détecter et pour se défendre et le mettre dehors si jamais il rentre.

Quel SOC utilisez-vous aujourd'hui ?

Luc Dufresne : Nous faisons appel à un prestataire, n'étant pas assez nombreux pour surveiller 24h sur 24. Il s'agit d'une société privée de Nantes. Ils nous alertent quand ils détectent des signaux inquiétants. Nous poursuivons l'investigation nous-mêmes.

Nous traitons plus de 20 incidents de sécurité chaque mois, qui sont des faux positifs, des fausses alertes ou qui relèvent de mauvais usages…

Cette cyberattaque a-t 'elle eut un impact sur le territoire intelligent ?

Jérôme Guiho : Non, aucun, si ce n'est qu'on a là aussi renforcé le volet sécurité au sein du projet, à l'image de ce qui s'est fait et de ce qui s'est déployé au sein de la collectivité.

Le territoire intelligent est un projet parmi d'autres, on déploie un certain nombre de projets avec des outils numériques donc celui-ci en est un, mais c'est loin d'être le seul.

Luc Dufresne : C'était quand même une motivation pour créer, à l'époque, le poste de RSSI que j'occupe. La collectivité a anticipé ce besoin de sécurité, notamment pour ce type de projet qui concerne le territoire.

Dernière question : le budget dédié à la cybersécurité est stable depuis la cyberattaque. Va-t-il être augmenté ?

Jerôme Guiho : La somme varie chaque année, en fonction des projets, de la capacité, de la dimension du projet et de la capacité des agents de la DSIN notamment à porter ce projet. Nous sommes à leur écoute.

Luc Dufresne : Si j'avais un budget illimité, je serais incapable de le dépenser. Ce n'est pas moi qui sécurise le système d'information mais ce sont mes collègues qui font du réseau, du système.

L'idée c'est surtout de convaincre tout le monde de prendre son rôle dans la sécurité via la gouvernance, de l'élu, du maire président jusqu'à l'agent de l'autre côté de la pyramide, chacun a un rôle à jouer.

Jerôme Guiho : C'est une question d'acculturation, de maturité, de Formation aussi pour certains.

Luc Dufresne : C'est comme de la sécurité au travail, c'est comme de la sécurité routière, c'est comme tout.

Jerôme Guiho : Ce n'est pas quelque chose qu'on a envie de faire de manière native. C'est un peu à l'image de la protection des données. On a mis en place une culture interne autour de la protection des données qui aujourd'hui porte totalement ses fruits.

Parution le 17 octobre 2025

Le Data Act, l'éléphant dans le couloir

SEBASTIEN VIOU
Stratège Cybersécurité
Fortinet

Adopté officiellement en janvier 2024 et applicable à partir du 12 septembre 2025, le Data Act est présenté comme la grande réforme européenne nécessaire à la construction d'un marché unique de la donnée. Son objectif est clair : faciliter l'accès, la portabilité et l'utilisation des données générées par les utilisateurs de produits et services numériques, qu'il s'agisse d'objets connectés, de services cloud, ou de plateformes SaaS. En théorie, tout le monde devrait se réjouir : plus d'innovation, moins de dépendance, plus de concurrence. En pratique, le Data Act avance dans un silence assourdissant, éclipsé par NIS2 qui, dans les médias et les conférences, rafle toute l'attention. Pourtant, ce texte pourrait avoir des conséquences plus lourdes encore sur le quotidien des entreprises. Et à ce rythme, il faut le dire franchement : personne ne sera prêt.

Objectif : ouvrir le marché Européen du Cloud

Pour rappel, le Data Act impose que les données générées par un produit ou un service soient accessibles à son utilisateur et transférables vers un tiers de son choix. Conséquence directe : l'ère des écosystèmes fermés touche à sa fin. Prenons l'exemple d'une entreprise qui utilise des machines industrielles connectées : les données de performance ne pourront plus être verrouillées par le fabricant, elles devront être mises à disposition de l'entreprise utilisatrice et de tout prestataire tiers désigné. Même logique pour un particulier qui possède une voiture connectée : les données ne

pourront plus être exclusivement réservées au constructeur, elles devront pouvoir être partagées avec un garagiste indépendant. Sur le papier, c'est une révolution. Mais combien d'acteurs sont techniquement prêts à fournir cette interopérabilité de manière sécurisée et documentée ?

Un impact sur l'ensemble des contrats

D'autant que le Data Act ne se limite pas à la technique. Il impose une véritable révolution contractuelle. Les clauses interdisant ou limitant l'accès et la portabilité des données deviennent clairement abusives, et même illégales. Les fournisseurs devront revoir leurs contrats de service en profondeur. Par exemple, un éditeur SaaS ne pourra plus imposer des frais prohibitifs pour exporter les données d'un client. De même, un fournisseur cloud ne pourra plus insérer dans ses CGU des clauses rendant la migration impossible ou dont le coût serait à définir au moment de réaliser l'action. Les juristes d'entreprise et les directions achats vont devoir se retrousser les manches pour réécrire leurs contrats. Et une fois le contrat rédigé, ce texte devient une gigantesque source de potentiels litiges, que le monde juridique se fera un plaisir de traiter.

Le tout, dans le respect de l'état de l'art Cybersécurité

Et puisque l'on parle de contractuel, il va de soi que partage et portabilité ne signifient pas abandon de la sécurité. Le Data Act insiste : les données doivent circuler en toute confiance. Cela implique chiffrement systématique, contrôle d'accès granulaire, journalisation exhaustive et traçabilité. Imaginez une entreprise de santé qui souhaite transférer ses données patients d'un cloud vers un autre : le fournisseur sera obligé de garantir un transfert chiffré de bout en bout, avec un suivi détaillé des accès. Même chose dans l'industrie aéronautique : si un sous-traitant transfère des données de maintenance, il devra démontrer que ces données sont protégées à chaque étape.

Et avec le maximum de simplicité

Que l'on se rassure cependant, le transfert est simple. Ou plutôt, il le sera forcément. Pourquoi ? Parce que le Data Act l'exige. Comment ? Avec l'utilisation d'API standard et documentées. Oubliez les formats propriétaires conçus pour dissuader les clients de migrer. Désormais, un fournisseur devra mettre en place des interfaces claires, normalisées et publiques. Prenons l'exemple d'une solution de gestion RH en SaaS : les données des salariés devront pouvoir être extraites via des API lisibles par des tiers, pas seulement par l'éditeur d'origine. Même contrainte pour un constructeur de capteurs IoT industriels : les données de télémétrie devront être accessibles par des standards ouverts. L'impact est colossal : cela implique de revoir les architectures techniques, de développer des passerelles fiables et d'investir dans l'interopérabilité. Un travail considérable qui, même s'il est aidé par de nombreux langages standardisé (REST API, JSON), reste largement sous-estimé.

Dans un délai acceptable et encadré

Pour finir sur le terrain des mesures applicables, la cerise sur le gâteau, le Data Act ne se contente pas de définir des principes : il impose des délais d'application stricts. Un client qui souhaite changer de fournisseur ne pourra pas être retenu captif indéfiniment. Le texte fixe deux contraintes claires : un préavis maximum de deux mois et un transfert des données devant être achevé en moins de trente jours. Prenons un exemple concret : une entreprise qui souhaite migrer d'un fournisseur cloud A vers un acteur G devra pouvoir le faire en respectant ce calendrier. Le fournisseur sortant n'aura pas le droit de ralentir volontairement le processus ou de facturer des frais excessifs. Dans l'absolu, c'est une bonne nouvelle pour les clients. Mais dans la réalité, combien d'opérateurs cloud sont capables de garantir un transfert complet, sécurisé et opérationnel en 30 jours ? Très peu. Et encore moins de clients ont anticipé ces obligations pour l'inclure dans leur gouvernance IT.

Avec des conséquences business et industrielles fortes

On le sent à travers ces paragraphes, les conséquences pour les entreprises sont importantes, surtout que le Data Act ne concerne pas uniquement les géants du cloud. Il touche aussi les PME, les startups et les industriels. Et ce quelque soit le pays d'origine de l'entreprise, à partir du moment où elle commercialise un produit au sein de l'Union Européenne. Un fabricant d'objets connectés devra revoir sa stratégie de données, un éditeur SaaS devra repenser son modèle économique, un prestataire de service SOC devra anticiper la traçabilité de ses échanges de données. A court terme, cela représente un coût de mise en conformité considérable : adaptation des systèmes, mise à jour des contrats, formation des équipes. A long terme, c'est un changement complet de paradigme : l'économie de la donnée ne sera plus fermée, mais ouverte et transparente.

En conclusion : serez-vous prêt ?

Pour conclure, le Data Act est, en théorie, une avancée majeure pour l'économie numérique européenne. En pratique, il est invisible dans le débat public, éclipsé par NIS2 et le CRA. Or, entre l'ouverture des données, la mise à jour contractuelle, l'adoption d'API standard et le respect des délais de migration, les défis sont immenses. Et soyons honnêtes : à ce rythme, la majorité des entreprises concernées ne seront pas prêtes en septembre 2025. Le Data Act avance dans l'ombre, mais son impact n'en sera que plus brutal. Et cette fois, il ne suffira pas de lancer un plan d'action improvisé pour éviter les sanctions : la révolution des données est en marche, et elle ne laissera personne intact.
Il est très probable que ce dernier paragraphe vous ai interpelé, car oui, Septembre 2025, c'était bien il y a 2 mois…

Parution le 24 octobre 2025

La cybersécurité : un socle pour les territoires intelligents

DENIS HAMEAU
Adjoint à la maire, délégué Qualité du service public,
Relation aux usagers et innovation - Dijon
Conseiller délégué Smart City, On Dijon,
enseignement supérieur, université - Dijon Métropole

Comment est né ON DIJON, cette initiative pionnière dans le pilotage de l'espace public ?

Le projet ON DIJON est né il y a une décennie d'une double nécessité : assurer le pilotage intelligent de l'espace public, et répondre à un enjeu économique autour de la filière numérique dont on souhaitait qu'elle se structure sur le territoire, développer des compétences, et ce dans une logique d'attractivité du territoire. Au-delà du projet centré sur la ville, nous avons souhaité intégrer les 23 collectivités de la Métropole qui faisaient face aux mêmes enjeux, sans disposer ni des ressources humaines ni des compétences pour adresser les sujets en lien avec le numérique, la cybersécurité pour y répondre efficacement. D'où l'idée d'un projet mutualisé à l'échelle métropolitaine.

En parallèle s'est opérée une mutualisation progressive des services numériques dans les collectivités au niveau de la Métropole avec une logique d'acquisition et de développement des compétences y compris sur le domaine de la cybersécurité.

L'objectif de notre démarche était clair : mutualiser les compétences et rationaliser les coûts pour offrir des services adaptés aux citoyens et optimiser la gestion de l'espace public.

Quelle a été la méthode mise en place pour structurer ce projet aussi ambitieux ?

Pour construire ce type de projets les process sont fondamentaux. Un accompagnement politique et administratif doit être conduit en parallèle et se rejoindre. ON DIJON est un projet transversal, porté par la direction générale des services (DGS). Dès le départ, les agents ont été associés.

Un groupe projet a réuni RH, direction du numérique, agents de terrain, DGST, élus référents – notamment en voirie – et le président de la Métropole. Nous avons mis en place un dialogue compétitif autour d'un appel d'offre spécifique car ce que nous inventions n'existait pas encore sur le marché. L'enjeu était aussi de soutenabilité financière sur le long terme – 105 millions d'euros sur douze ans via un contrat CREM. Quatre grands groupes ont répondu, avec des expertises variées en infrastructure, cybersécurité, IA, et déploiement applicatif. Le volet cybersécurité a été déterminant dans l'évaluation des offres.

Quels résultats concrets ont été obtenus depuis 2018 ?

Aujourd'hui, nous pilotons l'éclairage public, la vidéoprotection, la voirie, en lien étroit avec les agents de terrain. Côté RH, un travail a été mené pour diagnostiquer les compétences numériques service par service, dans une logique de conduite du changement.

La période du COVID a été un véritable crash test pour le dispositif qui a montré toute sa capacité à favoriser le dialogue en cas de crise.
Nous avons également développé une application métropolitaine qui offre

plusieurs services aux citoyens – comme le paiement de la cantine, la réservation de livres ou de films à la médiathèque… – et qui lui permet aussi de signaler en temps réel les problèmes dans l'espace public. Ils deviennent acteurs de la gestion de la ville. Et cette interaction doit aussi se faire dans un cadre sécurisé.

ON DIJON a également permis de structurer un partenariat étroit avec l'Université de Bourgogne, devenue établissement public expérimental avec 12 établissements associés. L'IA y est un axe fort avec un pôle dédié, et nous avons insisté pour y intégrer également la cybersécurité.

Vous avez aussi ouvert la voie à l'open innovation. Comment cela s'est-il concrétisé ?

L'open innovation est au cœur de notre approche. Dès 2018, nous avons lancé des « data challenges » avec VivaTech pour valoriser nos données et favoriser le développement de start-up à travers nos cas d'usages. Premier champ d'application : la mobilité, pour améliorer le commerce de centre-ville ou l'expérience touristique.

Nous avons ainsi travaillé avec des start-up après sélection pour développer un « coach mobilité » qui propose des parcours optimisés, permettant aussi de mesurer l'impact carbone et l'impact sur la santé de vos déplacements. D'autres ont permis de mieux flécher nos investissements dans l'espace public, via l'identification des zones de départementales les plus dangereuses par l'analyse des données.

Et l'intelligence artificielle dans tout cela ?

L'IA était déjà présente dans le projet initial mais le contrat a été pensé pour permettre l'introduction progressive de nouvelles technologies, dont l'IA générative. Elle ouvre des perspectives, mais elle doit s'inscrire dans

un cadre éthique, transparent et compréhensible. Nous avons porté une attention particulière autour de l'éthique de la gestion de la donnée. Un comité métropolitain de la donnée a été créé en 2019-2020. Il vient de voter cette année une charte métropolitaine de la donnée qui s'impose à tous les délégataires.

L'objectif : créer de la valeur sans générer de défiance par les citoyens. D'où la nécessité d'expliquer pour favoriser l'adhésion. Et bien sûr de gérer les risques de tels développements. L'éthique, la transparence et l'explication sont essentielles pour maintenir la confiance des citoyens.

Comment la cybersécurité est-elle gérée au quotidien aujourd'hui ?

C'est notre socle depuis le départ. On ne se lance pas dans le monde des territoires intelligents sans cybersécurité. Notre système subit plus de 1000 attaques par jour. Un tableau de bord nous permet d'y faire face. Nous collaborons aussi avec des start-up, comme celle identifiée via la French Tech Réunion, qui propose des tests pédagogiques de résistance de nos systèmes : un exemple de la coopération qui peut se faire avec nos territoires d'outre-mer. La cybersécurité est vivante : elle évolue avec les menaces.

La direction du numérique travaille également à développer une culture cyber chez les agents, pour ne pas laisser de maillon faible. On ne peut pas protéger un système sans embarquer ses utilisateurs.

Demain, avec une potentielle relocalisation des industries, ou une évolution vers plus d'industries, il va falloir avoir être attractif et donc avoir les compétences localement. On n'est pas dans le prospectif, on est dans un élément d'attractivité fondamental du territoire : la cybersécurité est un socle et il faut qu'elle irrigue dans les différents systèmes parce

qu'elle est une condition de pérennité de nos systèmes et de notre capacité à agir. Aujourd'hui, le numérique et la cybersécurité ne sont pas encore intégrés dans les logiques économiques classiques. Il est urgent de changer cette vision. C'est aussi une question de souveraineté. D'où le projet sur lequel je travaille au niveau de la Région d'un véritable Campus Cyber construit autour des filières industrielles du territoire. Mais le modèle économique reste à trouver.

Quel regard portez-vous sur la directive européenne NIS 2 ?

Les collectivités doivent monter en maturité mais la cybersécurité ne se décrète pas. Elle se construit par l'adhésion. Il ne suffit pas d'imposer des normes : il faut accompagner les collectivités dans leur montée en compétences.

On pourrait imaginer un horizon de trois ans pour les grandes collectivités, pour atteindre un niveau permettant ensuite de mutualiser leur expertise et de favoriser leur environnement. Mais il faut donner les moyens.

Un dernier mot sur la résilience ?

C'est un enjeu central. Nos territoires doivent apprendre à gérer les crises de toutes sortes, y compris cyber. A l'image des territoires ultramarins, il nous faut développer une véritable culture de la résilience. Et donc de la cybersécurité.

Parution le 31 octobre 2025

De l'intelligence artificielle dans l'éducation

LAURANE RAIMONDO
Advisor
CyberCercle

Parmi les discussions qui fâchent autour de la table du repas de Noël, après la politique, vient le numérique, ses outils et désormais : l'« intelligence artificielle ». Tous auront un avis. De l'époque où seul l'avis du père comptait, aujourd'hui même la personne la moins informée du monde en a un. Or, hier comme aujourd'hui, les enfants écoutent, la plupart du temps, silencieusement. Mais hier, ils n'avaient pas entre les mains l'objet de ces controverses. Hier, il était socialement moins problématique d'interdire à un enfant de jouer avec un objet jugé contraire à son intérêt. Désormais, après des décennies de retard sur la formation de la société civile aux enjeux numériques – de la protection des données au cyberharcèlement en passant par les cyberarnaques et les graves problèmes d'addiction aux écrans –, il devient beaucoup plus compliqué d'aller contre cette masse devenue incompétente sans son prolongement technologique : le smartphone.

Les applications lui doivent leur réussite. Lui seul a permis de noyer le monde sous une avalanche de nouveaux « services » en ligne : il fait office de… tout. Les applications ont remplacé le téléphone fixe, les annonces météo, la carte routière, le journal du matin, la télévision, la radio, le courrier postal, les livres de cuisine, les coachs sportifs, les recommandations cinématographiques, les disques de musique, les professeurs, etc. La vie entière du plus grand nombre est désormais

rattachée à deux cents grammes de technologie non pas au fond de la poche mais dans le creux de la main.

« Il ne s'agit pas de savoir s'il faut utiliser l'IA, il s'agit de savoir ce que l'IA fait de nous, et ce qu'elle fera de nos enfants. »

Alors même que les premières inquiétudes révèlent enfin des études sérieuses liées à l'usage de ces outils par les plus jeunes, novembre 2022 est venu renverser à nouveau la table. ChatGPT était lancé. Il n'a pas fallu attendre trois mois pour voir apparaître les premiers travaux des élèves comme des étudiants, réalisés avec une « intelligence » qui n'était pas la leur. Le repas de Noël se transformera cette année en une arène où la discrète application d'« intelligence artificielle » sur le smartphone – qui ne devrait même pas être dans les mains d'un mineur – se fera toute petite. Et les enfants entendront soit une charge violente contre l'usage de l'IA, soit une allégorie de celle-ci, si merveilleuse qu'il ne faut pas s'en priver. Beaucoup essaieront de tempérer avec une demi-mesure, disant que désormais il n'est plus possible de passer outre et qu'il faut bien suivre le progrès technologique. Néanmoins, le fond de la question n'est toujours pas le bon. Il ne s'agit pas de savoir s'il faut utiliser l'IA, il s'agit de savoir ce que l'IA fait de nous, et ce qu'elle fera de nos enfants.

Dans beaucoup de foyers, la bagarre des devoirs est un souvenir désagréable ou une réalité qui l'est tout autant. Mais que demande l'instruction ? Un effort. Et c'est tout d'abord un effort d'attention, le premier et le plus fragile. Apprendre, c'est maintenir son attention sur une tâche exigeante malgré le plaisir de l'ennui qui appelle à grands cris, malgré la peur de l'échec ou la distraction qu'une simple mouche dans la pièce peut apporter. L'IA, en répondant instantanément, sans délai de réflexion ni frustration, sans peur de l'échec et en offrant la possibilité de se distraire pendant que la réponse jaillit, vient court-circuiter l'attention exécutive, autrement dit, bousille l'apprentissage de la patience.

« Une IA ne comprend pas, elle restitue. Elle mime la mémoire sans jamais la vivre. »

Mais pas seulement ! La mémoire, le noyau anthropologique du savoir, c'est ce que l'instruction cherche à former. Apprendre, ce n'est pas juste retenir sa leçon, c'est former la mémoire. Pas seulement celle de l'enfant, de l'étudiant, mais celle de la civilisation. Répéter, relire, reformuler, jusqu'à ce que le savoir s'enracine dans le temps, c'est inscrire dans la mémoire individuelle une trace du passé collectif, une continuité entre les générations. C'est ainsi que se transmettent les langues, les nombres, les récits et les symboles ; autrement dit, tout ce qui permet à une société de se penser elle-même ! Enseigner, ce beau métier si dévalorisé, est loin de seulement transmettre des contenus. Ça, l'IA peut le faire, un livre aussi. C'est assurer la continuité d'un monde. Chaque génération, en enseignant, et en apprenant ce qui est enseigné, réinterprète ce qu'elle a reçu, et c'est dans cet effort de réappropriation que naît la culture. Mais en introduisant dans ce processus si méconnu et précieux une « intelligence artificielle », on altère la nature même de la transmission. Lorsque l'Éducation nationale envisage d' « intégrer l'IA » comme un outil pédagogique légitime, c'est institutionnaliser la rupture dans la transmission. Une IA ne comprend pas, elle restitue. Elle reproduit des formes sans en porter la signification, elle mime la mémoire sans jamais la vivre, comme le font les enseignants : ils vivent leur métier – et s'ils pouvaient en vivre, ce serait bien aussi. Rédiger avec ChatGPT, c'est la fin de la mobilisation de sa propre mémoire du langage, de l'histoire et même de ses propres idées : c'est une interruption de la chaîne du sens. Soudainement, tout ce qui devait être intériorisé devient externalisé, et ce qui devait être compris devient simplement disponible. L'usage individuel ou ludique s'oublie : l'institution chargée de la mémoire commune reconnaît que la culture peut se transmettre sans conscience. Après tout, cela correspond aux objectifs d'économie dans l'Éducation. L'abonnement ChatGPT est moins onéreux qu'un salaire d'enseignant.

Fondamentalement, le danger guette autrement. Tandis qu'Édouard Geffray admet que « la situation de l'école est extrêmement inquiétante », celle-ci, censée être garante de la transmission du savoir, est sur le point de ne devenir plus qu'un lieu de circulation du contenu ; et ce que l'élève retient n'est plus ce qu'il a compris, mais ce que la machine a produit pour lui. On n'apprend plus le français : on consulte la langue. On ne découvre plus l'histoire : on en télécharge des fragments. La mémoire humaine n'est pas une base de données : elle est une architecture vivante, faite d'oublis nécessaires, de déformations fécondes et de liens affectifs. C'est cette plasticité qui nous fait humains : nous ne nous rappelons pas, nous nous racontons !

Cette perte de mémoire est comparable à une désactivation de la pensée. L'élève comme l'étudiant extrait de la mémoire des capacités qui lui permettent de remonter du concret à l'abstrait : il apprend à conceptualiser, à comprendre le monde au-delà de ce qu'il perçoit. Cet effort, fondateur de toute pensée rationnelle, passe nécessairement par l'erreur, la reformulation et la lenteur. Or, l'IA ne connaît pas cela : elle délivre les explications dénichées sur Internet, prêtes à consommer, elle produit des synthèses de surface et donne à comprendre sans faire comprendre. Encore un court-circuit, celui du passage obligé de l'incompréhension féconde, chemin par lequel se forment rigueur et pensée critique : l'aboutissement de la vie d'un étudiant. L'IA vient faire du jeune esprit en formation un être inconscient qui n'apprendra pas à douter, ne ressentira pas le heurt entre ce qu'il croyait savoir et ce qu'il a découvert, puisqu'elle lui aura donné des réponses, une « vérité » qu'il n'aura pas construite, une vérité sans conscience. Qu'elle était belle, cette image d'Épinal de l'étudiant torturé par ses doutes. Mais à force d'obtenir sans effort la bonne formulation, le chemin par lequel elle aurait normalement dû être trouvée disparaît. Et l'étudiant torturé avec. C'est dans ces tâtonnements, dans la réécriture d'un travail une dizaine de fois,

que l'on s'exerce finalement à la cohérence, la nuance et la contradiction. Réside ici un glissement redoutable : l'acte d'apprendre se transforme en acte de vérification. L'élève ne cherche plus, il valide ; il ne pense plus non plus, il compare. Hésiode écrivait que « les dieux ont placé la sueur au seuil de la vertu. » Il dirait que l'IA, en offrant la clarté sans la sueur, serait bien tout sauf vertueuse, en venant « éduquer » des esprits qui ne savent plus apprendre.

« Celui qui ne peut dire, agit. » - Françoise Dolto

Il va de soi qu'un esprit sans mémoire, ne sachant plus apprendre, ne sait pas non plus s'exprimer. Or, nous savons que les êtres qui ne savent pas s'exprimer deviennent violents. Oui, le déficit de langage est corrélé à l'agressivité. Françoise Dolto nous regarde du coin de l'œil et rappelle que verbaliser les émotions constitue un rempart contre l'agir impulsif : « Celui qui ne peut dire, agit. » Voilà un point bien peu développé lorsqu'est évoquée l'« intelligence artificielle » dans l'enseignement, et qui vaudra quelques inimitiés. Nul n'ignore que l'effort d'expression, c'est l'apprentissage de la maîtrise. Sans passer par la genèse intellectuelle du langage « grâce » à l'IA, l'élève, l'étudiant et même l'adulte parlent juste, mais pensent faux. Produire un simulacre de discours sans même en comprendre la logique interne, accepter la syntaxe sans recevoir la pensée, c'est se transformer en perroquet de salon incapable de répondre à l'insulte autrement que par le poing. Moucher son adversaire par le verbe plutôt que par le sang a beaucoup plus de classe. Une époque révolue. De là à penser que l'IA rendra notre monde encore plus violent, il n'y a qu'un pas. Franchi par les chiffres : 74 % des 18-25 ans reconnaissaient en 2024 avoir déjà utilisé l'IA pour rédiger un devoir ou un message professionnel et, surtout, près d'un tiers d'entre eux déclaraient « ne plus savoir formuler correctement leurs idées sans aide numérique ». L'ère numérique laissera-t-elle la place à l'ère des assistés du langage ?

L'illusion de l'IA dans la pédagogie ne relève pas d'un fantasme technophobe. Les chiffres parlent. Le rapport PISA 2022 relève une quinzaine de points en moins en mathématiques concernant les élèves utilisant fréquemment les outils numériques à l'école par rapport à ceux qui les utilisent peu. Quant à la baisse de la compréhension en lecture, elle touche la quasi-totalité des pays membres. Même l'Éducation nationale, à travers son étude sur les compétences fondamentales en 2023, montre qu'à la fin du primaire, près d'un élève sur trois a des difficultés à lire un texte simple à voix haute ! Sur la production écrite, c'est l'effondrement : faible vocabulaire, syntaxe bringuebalante et phrases limitées. Petit cadeau complémentaire : l'INSERM et l'Université Paris-Cité notent en 2022 une chute de 20 % des performances attentionnelles chez les adolescents exposés plus de trois heures par jour aux écrans. Et là, c'est une étude d'Ipsos avec Bayard/Milan et Unique Heritage Media qui a calculé que le temps passé devant les écrans des 13-19 ans est désormais de… 5 h 10 par jour.

Cette suite de chiffres peu digeste illustre un déclin qui n'est pas seulement moral ou culturel, mais qui est mesurable. L'« intelligence artificielle » est un artifice ! Remplacer l'apprentissage par la consommation, l'effort par la rapidité, la construction du sens par l'exigence de résultats, c'est perdre l'espace même où se forme l'intelligence, en croyant « gagner du temps ». Finalement, la réponse ne se trouvait ni dans la diabolisation, ni dans la glorification, et toujours pas dans la demi-mesure. Les outils numériques ne sont que des outils, et doivent le rester. Rien n'est inéluctable, pour peu que le réveil ne soit pas trop tardif, un peu à l'image de la sécurité numérique. La réponse réside en un choix : celui que nous ferons tous, en tant que professionnels ; en tant qu'individus ; en tant que parents. Nulle institution n'a à forcer la main sur l'usage d'un outil qu'elle ne maîtrise pas et qui est susceptible de détruire l'avenir même de la société. Cette technologie qu'est l'« intelligence artificielle » générative est ce que nous en ferons. Sauf à la laisser nous transformer.

Aussi, comme tout bon pédiatre déconseillera l'usage d'objets donnant à un bébé les compétences qu'il n'a pas, tel un trotteur, un bon professionnel conseillera de commencer par acquérir – et préserver – la compétence avant de la déléguer. L'usage de l'IA, comme de tout outil numérique d'ailleurs, doit être cloisonné, hiérarchisé et conditionné à la maturité cognitive de l'usager. Avant un certain âge, une certaine instruction, on ne possède ni la mémoire, ni la distance critique pour interroger une machine, et encore moins les compétences intellectuelles pour en corriger les erreurs. L'instruction du XXIe siècle ne doit pas être « connectée », elle doit choisir si, quand et pourquoi elle se connecte. C'est le choix d'une pédagogie du discernement.

« L'instruction du XXIe siècle doit choisir si, quand et pourquoi elle se connecte. C'est le choix d'une pédagogie du discernement. »

Par là, il faut entendre que la responsabilité ne pèse pas que sur le corps professoral, mais aussi sur les épaules des parents, à qui l'État doit apprendre à faire à nouveau confiance, mais également sur les siennes, lui seul étant capable de frapper le marteau de l'interdiction ferme dans les lieux d'instruction. Ces lieux, qu'ils soient publics, privés ou familiaux, doivent comprendre l'urgence d'enseigner le numérique sans en dépendre, c'est-à-dire sans écran. Il est parfaitement possible de former les jeunes esprits à comprendre les principes d'un algorithme, d'un modèle de langage, d'un biais cognitif ou statistique par le jeu, par la logique, par la discussion. Les principes fondamentaux du numérique peuvent s'apprendre par analogie et par simulation, sans exposition aux écrans. C'est même ainsi que l'on développe une véritable culture numérique critique, affranchie de la fascination technologique. En d'autres termes : le numérique n'a pas besoin d'écran pour être compris, pas plus que la

littérature n'a besoin de tablette pour être aimée.

Réapprendre à cloisonner, temporiser, interdire, ce n'est pas revenir en arrière : c'est retrouver la mesure humaine du progrès. La pédagogie doit redevenir un espace de maturation, pas de performance. On ne forme pas un citoyen libre avec des outils qui pensent à sa place.

Si l'intelligence artificielle peut être un outil d'émancipation, elle ne le deviendra qu'en restant un… outil. L'instruction, elle, doit rester le lieu où l'on apprend à s'en passer. L'avenir n'appartient pas aux machines qui calculent, mais aux peuples qui se souviennent.

Parution le 7 novembre 2025

Métropole du Grand Paris : un programme ambitieux de cybersécurité pour ses communes

GEOFFROY BOULARD
Vice-Président délégué à la Communication à l'Innovation et au Numérique
Métropole du Grand Paris

Depuis février 2025, la Métropole propose aux communes volontaires de son territoire un programme d'accompagnement « clé en main », 100% gratuit. Le succès est au rendez-vous : les objectifs initiaux ont été dépassés en trois semaines. Le point avec Geoffroy BOULARD, Vice-Président délégué à la Communication, à l'Innovation et au Numérique de la Métropole du Grand Paris.

Le 7 février 2025, la métropole a lancé, depuis et avec le Campus Cyber, un programme ambitieux de cybersécurité pour les communes du Grand Paris.

De quoi s'agit-il ?

Ce programme est conduit dans le cadre du dispositif CYBIAH, acronyme de « Cybersécurité et Intelligence Artificielle Hub ». Ce consortium rassemblant dix partenaires est co-financé par l'Union européenne (environ 100 000 euros annuels). La Région Ile-de-France se concentre sur les TPE/PME et la Métropole se consacre aux 130 communes du territoire.

L'objectif à terme est d'accompagner toutes ces communes, au rythme d'une quarantaine chaque année. Initialement, 30 municipalités se sont inscrites dès le lancement du programme, en février 2025.

Ce fut immédiatement un succès : devant le nombre de communes s'inscrivant en liste d'attente, le bureau métropolitain a voté, en juin dernier, une extension du programme pour dix communes supplémentaires, identifiées comme les plus vulnérables. Elles ont intégré le programme en septembre. Et une vingtaine de municipalités sont déjà sur liste d'attente pour 2026.

Comment expliquez-vous cet engouement ?

Si on dresse un bilan rapide, je peux dire que les communes sont très satisfaites de manière générale, pour les quelques restitutions auxquelles j'ai pu assister. Cette restitution est très opérationnelle donc ça leur donne un plan avec des axes d'amélioration concrets.

Nos experts donnent vraiment des points aussi bien organisationnels que documentaires avec de la gouvernance, ou parfois même très techniquess. Nous leur avons demandé de fournir une liste avec un ordre de priorité et d'identifier les points les plus vulnérables pour les communes.

L'enjeu est donc si grand ?

Oui.
D'après les baromètres de Cybermalveillance.gouv.fr, une commune sur dix a été attaquée en 2023. L'hameçonnage représente 35% des attaques. Elles ont un impact concret sur les services publics numériques et entraînent un coût humain important pour la reconstruction post-attaque, comme illustré par l'exemple de la mairie de Bondy (ndlr : cyberattaquée en novembre 2020).

Face à l'augmentation des cyberattaques, le programme porté par la Métropole est une démarche proactive de protection des services publics locaux. C'est un peu une première, en France, cet accompagnement très actif, qui va au-delà du diagnostic jusqu'au financement d'actions.

D'ailleurs, je plaide pour un grand plan cyber à l'échelle nationale, calqué sur celui de la Métropole du Grand Paris.

Comment s'articule ce programme ?

CYBIAH se décompose en trois phases : diagnostic de maturité cyber, élaboration d'un plan d'action adapté puis cofinancement de solutions. Le programme dure trois ans. C'est là que le Fonds « Innover dans la Ville » de la Métropole du Grand Paris intervient pour soutenir la mise en place de leur plan de sécurisation avec une prise en charge de 50 % du coût du projet dans la limite d'un plafond de 200 000 €. Le budget de ce fonds est en augmentation pour répondre à la demande croissante des communes.

L'an prochain, vous aurez 40 communes en accompagnement. Comment organisez-vous le financement avec cette augmentation ?

Sur cette année, nous avons des limites budgétaires. Vous n'êtes pas sans savoir que la loi de finances va avoir des impacts aussi sur les communes. Mais sur ces sujets là, on est plutôt sur des budgets qui sont sanctuarisés, voire plutôt en hausse et je m'en félicite.

L'idée est de poursuivre. Évidemment, en 2026, il y a des élections municipales, donc il y aura un renouvellement aussi du Conseil métropolitain. CYBIAH fait partie des programmes permanents de la métropole et donc il y aura une continuité de l'action.

Nous avons mis du temps au départ pour trouver le bon programme car nous souhaitions nous coordonner avec plusieurs acteurs, notamment la Région Ile-de-France. La métropole a l'ambition de poursuivre pour toucher toutes les communes à terme, en fonction de la criticité aussi évidemment de leur système L'idée n'est pas non plus d'imposer.

Que prévoit la métropole pour l'arrivée des règlementations européennes ?

La métropole étudie l'impact sur les communes concernées selon le seuil d'habitants défini et alerte sur les conséquences financières et budgétaires. Des ateliers spécifiques sont également organisés en vue de la mise en œuvre de la réglementation NIS 2 pour les communes de plus de 30 000 habitants. Le but est d'accompagner les communes faces aux exigences européennes.

Mais bien sûr, notre action est en complément de celle de l'État, qui doit garder son rôle protecteur et régalien.

Parution le 14 novembre 2025

Les données de santé des animaux d'élevage face au risque cyber

PASCALINE BOSSARD
Experte cybersécurité
Life science

Un secteur hautement stratégique mais non abordé en termes de cybersécurité et de protection des données.

Si la sécurité des données de santé humaines est un sujet fortement évoqué et traité, le pendant chez les animaux d'élevage est un domaine quasiment inconnu du grand public. Les enjeux sont certes différents mais les deux sont pourtant étroitement liés : 70 % des maladies infectieuses humaines ont une origine animale (source OMSA).

En France, les animaux d'élevage (dit de rente) font l'objet d'un suivi sanitaire strict, coordonné par la filière du diagnostic vétérinaire.

Il est un maillon essentiel de la santé publique et de la souveraineté alimentaire. La notion de sécurité alimentaire peut être représentée par le concept « from farm to fork », de la ferme à la fourchette. Le diagnostic vétérinaire est le maillon de la chaine qui fait le lien entre l'agriculture et l'agroalimentaire, garant par les analyses réalisées au quotidien de la qualité du lait ou de la viande qui sortent des élevages pour être transformés avant d'être consommés. Soumis à l'instabilité géo politique mondiale, à des contraintes environnementales de plus en plus importantes, à des besoins de traçabilité toujours plus poussés…son environnement est en constante

évolution, avec un facteur d'accélération ces dernières années.

Les analyses réalisées servent des objectifs économiques, sanitaires et réputationnels sur les marchés.

Chaque jour, des milliers de données relatives à la santé des animaux ou à la production de lait sont générées pour permettre à la filière de fonctionner efficacement, et ce depuis de nombreuses années. A titre d'exemple, le secteur laitier représente à lui seul 120 millions d'analyses chaque année[1]. On peut parler de big data. Ces données sont indispensables au quotidien pour les différents intervenants de la filière. La dépendance accrue aux systèmes numériques expose le secteur à des risques de cybersécurité. Cela nécessite une réelle compréhension des enjeux cyber afin de préparer sa protection de manière adaptée en tenant compte des menaces spécifiques à ce secteur.

Comme pour les données de santé humaine, les données de santé animale sont riches, stratégiques et sensibles. Leur compromission entraîne des risques majeurs.

Risque sanitaire : un blocage des systèmes de suivi de troupeau peut fausser un diagnostic, retarder la détection des maladies ou compromettre la gestion des traitements.

Risque économique : la perte de traçabilité – qu'il s'agisse de données de troupeau ou d'archives de filière – ou l'indisponibilité d'outils essentiels au diagnostic peut provoquer l'arrêt brutal d'une activité et générer des pertes considérables.

Risque de réputation : avec la sensibilité connue du grand public sur les sujets sanitaires, une fuite de données sensibles ou une campagne de désinformation peuvent altérer la confiance des consommateurs et nuire aux filières.

Quel est le niveau de maturité face aux risques et menaces encourus ?

Au-delà des attaques d'opportunités pour des raisons financières avec demande de paiement de rançons, nombre d'acteurs malveillants peuvent avoir des intérêts dans la déstabilisation de la filière, qu'il s'agisse d'hacktivistes/activistes ou d'acteurs étatiques. En France, l'élevage est un secteur économique important. La France est le 6ème exportateur mondial de produits agricoles et agroalimentaires. Au niveau Européen, la France est un des leaders sur le marché : premier pour la production de viande bovine, second en tant que producteur laitier ; elle détient le 3ème cheptel porcin. Ce qui en fait un acteur clé pour le pays, mais aussi la communauté européenne et donc une cible pour les entreprises ou états concurrents.

Des menaces spécifiques au secteur pèsent sur la disponibilité des données, leur intégrité, leur confidentialité et leur traçabilité avec des impacts plus ou moins importants. Cela est amplifié par l'utilisation d'outils métiers dont certains ne sont pas au standard de sécurité attendu. L'arrivée des objets connectés dans les élevages est aussi un facteur à prendre en compte dans le développement de la surface d'attaque.

Non soumis à des réglementations fortes et contraignantes (non inclus dans NIS1, non considéré comme organisme d'importance vitale, hors cadre du RGPD…), la maturité globale du secteur n'est pas au niveau pour faire face aux menaces et risques identifiés. Il y a une sous-estimation de ces derniers, avec une méconnaissance de l'importance de la valeur des données produites ou utilisées. Pourtant les attaques d'origine cyber sont déjà une réalité dans le secteur, en France et à l'étranger, ce qui tend à introduire le sujet mais de manière encore très timide. Nous pouvons ici illustrer les propos avec la cyberattaque subit par une coopérative agricole impactant près de 30 000 éleveurs dans 22 départements français en décembre 2024 [2].

Le niveau de maturité est très différent selon les structures. De manière générale, il est assez faible au regards des enjeux. Contrairement à ce qui peut exister dans d'autres secteurs d'activités, il n'y a pas de coordination sur la cyber défense dans le secteur du diagnostic vétérinaire.

Combler les vulnérabilités pour réduire les risques.

Des actions sont à entreprendre du niveau le plus local à celui de l'état pour une montée en compétences de tous les acteurs. La modernisation des outils obsolètes (notamment étatique) est indispensable ou à minima, les isoler quand cela est possible. Toutes les technologies qui permettraient de sécuriser la filière existent sur le marché. Mais pour pouvoir installer les systèmes nécessaires de manière efficace, il faudra revoir les processus, notamment l'ultra segmentation des bases de données.

Une réelle prise de conscience est nécessaire par tous les acteurs afin de pouvoir faire progresser l'existant. Une sensibilisation à tous les niveaux semble indispensable afin de créer une réelle culture de la protection des données produites et échangées. La compréhension des enjeux et des besoins sera alors la meilleure des préventions. Contrairement à d'autres secteurs déjà imprégnés par la notion de cyber sécurité, par le bais de la formation ou de la réglementation, le secteur vétérinaire dans son ensemble n'aborde pas ou peu ces sujets. Par exemple, il n'y aucune formation sur la sécurité des données ou la partie juridique liés aux données dans les écoles vétérinaires ou les cursus scientifiques.

Le changement ne pourra se faire sans une gouvernance forte permettant de regrouper les acteurs autour des problématiques de sécurité des données. Le maillage actuel rend complexe la montée en compétence globale. La posture individuelle ne sera pas suffisante pour protéger toute la chaine. Placer l'intérêt commun au-dessus sera un levier indispensable pour aligner toute la filière sur des standards, comme cela a pu être fait

dans la santé humaine par exemple. De l'union viendra la force, au sein de chaque métier d'abord puis au sein de l'éco système.

L'évolution du cadre réglementaire, notamment avec la transposition de NIS2 et du data act en 2025 devrait assoir des règles pour une partie des acteurs. Une réelle compréhension de ce cadre et surtout son application vont imposer la mise en place d'un certain nombre de processus accentuant la protection des données.

Quel avenir ?

L'exploitation des données produites par le diagnostic vétérinaire serait bénéfique à la fois pour l'efficacité de la surveillance sanitaire et pour la protection des nouvelles infrastructures. Un environnement où les données sont non seulement disponibles, intègres, mais aussi mieux sécurisées est indispensable. L'arrivée de l'IA avec des modèles permettant de réaliser des diagnostics en amont des analyses est déjà en train de s'établir ce qui va complexifier le système actuel.

Sécuriser la filière est une priorité avant que les données ne soient en dehors des organismes actuels et donc en dehors de leur contrôle.

Parution le 21 novembre 2025

[1] Rapport annuel d'activité du CNIEL - 2023
[2] « Ils nous ont contactés via une messagerie cryptée pour obtenir une rançon : cette cyberattaque rend la vie impossible aux éleveurs », France Info, 2 janvier 2025

L'Intelligence Artificielle dans la guerre de l'information : vers la lutte informationnelle algorithmique

COLONEL BERTRAND BOYER
Chef de corps
Centre interarmées des actions sur l'environnement (CIAE)

Il est 1h52 dans la nuit du 28 août 2023, lorsque qu'une attaque informationnelle contre les armées françaises est lancée sur les réseaux sociaux. Cette action prend la forme d'un faux document de 12 pages, présenté comme une « fuite » et détaillant les préparatifs d'une prétendue opération militaire française contre la junte nigérienne. L'objectif de cette manipulation : attiser le sentiment antifrançais au Sahel, dans un climat tendu après le coup d'État du 26 juillet. Cette opération grossière est rapidement détectée et ses effets sont limités, mais qu'en serait-il si nos adversaires avaient eu recours massivement à des outils d'intelligence artificielle ? Et si la diffusion de ce faux avait été propulsée artificiellement en s'appuyant sur l'exploitation algorithmique des biais des auditoires cibles ?

De la guerre de l'information à la guerre cognitive

Depuis 2022 et l'introduction de l'influence au rang de sixième fonction stratégique dans La Revue nationale stratégique, les autorités françaises structurent un domaine qui évolue plus vite que notre capacité à le circonscrire. Directement confrontées aux effets de la désinformation et de la manipulation de l'information, les Armées construisent et consolident une nouvelle aptitude interarmées : « influence et lutte informationnelle ».

Il s'agit dès lors de se doter d'une capacité à détecter, caractériser et agir face à ces menaces. Ce chantier s'inscrit dans un contexte où les évolutions technologiques constantes modifient profondément l'approche de ce type d'affrontement. La guerre de l'information aujourd'hui, ne se limite plus à diffuser un récit pour infléchir des perceptions sur un théâtre d'opérations, mais elle vise aujourd'hui directement nos processus cognitifs. Cet élargissement du domaine est rendu possible par la prédominance du fait technique dans notre relation à l'information. Cette part croissante de l'intermédiation technologique rend alors possible la création d'un véritable « marché » de la désinformation et l'émergence d'une économie de l'influence informationnelle.

Comme le souligne Samuel Henry dans son article sur « la matérialité de la désinformation »[1], nous assistons aujourd'hui à une industrialisation des processus de désinformation qui gomme la frontière entre manipulation et information et nous plonge dans l'ère de la post vérité. Nous n'avons plus affaire à des séries d'actions isolées mais un écosystème complexe où la matérialité des techniques et des infrastructures joue un rôle déterminant. Dans ce cadre, la compréhension des mécanismes algorithmiques soutenant le modèle économique des plateformes de réseaux sociaux est un prérequis essentiel à l'action. Les acteurs étatiques et non-étatiques qui investissent massivement dans des dispositifs techniques sophistiqués pour amplifier leur capacité d'influence, transformant la désinformation en une véritable infrastructure stratégique. Ce que l'on qualifie aujourd'hui de « guerre de l'information » apparaît pourtant assez tôt dans l'histoire des conflits ; elle se fonde à l'origine sur la notion de ruse et agit sur les perceptions de l'adversaire. Sans définition établie, la guerre de l'information demeure un concept flou, propice aux interprétations divergentes. Le chercheur François-Bernard Huyghe la définissait en 2016 comme « l'ensemble des méthodes visant à infliger un dommage à un rival ou à se garantir une supériorité par l'acquisition d'information, par la dégradation de celle de l'adversaire ou par la

propagation de messages favorables à ses desseins stratégiques ». Mais avec l'émergence des réseaux sociaux et des nouveaux opérateurs de l'information, le concept déborde du champ strictement militaire et devient un outil au service des stratégies de pouvoirs étatiques.

David Colon, historien et spécialiste de l'histoire de la propagande, définit pour sa part la guerre de l'information comme « le fait pour un État de recourir à l'information comme à une arme, à des fins militaires, politiques, économiques, culturelles ou diplomatiques. Elle repose sur l'usage de l'information non seulement comme une source de pouvoir, mais comme un pouvoir en soi, autrement dit comme un levier de puissance dans les relations internationales ». Cette forme d'affrontement se développe sur trois niveaux distincts, le politico-militaire et les opérations, l'économie et le volet socio-culturel.

Aujourd'hui, avec les possibilités offertes par les technologies de l'intelligence artificielle, nous assistons probablement à une nouvelle évolution majeure qui permet de façonner plus en profondeur des franges croissante de la société. La guerre de l'information se mue en guerre cognitive et elle exploite les ressorts des algorithmes des plateformes.

Cette évolution conduit à explorer le concept de guerre cognitive algorithmique. Là où la guerre de l'information vise à modifier des comportements par l'action sur les perceptions, la guerre cognitive algorithmique va plus loin et cherche à influer sur les croyances profondes et modifier notre « lecture du monde et des événements ». C'est le processus de traitement de l'information par l'individu via les plateformes qui est ainsi ciblé et les usages numériques rendent ces manipulations possibles à une variété d'acteurs.

L'émergence de la guerre cognitive algorithmique

Le concept de « guerre cognitive algorithmique » est principalement développé par des chercheurs chinois et il fait l'objet de nombreuses études dans le cadre de leçons tirées du conflit en Ukraine. En effet, l'invasion de l'Ukraine par la Russie en 2022 a marqué un tournant dans la manière dont certaines puissances conçoivent la guerre cognitive, notamment l'importance des algorithmes et de l'intelligence artificielle. La capacité de l'Ukraine à utiliser les réseaux sociaux pour établir un « récit alternatif » par rapport à la Russie a été identifiée comme un facteur clé de son succès, notamment sur des plateformes comme TikTok.

Un rapport du « Special Competitive Studies Project »[2] de novembre 2024, présente la guerre cognitive comme un agrégat de « guerre d'opinion publique, guerre psychologique, guerre juridique et commerciale, guerre diplomatique, guerre technologique et guerre idéologique ». Cette approche très large n'est pas sans rappeler les intuitions des colonels Qiao Liang et Wang Xiangsui dans leur ouvrage de référence « La guerre hors limites » publié en 1999. Cette continuité souligne l'importance, pour les stratèges chinois, de développer des outils afin de contrôler les croyances de l'ennemi par des messages ciblés.

Cette forme de contrôle sur l'adversaire est considérée par les théoriciens chinois comme « potentiellement plus bénéfique que de détruire par la puissance de feu, de prendre le contrôle des troupes ou de conquérir des villes et des territoires ».

Un aspect crucial de cette approche est son caractère permanent : les opérations cognitives sont réparties entre les agences militaires, de sécurité et de renseignement, gommant les frontières entre temps de paix et de guerre. Ainsi, la guerre cognitive est conçue comme un engagement continue et de temps long, bien avant que les premiers soldats ne soient

mobilisés ou que les obus ne tombent. Cette continuité-là rend ainsi particulièrement difficile à identifier ou à contrer.

L'IA comme un catalyseur de la lutte informationnelle

Avec l'apparition des médias sociaux et le développement rapide de l'intelligence artificielle, les algorithmes sont devenus des outils capables de « créer un cadre cognitif flexible et de façonner les pensées et la cognition de l'adversaire sans qu'il ne le sache par la diffusion précise de messages tendancieux[3] ».

Les algorithmes sont perçus comme des « contrôleurs », des « portiers » et des créateurs de « cocons d'information ». Cette notion est en réalité beaucoup plus puissante que la simple bulle de filtre car elle repose sur une stratégie de manipulation volontaire des algorithmes par les créateurs de contenus. Le cocon sémantique résulte d'une analyse de l'intention de recherche de l'utilisateur, une extrapolation de l'intention basée sur la sémantique.

L'infrastructure technique sous-jacente aux campagnes de désinformation comprend désormais à côtés des « usines à trolls » hautement organisées, des fermes de robots automatisés (bots), et des systèmes d'IA capables de générer du contenu trompeur à grande échelle. Ces infrastructures matérielles constituent le squelette invisible mais essentiel des opérations d'influence contemporaines et sont essentielles au développement de la guerre cognitive. Les apports de l'IA sont alors doubles. Ils permettent d'une part d'automatiser un certain nombre de tâches qui auparavant incombaient à des opérateurs humains, simplifiant un aspect important de la guerre de l'information par la création de contenus. D'autre part l'IA permet surtout d'amplifier l'enfermement cognitif par un ciblage affiné des auditoires.

Agissant ainsi sur le ciblage, le développement de récit et l'automatisation de la diffusion, l'IA est aujourd'hui plus qu'un facteur de franchissement de seuil dans la guerre informationnelle mais potentiellement un élément de sa mutation vers la guerre cognitive algorithmique.

Quel modèle opérationnel de la guerre cognitive algorithmique ?

L'analyse des productions sur le domaine laisse entrevoir les apports de l'intelligence artificielle suivant un processus en six étapes :

❶ **Ciblage et « portrait de l'utilisateur » :** Le traitement algorithmique permet d'identifier les audiences cibles à grande échelle, et d'analyser l'état psychologique individuel comme les tendances sociales. Ce secteur est déjà exploité depuis de nombreuses années pour le marketing mais également dans le cadre des processus électoraux comme le scandale Cambridge Analytica a pu le mettre en lumière dès 2016. Il gagne pourtant en pertinence et change de nature en particulier par la connexion permanente de nombreux capteurs et la captation continue de données personnelles.

❷ **« Attirer l'attention » :** L'IA génère du contenu personnalisé, basé sur l'état psychologique en temps réel, afin de désarçonner le cadre cognitif existant de l'utilisateur. C'est ici que l'exploitation des biais cognitifs, couplée à un ciblage fin, se révèle particulièrement efficace. L'usage de plus en plus répandu des « chatbot émotionnels » témoigne ainsi de l'emprise potentielle de ces outils.

❸ **Suggérer des références :** Une fois le cadre fixé, l'attention captée, l'approche de la guerre cognitive algorithmique consiste à utiliser les mécanismes de diffusion pour faire apparaître la viralité de certains sujets comme naturelle. En exploitant ainsi certains biais informationnels, les cibles admettent progressivement un nouveau cadre de références.

❹ **Induire une réaction :** Les algorithmes regroupent les individus dans de nouveaux « cocons d'information ». En anticipant les recherches potentielles et en présentant des contenus, liens et produits statistiquement susceptibles d'intéresser les audiences et donc de les maintenir dans le « cocon ». On cherche ici, l'interaction avec le contenu, le clic, le « like », le commentaire.

❺ **Intervention opportune :** Des messages spécifiques sont utilisés pour s'assurer que ces interactions évoluent dans la direction souhaitée, maintenant la cible dans son « cocon ». C'est dans cette étape une sorte de recadrage de l'interaction qui permet le renforcement induit dans la phase suivante.

❻ **Superviser la gratification :** L'algorithme mesure la gratification sociale des cibles et modèle les dynamiques internes de ces nouveaux regroupements, renforçant l'enfermement dans un cadre cognitif spécifique.

Au cœur de cette nouvelle forme de guerre se trouve les données. Celles-ci sont fondamentales à cette approche algorithmique, et il faut non seulement des données en masse mais des données précises et de qualité. Comme le souligne un chercheur chinois cité dans le rapport : « bien que les algorithmes soient le cœur (de la guerre cognitive algorithmique), l'information de renseignement est la clé ».

Le profilage algorithmique permet donc de concevoir des contenus sur mesure, adaptés à l'état cognitif et psychologique de chaque individu, mais cela implique la collecte et le traitement de vastes quantités de données personnelles : historique d'achat, données de voyage, données de santé, etc. Cette exigence explique en partie certaines cyberattaques d'envergure attribuées à des acteurs étatiques, visant à alimenter leurs systèmes en données personnelles pour créer des profils complets de citoyens étrangers.

Cette infrastructure de données sophistiquée qui comprend des bases de données comportementales, des historiques de navigation, et des modèles prédictifs capables d'identifier les vulnérabilités cognitives et émotionnelles des populations ciblées est essentielle à ces opérations. La collecte massive de données personnelles n'est donc pas simplement un enjeu de vie privée, mais devient un véritable enjeu de sécurité nationale, transformant les plateformes numériques en potentielles armes informationnelles. Cette matérialité des infrastructures de données pose de nouvelles questions quant à la souveraineté numérique des États et leur capacité à protéger leurs populations des manipulations extérieures[4].

Défis et perspectives

La propagande massive non ciblée et grossière, si elle n'a pas disparu, ne vise pas à produire les mêmes effets que l'approche cognitive algorithmique qui se développe. L'une cherche à diviser et s'impose comme un instrument des « ingénieurs du chaos », l'autre cherche à modifier les croyances en profondeur. C'est là une différence fondamentale. Ce mécanisme se nourrit par ailleurs, d'un modèle économique hybride où les techniques de persuasion sont autant utilisées pour vendre des produits que pour conduire une campagne d'ingérence lors d'une élection. De nouveaux opérateurs apparaissent, repoussant les limites éthiques et contournant les réglementations et proposent littéralement des services de désinformation.

Dans ce contexte d'affrontement permanent, où l'innovation technologique entraîne un renouvellement constant des pratiques, les forces armées doivent, pour garantir l'efficacité de leurs actions, intégrer une pluralité de facteurs au sein d'une approche multichamps et multimilieux. La mobilisation résolue et massive de l'arme informationnelle par nos compétiteurs exige une refonte profonde de notre concept d'opérations d'information.

La structuration d'une capacité d'influence et de lutte informationnelle au sein des armées représente une occasion décisive de surmonter les résistances culturelles et techniques sans aucun renoncement à notre cadre légal et éthique. Il nous incombe dès lors de promouvoir une culture de l'hybridité, intégrant naturellement des actions indirectes et développant nos propres capacités d'action.

Pour peser dans ce système d'affrontement, plusieurs niveaux d'action sont possibles, mais le combat prioritaire semble être celui de la maîtrise des données. En s'inscrivant en complémentarité d'un dispositif interministériel éprouvé, les armées contribuent pleinement à la prise en compte de cet enjeu vital pour nos démocraties dans l'ère de l'intelligence artificielle.

Parution le 28 novembre 2025

[1] La matérialité de la désinformation. Samuel Henry
[2] Algorithmic Cognitive Warfare: The Next Frontier in China's Quest for Global Influence
[3] Chen Changxiao, Lee Ho, Feng Mingyue, Shu Shuai, https://d.wanfangdata.com.cn/periodical/gfkj202401019
[4] Samuel Henry, Quelle matérialité de la désinformation ? https://www.diploweb.com/Quelle-materialite-de la-desinformation.html

Menaces informationnelles : le développement du « Trust & Safety » dans les organisations

CAROLINE RABOURDIN
Doctorante sur les guerres de l'information
en Sciences de l'information et de la communication
Programme doctoral Défense-Sécurité intérieure
Université Aix-Marseille

Alors que les départements Trust & Safety sont connus aux Etats-Unis, a contrario en France, la majorité des entreprises ignorent tout de leur existence.

Né aux Etats-Unis, au début des années 2000 sous l'impulsion des géants du numérique comme eBay, Google et Facebook pour garantir la confiance des utilisateurs et la sécurité des réseaux, le « Trust & Safety » (« Confiance & Sécurité ») désigne aujourd'hui un ensemble de pratiques regroupées au sein d'un domaine d'activité devenu un département d'entreprise au même titre que le marketing, les ressources humaines ou la comptabilité.

Si les plateformes numériques ont été les premières à mettre en place des départements Trust & Safety, d'autres secteurs ont depuis emboîté le pas, comme les fintechs, marketplaces, jeux en ligne, assurances, services de santé, mobilité, institutions, etc.

Face à la multiplication des cyberattaques, à l'utilisation malveillante croissante des intelligences artificielles et à l'essor des campagnes de

désinformation, les entreprises sont confrontées à des risques multiples et protéiformes. Elles doivent sans cesse s'adapter pour répondre aux attaques et garantir la sécurité des personnes, systèmes et données, tout en préservant leur réputation et en respectant les lois, les règlementations et la vie privée de chacun. Le Trust & Safety apparaît donc comme une parade pour contrer les menaces informationnelles diverses.

Un domaine transversal et pluridisciplinaire

Le Trust & Safety est à la fois un ensemble de procédés, une fonction transversale et un domaine d'activité. En entreprise, la taille des équipes Trust & Safety varie considérablement d'une organisation à une autre. En mars 2024, Google comptait environ 250 collaborateurs, tandis que chez X (ex-Twitter), l'équipe Trust & Safety était composée de 2 300 personnes. Quant à Meta et TikTok, ils ont chacun annoncé employer près de 40 000 personnes.

Le Trust & Safety consiste à prévenir, détecter, protéger, répondre aux manipulations de l'information comprenant entre autres cyberattaques, désinformation, contenus trompeurs ou dangereux, fraudes, usurpations d'identité, etc. Il consiste à prévenir les atteintes psychologiques (harcèlement, menaces…), physiques (appels à la violence…), légales (contenus extrémistes, pédocriminels…) et économiques (escroqueries, ransomwares…).

Pluridisciplinaire, le Trust & Safety regroupe gestion des risques, cybersécurité, compliance (ou conformité), gestion des contenus, intelligence économique, communication, design produit, droit, expérience utilisateur (UX). Il rassemble ainsi experts cyber, modérateurs, analystes, juristes et avocats, data scientists, ingénieurs, responsables produits, rédacteurs, détectives…
Les équipes analysent les comportements des utilisateurs, détectent des schémas suspects (« pattern recognition »), répondent aux incidents,

alertent ou sensibilisent les clients, élaborent des politiques internes, rédigent des rapports de transparence, renforcent leurs protocoles, collaborent avec différentes parties prenantes, etc.

Leur approche est aussi proactive. En effet, le T&S ne se contente pas de réagir aux attaques : il anticipe également les menaces émergentes grâce à une veille stratégique et technologique, et finance des recherches scientifiques sur le sujet.

Quelles sont les missions du Trust & Safety ?

Gestion des risques
La démarche Trust & Safety commence par une analyse des risques spécifique. Il ne s'agit pas là d'une gestion des risques complète à l'organisation mais bien dédiée aux manipulations de l'information. Cette étape vise à identifier les vulnérabilités liées à la sécurité des données, des personnes, des infrastructures numériques et des flux informationnels internes comme externes. Puis, une stratégie de gestion des risques identifiés est déployée. Elle comprend notamment la mise en place de mesures préventives (protocoles de sécurité, formation, veille…) et curatives (réponse aux incidents…)

Cybersécurité
Le Trust and Safety inclut également la cybersécurité, permettant de protéger l'entreprise et ses utilisateurs contre les brèches de sécurité et accès non autorisés, les malwares (virus, spywares, ransomwares…), les tentatives de phishing, le vol, l'exfiltration ou la corruption de données, les utilisations malveillantes des intelligences artificielles (deepfakes, automatisation d'attaques, etc.).

Cela passe par des audits de sécurité et divers « pentest » (tests de pénétration) et le renforcement des systèmes d'information et des dispositifs

de détection des anomalies. Les équipes doivent ensuite s'assurer que les protocoles et les solutions déployées sont bien compliants avec les réglementations en vigueur (RGPD, DSA, NIS2, etc.). Enfin, les experts cyber sensibilisent les équipes, clients et parties prenantes sur la sécurité des mots de passe, l'authentification à double facteur et l'hygiène numérique.

Modération des contenus

Aujourd'hui, la majorité des entreprises ont un site Internet, intégrant éventuellement une boutique en ligne, et sont sur les réseaux sociaux. Autant de points d'entrée potentiels pour des acteurs malveillants. Si le Trust & Safety intervient sur la partie cyber, il ne se limite pas pour autant aux infrastructures techniques. Il vise aussi à lutter contre les menaces informationnelles relatives au contenu, dirigées contre l'entreprise, ses salariés, clients, parties prenantes, ainsi que contre ses produits.

Désinformation, propagande, chantage, menaces, discours haineux, apologie du terrorisme, incitation à l'auto-destruction, contenu violent, challenges dangereux sont passés au crible, tout comme les avis clients, les commentaires et autres contenus créés par autrui (« user-generated content »). Le but : éviter, limiter et contenir les crises réputationnelles ou sécuritaires. Pas question en effet de laisser passer sur les réseaux sociaux de fausses informations sur le dirigeant ou de révéler publiquement son adresse, ou encore d'accepter qu'un compte social utilise l'image de la marque, propage des fake news sur l'un de ses produits, ou menace certains salariés par messages privés.

Pour modérer l'ensemble des contenus, les équipes s'appuient sur des outils automatisés et recourent à des interventions humaines pour évaluer le second degré, l'humour et les références culturelles.

Elles peuvent également être amenées à travailler en partenariat avec les gouvernements dans le cadre de leur lutte contre la désinformation, lors de guerres hybrides notamment.

Pour les entreprises, la modération peut aussi inclure un volet Diplomatie digitale afin d'échanger avec les plateformes, connaître leurs règles de modération ou demander la suppression de certains contenus malveillants.
Management de l'escalade

En cas de plaintes de clients sur les réseaux sociaux, de conflit avec l'organisation ou d'amplification d'une crise réputationnelle, le département gère l'escalade en mettant en place des stratégies de réponses pour réagir de manière proportionnée, rapide, efficace, tout en respectant les valeurs de l'entreprise, ses conditions générales (« policies ») ainsi que le cadre légal. Les équipes implémentent des systèmes de détection et des protocoles de signalement, attribuent des pénalités (« red flag »), suppriment tout contenu portant atteinte, bloquent les comptes et recourent à des actions juridiques, si besoin.

L'objectif est double : garantir un espace numérique sûr pour tous et maintenir un climat de confiance avec la marque.

Intelligence économique
Lors d'une attaque informationnelle, le département T&S mobilise ses analystes pour mener des investigations et remonter à son origine. Il intervient également lors de fraudes, d'escroqueries, d'usurpations d'identité, de vol. Les experts analysent les comportements suspects et schémas d'activité, identifient les acteurs malveillants, cartographient les réseaux d'attaquants et attribuent des responsabilités. En collaboration avec des détectives, ils collectent les éléments qui serviront plus tard de preuves devant les tribunaux.

Selon le domaine d'activité de l'entreprise, les équipes Trust & Safety peuvent être amenées à identifier les campagnes d'influence étrangères, assurer le suivi de certains posts, suivre une tendance, afin d'aider les gouvernements dans leur lutte contre les ingérences.
Enfin, les équipes Trust & Safety mènent une veille stratégique et technologique pour anticiper les menaces et concevoir des outils de détection et de protection adaptés.

Politique d'utilisation (« Policy »)
Le Trust & Safety inclut la rédaction et la mise à jour de conditions générales ou politiques d'utilisation. Ces codes de conduite définissent les règles de ce qui est acceptable et ce qui ne l'est pas. Ils concernent la modération des contenus, la gestion des données personnelles, la résolution de conflits, etc. Ces conditions peuvent prendre la forme de chartes, standards, procédures, règlements. Elles évoluent en permanence afin de s'adapter aux nouvelles menaces et tactiques des attaquants, et servent de guide de conduite aux modérateurs, notamment.

Application de la loi (« Law enforcement »)
En cas d'activités malveillantes, juristes et avocats interviennent pour faire appliquer les conditions générales d'utilisation et les obligations légales (RGPD, DSA, Section 230…). Ils participent aussi à la définition de protocoles de réponse aux violations des CGU, aux fraudes, aux actes de contrefaçons ainsi qu'aux incidents de cybersécurité. Ils défendent également la propriété intellectuelle et le droit à l'image, et luttent par exemple contre l'utilisation non autorisée des licences, du nom de la marque ou de l'image de ses produits. En cas de besoin, une collaboration étroite avec les autorités est engagée lors d'enquêtes.

La transparence
L'obligation de communiquer de manière transparente incombe également à ce département. Dans ses rapports, qu'ils soient internes ou publics,

l'organisation doit expliciter ses règles, ses politiques de modération, ainsi que ses conditions générales d'utilisation. Ils expliquent comment les données sont collectées, utilisées, protégées, stockées, comment le contenu est modéré et les comportements d'utilisateurs gérés. Selon le domaine d'activité, ces documents détaillent le volume de modération et les demandes des autorités. La société peut aussi rendre publique certaines décisions, en particulier celles liées aux suspensions, aux retraits de contenus ou aux sanctions. En cas de défaillance ou d'incident majeur, elle peut être amenée à publier des excuses et à annoncer des mesures correctives afin de restaurer la confiance.

Vers un « Safety by design » ?

Et si la sécurité était pensée et réfléchie dès le début ? Le « Safety by design » consiste à intégrer l'ensemble des activités du Trust & Safety dès la création d'une entreprise ou de la conception d'un nouveau produit (« Product management ») ou d'un service. Les menaces informationnelles sont ainsi prises en compte dès le départ. Dans son rapport intitulé « Technology and Trust and Safety » publié en 2024, le gouvernement britannique estime que 65 % des organisation incluent les équipes Trust et Safety dès la phase d'idéation.

Cela inclut par exemple le développement de fonctionnalités, d'interfaces et de systèmes visant à protéger à la fois les infrastructures (sites web, plateformes, réseaux, bases de données…) mais aussi l'ensemble des parties prenantes (utilisateurs, clients, salariés, partenaires, fournisseurs…) contre les attaques cyber et celles liées au contenu.

Dans le cadre du « Product Management », le T&S est placé au cœur de chaque étape du cycle de vie d'un produit : de sa création à son utilisation sur le long terme, voire à ses mises à jour successives dans le cas d'un produit numérique.

Mais la démarche dépasse largement le champ du numérique. Elle concerne tout type d'organisation qui cherche à instaurer une relation de confiance durable avec ses usagers.

Enfin, le Trust & Safety inclut aussi l'expérience utilisateur (« User Experience » ou « UX »). Ici, la sécurité va de pair avec l'ergonomie d'un site Internet, d'une application, ou d'un service. Il s'agit de combiner sécurité et expérience client.

Une certification ISO

Les pratiques T&S font à présent l'objet d'une norme ISO. En juin 2025, l'ISO a publié une nouvelle norme internationale intitulée ISO/IEC 25389:2025, aussi appelée « The Safe Framework ». Elle fournit un cadre de recommandations aux organisations proposant un produit ou service numérique à destination du grand public, afin d'identifier, prévenir et maîtriser les risques liés aux contenus et aux comportements. Cette norme propose également des critères d'évaluation pour mesurer l'efficacité des pratiques mises en place.

Quel retour sur investissement ?

Dans son rapport « Technology and Trust and Safety » publié en 2024, le gouvernement britannique rapporte que même si le T&S permet de limiter les risques au sein d'une organisation, il reste difficile de quantifier le retour sur investissement.

Contrairement à d'autres fonctions en entreprise, il n'existe pas de formule unique : chaque organisation doit définir ses propres indicateurs en fonction de son secteur et de ses risques. Une entreprise pourra par exemple mesurer la baisse de commentaires négatifs, alors qu'une plateforme e-commerce suivra la diminution du taux de fraude. Le ROI mêle résultats

tangibles (réduction des fraudes, baisse des coûts juridiques) et résultats intangibles (confiance des utilisateurs, réputation de la marque).

Toutefois, le T&S est bien synonyme de résultats. Ainsi, le gouvernement britannique précise que les entreprises mettant l'accent sur la sécurité des données, la propriété intellectuelle et la confidentialité obtiennent de meilleurs résultats commerciaux et un meilleur retour sur investissement (ROI).

De plus, selon l'enquête Trust and Safety Survey 2025 menée par PwC, la mise en place d'une démarche Trust & Safety a un impact mesurable et favorable sur les consommateurs.

Le T&S ne se contente pas d'atténuer les risques informationnels, il augmente aussi les gains et accroît la valeur et le chiffre d'affaires d'une entreprise. Il augmente la confiance, la sécurité et la réputation, trois actifs immatériels qui conditionnent, à long terme, la performance et la croissance d'une entreprise.

Quelques cas concrets

Après un incident majeur en 2011 ayant ébranlé la crédibilité de la plateforme, Airbnb a massivement investi dans des dispositifs de Trust & Safety. L'entreprise a mis en place des systèmes de vérification d'identité, de paiement sécurisé, des services de photographie professionnelle pour valoriser les annonces, ainsi qu'un mécanisme d'avis et un programme de garantie pour les hôtes. Ces innovations ont permis de réduire les risques perçus par les utilisateurs et de créer une infrastructure forte.
Après avoir amélioré ses opérations de Trust & Safety, une plateforme d'e-commerce a constaté un taux de 99 % des problèmes résolus en moins de 24 heures.

Grâce à une refonte des processus de support et de modération, une plateforme nord-américaine de covoiturage a permis de réduire de 40 % les demandes répétées des usagers, d'atteindre 93 % de précision dans la résolution des cas et de garantir des délais de traitement inférieurs à 24 heures.

Conclusion

Alors que la mise en place de cellules d'intelligence économique peine encore à voir le jour au sein des entreprises françaises, les départements Trust & Safety pourraient leur permettre de rattraper ce retard.

Le Trust & Safety est une démarche globale qui vise à protéger l'entreprise ainsi que son écosystème, comprenant son patrimoine matériel et immatériel (ressources humaines, actifs financiers, propriété intellectuelle, réputation…). Face à des menaces informationnelles protéiformes et en constante évolution, et dans un contexte où la confiance est un atout clé, le Trust & Safety s'impose comme un levier stratégique pour assurer la pérennité, la sécurité et la compétitivité des organisations.

Parution le 19 décembre 2025

Merci à Thibault RENARD, expert IE, senior advisor du CyberCercle, qui a supervisé la rédaction de ce texte, ainsi que Fabienne CROP, spécialiste en IE, et Fabrice FROSSARD, Fondateur Faber Content, qui en ont assuré la relecture.

Sources bibliographiques

DeNARDIS, L., & HACKL, A. M. (2015). Internet governance by social media platforms. Telecommunications Policy, 39(9), 761–770

GILLESPIE, T. (2018). Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.

GILLESPIE, T. (2020). Content moderation, AI, and the question of scale. Big Data & Society, 7(2).

GORWA, R., BINNS, R., & KATZENBACH, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. Big Data & Society, 7(1).

JHAVER, S., GHOSHAL, S., BRUCKMAN, A., & GILBERT, E. (2018). Online harassment and content moderation: The case of blocklists. ACM Transactions on Computer-Human Interaction, 25(2), 12:1–12:33.

KLONICK, K. (2018). The new governors: The people, rules, and processes governing online speech. Harvard Law Review, 131(6), 1598–1670.

MATAMOROS-FERNÁNDEZ, A. (2017). Platformed racism: The mediation and circulation of an Australian race-based controversy on Twitter, Facebook and YouTube. Information, Communication & Society, 20(6), 930–946.

MOLLICK, E., & TAN, C. (2022). Trust and safety in the age of AI. MIT Sloan Management Review.

RIEDL, M. J., & YOUNG, R. M. (2005). An objective character believability evaluation procedure for multi-agent story generation systems. International Journal of Human-Computer Studies, 62(2), 263–298.

ROBERTS, S. T. (2019). Behind the screen: Content moderation in the shadows of social media. Yale University Press.

SCHWEMMER, C., & ZIEWITZ, M. (2022). Moderation at scale: Content moderation, collective control, and the regulation of platforms. Social Media + Society, 8(1).

SUZOR, N., WEST, S. M., QUODLING, A., & YORK, J. C. (2019). What do we mean when we talk about transparency? Toward meaningful transparency in commercial content moderation. International Journal of Communication, 13, 1526–1543.

https://www.nbcnews.com/tech/tech-news/big-tech-companies-reveal-trust-safety-cuts-disclosures-senate-judicia-rcna145435

https://techxplore.com/news/2024-03-google-trims-jobs-safety-clock.html

Table des matières

CyberCercle - 92 Cours Lafayette, 69003 Lyon
contact@cybercercle.com - cybercercle.com

Réalisation : S.I.M. Publicité - Photo d'illustration ©bestfoto77 - Shutterstock

Directeur de la publication : Bénédicte PILLIET
CyberCercle – 92 Cours Lafayette, 69003 Lyon
contact@cybercercle.com – cybercercle.com