UNIVERSITÉ CÔTE D'AZUR | ÉCOLE UNIVERSITAIRE DE RECHERCHE DROIT, SCIENCE POLITIQUE ET MANAGEMENT

SOIREE ENTREPRISE

30 juin 2026

GRAND ENTRETIEN

Colonel Christophe TORRISI
Conseiller aux affaires territoriales de la région de gendarmerie PACA, Commandant en second par intérim le groupement de gendarmerie des Alpes Maritimes

Caroline LEQUESNE
Vice-Doyenne aux relations socio-économiques, Maîtresse de conférences HDR en droit public, Directrice du Master II Droit algorithmique et gouvernance des données.

INTRODUCTION

Nous parlons beaucoup d'intelligence artificielle depuis deux ans. Souvent pour évoquer les gains de productivité, parfois pour s'inquiéter de ses dérives. Mais lorsqu'on échange avec les acteurs de terrain, ceux qui sont confrontés quotidiennement aux fraudes, aux cyberattaques, aux manipulations de l'information ou à la protection des données sensibles, une autre réalité apparaît.

L'intelligence artificielle ne crée pas seulement de nouveaux outils. Elle modifie profondément les rapports de force. Elle permet à des cybercriminels d'industrialiser leurs attaques, à des acteurs malveillants de produire des contenus trompeurs à grande échelle, mais elle offre également aux enquêteurs, aux entreprises et aux administrations des capacités inédites de détection, d'analyse et d'anticipation.

Face à cette accélération, une question se pose : comment conserver la maîtrise ?

Pour en parler, nous avons le plaisir d'accueillir le colonel Christophe Torrisi, conseiller aux affaires territoriales de la région de gendarmerie PACA, spécialiste des questions d'intelligence économique, de sécurité des entreprises et de transformation liée à l'intelligence artificielle.

I. LE NOUVEAU VISAGE DE LA MENACE

Caroline Lequesne : *Colonel, lorsque l'on parle de cybermenaces aujourd'hui, avons-nous affaire à une rupture ou à une évolution de phénomènes déjà connus ?*
Christophe Torrisi : Bonjour Caroline. Vous me demandez de choisir entre rupture ou évolution et je serai tenté de vous répondre de manière ironique « pourquoi choisir quand on peut avoir les deux ? ». En effet, de mon humble point de vue, nous pourrions dire qu'avec les cyberattaques, nous sommes désormais en présence d'une **évolution, mais que cette évolution est accélérée par une rupture technologique**.

Les modes d'action sont en réalité anciens, mais la vitesse et l'échelle ont changé. C'est un fait, l'IA générative permet d'industrialiser la criminalité. Ce n'est plus l'affaire de quelques experts isolés. Nous sommes plutôt en présence d'une criminalité d'opportunité accessible à tous. La **rupture** réside dans la capacité des attaquants à automatiser la détection **de vulnérabilités** et la **génération de vecteurs d'attaque personnalisés**, réduisant le temps de latence entre la découverte d'une faille et son exploitation à quelques secondes uniquement. Étant précisé que l'exploitation des outils d'IA peut désormais s'effectuer en langage naturel avec l'IA générative.

Caroline Lequesne : *On entend beaucoup parler de ransomware, de phishing, de deepfake, d'ingénierie sociale. Parmi toutes ces menaces, lesquelles vous préoccupent le plus aujourd'hui ?*

Christophe Torrisi : Ces menaces sont à la fois distinctes et complémentaires. Elles n'ont pas toujours les mêmes cibles ou les mêmes conséquences.

Le ransomware est un logiciel malveillant qui génère une rançon après le chiffrement et/ou l'exfiltration de données. Il cible de plus en plus les infrastructures critiques et les collectivités locales. Son impact peut se révéler catastrophique s'il l'entité victime ne s'y est pas préparée (sauvegarde des données, résilience des SI, communication, etc.).

Le phishing (hameçonnage) est une technique de tromperie visant à soutirer des informations sensibles ou à inciter la victime à exécuter une action malveillante. Cette menace est certainement la plus répandue. Les vecteurs d'attaque sont le plus souvent le mail ou le sms. On peut aussi parler de « spearphishing » (harponnage) lorsque le phishing est ciblé.

Le Deepfake (falsification de contenus audiovisuels par IA) et une menace particulièrement pernicieuse dans la mesure où, couplée avec les médias sociaux, elle peut altérer la notion de discernement, favoriser les ingérences numériques étrangères, et influer dans sa version la plus grave sur les enjeux démocratiques (d'où la création de VIGINUM en 2021 [développer si besoin]).

L'ingénierie sociale n'est pas vraiment une menace en soi. C'est plutôt un ensemble de techniques de manipulation psychologique visant à amener une personne à divulguer des informations confidentielles ou à exécuter une action précise (citer « Le petit traité de manipulation à l'usage des honnêtes gens » et développer si besoin).

La confiance se situe au cœur de chacun de ces dispositifs. Et j'aime bien rappeler cette citation qui dit que « **La confiance se gagne en goutte et se perd en litre** » !

Caroline Lequesne : *L'intelligence artificielle est souvent présentée comme un "game changer". Concrètement, qu'est-ce qu'elle change dans les capacités des attaquants ?*

Christophe Torrisi : L'IA change la **courbe d'apprentissage**. Il n'est plus nécessaire de savoir coder pour créer un malware sophistiqué ou une campagne de phishing ciblée. Il suffit de savoir utiliser une IA générative (prompt en langage naturel).

Certains sites se spécialisent même dans le partage de techniques et logiciels malveillants (FraudGPT, WormGPT par exemple).

Caroline Lequesne : *Dans nos discussions préparatoires, vous insistez sur un point intéressant : le danger n'est pas seulement la création de faux contenus, mais aussi la remise en cause de l'authenticité des contenus réels. Sommes-nous en train d'entrer dans une crise de la preuve et de la confiance ?*

Christophe Torrisi : Je ne pense pas que l'on puisse véritablement parler de crise de la preuve mais son admission dans le contentieux judiciaire, qu'il soit civil ou pénal, va certainement inciter les praticiens du droit à adopter des approches plus méthodologiques, voire des outils qui seront peut-être développés et mis à la disposition par la puissance publique, voire des acteurs privés (à l'image de « phishing initiative » distinct de « internet signalement »). Mais comme vous le soulignez, l'IA bouleverse la recherche probatoire et fait naitre quelques risques. Je n'en citerai que quatre.

Le risque premier est celui de la fausse preuve générée par IA

L'un des bouleversements majeurs vient de la capacité de l'IA à créer des preuves artificielles. Nous parlons ici de deepfakes, de fausses images, de voix synthétisées (3 secondes de voix suffisent), ou même de documents entiers générés. Ce ne sont pas de simples montages. Ce sont des fabrications capables de tromper l'œil humain et parfois les systèmes automatisés.

Le risque inverse est celui de la disqualification de preuves authentiques

Deuxième danger est peut-être celui de l'invalidation de preuves réelles sous prétexte qu'elles pourraient être artificielles. C'est l'effet inverse du deepfake : désormais, un enregistrement authentique peut être contesté au motif qu'il aurait pu être falsifié. C'est un risque de **paralysie probatoire**, voire de désinformation stratégique qui pourrait survenir dans le procès pénal. Nous serons peut-être amenés à doubler chaque preuve numérique d'un protocole de traçabilité, pour pouvoir garantir son authenticité à tout moment de la chaîne.

La perte d'intelligibilité : un algorithme qui décide seul

Certains outils d'IA intègrent des mécanismes décisionnels complexes, parfois opaques. Si l'on ne comprend pas comment un algorithme a abouti à une analyse, sa valeur en tant que preuve judiciaire est compromise.

Rappel réglementaire : selon la Charte de la commission européenne pour l'efficacité de la justice (CEPEJ), tout algorithme utilisé dans un contexte judiciaire doit être explicable, vérifiable, contestable. Cela exclut tout système dit "boîte noire".

L'illusion d'objectivité ou d'infaillibilité

Un danger insidieux est la crédulité face aux résultats produits par une IA. Parce que c'est automatisé, cela paraît incontestable. C'est faux. Une IA reflète la qualité des données qu'on lui donne, et les biais présents dans ces données se retrouvent dans les conclusions.

Caroline Lequesne : *Pour une entreprise ou une collectivité qui nous écoute aujourd'hui, quel est selon vous le risque cyber le plus sous-estimé ?*

Christophe Torrisi : Face à l'exposition aux risques numériques, toutes les entreprises et toutes les collectivités ne se valent pas. Si je devais l'imager, je dirais que cela revient à comparer un chef d'orchestre et ses musiciens (pour les grandes structures) à un homme orchestre (dans les petites structures). En clair, les petites structures sont plus exposées que les grandes.

Lorsque l'on parle de risque, on oublie très souvent de le qualifier ou d'en donner une définition précise. L'organisation internationale de la normalisation (ISO) en donne une définition précise et qualifie le risque comme « **l'effet de l'incertitude sur l'atteinte des objectifs** ». Son évaluation s'appuie sur deux composantes : la probabilité de survenance (**fréquence**) et son impact (**gravité**).

Mais pour répondre clairement à votre question sur le risque cyber le plus sous-estimé, c'est celui qui vise la chaine d'approvisionnement dans la mesure où ces attaques sont plus complexes à détecter et à maitriser. Les attaquants vont s'intéresser aux éléments les moins sécurisés de l'écosystème (prestataires, logiciels, cloud, sous-traitants technique, etc.).

Dit autrement, la force d'une chaine tient à la force de son maillon le plus faible.

II. DE LA CYBERSECURITE A LA GOUVERNANCE DU RISQUE

Longtemps, la cybersécurité a été perçue comme un sujet technique. Pourtant, ce qui semble se jouer aujourd'hui touche directement la gouvernance et la capacité des organisations à prendre des décisions éclairées.

Caroline Lequesne : *Quand vous échangez avec des dirigeants d'entreprise ou des responsables publics, quelles sont les erreurs d'appréciation que vous rencontrez le plus souvent ? Le premier maillon faible reste-t-il l'humain ?*

Christophe Torrisi : L'erreur principale pourrait être celle qui consiste à considérer la cybersécurité comme un centre de **coût (technique)** plutôt que comme un **vecteur de compétitivité**. Pourtant, les échanges commerciaux (pour les entreprises) ou les échanges entre administration et administrés sont **basés** en majeure partie **sur la confiance** (et le numérique) et comme nous avons pu l'évoquer précédemment la confiance peut rapidement être mise à mal face à une cyberattaque paralysante ou une exfiltration de données.

Lorsqu'il y a des erreurs d'appréciation, c'est souvent parce que la cybersécurité n'a pas été pensée en amont à travers **l'anticipation**, la **concentration** et l'économie des **moyens**. En effet, prioriser c'est **discerner ce qui est stratégique** de ce qui ne l'est pas, avant même de mettre en place les mesures de protection adaptées.

Dans les PME ETI et GE, cette responsabilité est souvent déléguée. Ceux qui l'exercent disposent de deux moyens pour **contraindre le dirigeant** : le **juridique** (responsabilité pénale) et le **financier** (moyens humains et matériels).

Quand on ne sait pas par quoi et comment commencer, on peut toujours raisonner selon trois **modes d'action** : **organisationnels** (structurels), **techniques** (utilisation de moyens technologiques) ou **comportementaux** (humains).

L'humain reste le maillon faible, mais pas seulement par négligence.

Caroline Lequesne : *Vous avez travaillé sur les questions d'intelligence économique et de sécurité des organisations. Observez-vous aujourd'hui une prise de conscience suffisante des dirigeants face aux enjeux cyber ?*
Christophe Torrisi : On l'oublie trop souvent mais la cybersécurité n'a pas d'autre finalité que de servir la sécurité économique globale d'une entreprise. À travers ce prisme, on comprend que la cybersécurité doit participer à conserver la maitrise de son **information stratégique** et de ses **savoir-faire**, c'est-à-dire tout ce qui donne de la valeur à l'entreprise et permet au dirigeant de se distinguer de ses concurrents.
Mais force est de constater que si **la prise de conscience des dirigeants est bien réelle**, elle est souvent **asynchrone** par rapport à la réalité technique (criminalité). C'est encore plus vrai lorsqu'il s'agit des dirigeants de petites structures qui ne savent pas toujours contre qui ou contre quoi se protéger.
C'est dans ce contexte que j'ai créé en 2019 un kit de sensibilisation baptisé « Le jeu des 8 familles d'atteintes à la sécurité économique » avec la volonté de relever 3 défis :
Le premier défi : accompagner les chefs d'entreprise parfois esseulés, souvent désemparés, et qui ne savent pas toujours contre qui ou contre quoi se protéger.
Le deuxième défi : renforcer la prise de conscience. En effet, la difficulté avec les atteintes à la sécurité économique est qu'elles peuvent se parer de légalité, ce qui les rend difficiles à déceler ou à dénoncer.
Le troisième défi : faciliter l'action des policiers et gendarmes confrontés à tous les maux de la société, et qui ne disposent pas toujours, en matière de sécurité économique, des clés de compréhension alors qu'ils se trouvent exposés en première ligne aux victimes d'atteintes en la matière.

Caroline Lequesne : *Les collectivités territoriales et les PME vous paraissent-elles mieux préparées qu'il y a cinq ans ?*
Christophe Torrisi : Elles sont **mieux informées, mais pas nécessairement mieux protégées**. La sensibilisation a augmenté grâce aux campagnes nationales et aux retours d'expérience médiatisés. Cependant, les moyens humains et financiers restent limités. Les collectivités ont souvent une dette technique importante (systèmes obsolètes) et peinent à recruter des experts. La clé n'est pas toujours l'outil, mais la **gouvernance des données** et la maîtrise des **accès**.

Pour rappel, **453 200 atteintes numériques ont été enregistrées en 2025** par le Ministère de l'Intérieur, ce qui représente une augmentation de **+87 % sur les cinq dernières années**.

Caroline Lequesne : *Que se passe-t-il concrètement dans les premières heures d'une cyberattaque importante ? Quelles sont les erreurs qui aggravent le plus souvent une crise ?*
Christophe Torrisi : Avant toute chose, il est essentiel de préciser que l'importance d'une cyberattaque se caractérise moins par l'ampleur des dégâts constatés sur les SI, que par les conséquences induites sur l'organisation qui en est vicitime. Une cyberattaque peut coûter plusieurs dizaines de millions à une entreprise sans que celle-ci ne disparaisse (exemple TV5 Monde) mais quelques dizaines ou centaines de milliers d'euros peuvent suffire à en faire disparaître une autre (exemple BRM Bressuire).
Une cyberattaque peut aussi débuter bien avant que la victime s'en aperçoit. Dans ce cas, l'attaquant va collecter un maximum d'informations publiques, se renseigner sur l'organisme, identifier les acteurs, consulter les médias sociaux et mettre en place sa stratégie pour dérober des identifiants et étudier les échanges (rôle, ton employé, moment opportun, etc) avant de procéder in fine à sa cyberattaque.
Les mesures d'urgence :

- Débrancher le réseau (filaire et sans fil) sans éteindre l'équipement.
- Prévenir le responsable informatique.
- Ne pas payer de rançon. Ne pas contacter le hacker.
- Ne plus toucher la machine (conservation des preuves).
- Déposer plainte à la brigade de gendarmerie ou au commissariat de police.
- Informer le CSIRT régional.
- En cas de fuite de données personnelles, informer la CNIL.

Caroline Lequesne : *À partir de quel moment faut-il considérer qu'une attaque cyber n'est plus seulement un problème informatique mais un problème de gouvernance ?*
Christophe Torrisi : Dès lors que l'attaque impacte la **continuité de l 'activité**, la **sécurité des personnes** et de biens, voire la **réputation**. Si un ransomware paralyse les services d'une mairie ou d'un hôpital, c'est un problème de continuité du service public, indépendamment des conséquences qui peuvent se révéler dramatiques. Si des données sensibles de citoyens sont volées, c'est un problème de conformité RGPD et de confiance.

III. COMMENT LA GENDARMERIE UTILISE ELLE-MEME L'IA ?

Cette transformation ne concerne pas seulement les attaquants. Elle touche aussi les moyens de protection et d'investigation.

Caroline Lequesne : *On parle beaucoup des usages malveillants de l'IA. Pourtant la gendarmerie utilise elle aussi ces technologies. Pour quels besoins concrets ?*
Vous évoquez notamment le traitement massif de données judiciaires. Comment l'IA aide-t-elle aujourd'hui les enquêteurs sans se substituer à eux ?

Christophe Torrisi : Effectivement, l'IA introduit un bouleversement dans la manière dont nous **observons**, **comprenons** et **agissons** sur l'environnement numérique.

Pour la Gendarmerie nationale, cette transformation n'est ni subie ni improvisée. Elle a été pensée, planifiée et encadrée.

Sa montée en puissance a débuté en 2020, face à l'emergence de nouvelles menaces cyber (NotPetya et Wannacry), avec trois grandes ambitions :

Renforcer la **protection du citoyen** (outils plus performants, identifcation..)

Améliorer les **conditions de travail** des gendarmes et soutenir leurs actions (ChatBot RH, IAccueil.

Inscrire notre action dans une logique de **transparence** et de **confiance**.

Dans le domaine judiciaire :

L'IA apparaît comme une réponse à la complexification des procédures :

Les enquêtes judiciaires sont aujourd'hui confrontées à une explosion de données numériques (téléphonie, cloud, supports de stockage, médias sociaux, objets connectés, vidéoprotection, etc.).

Chaque affaire peut générer des dizaines, voire des centaines de gigaoctets de données. Or, la capacité humaine d'analyse a ses limites. L'IA autorise dans ce cas précis un saut qualitatif : elle classe, trie, relie et contextualise les informations. Elle permet de dégager rapidement des signaux faibles, de repositionner dans une échelle de temps, de détecter des incohérences, voire des schémas relationnels.

L'IA peut aussi rendre la preuve plus robuste et structurée grâce à la modélisation

L'IA permet de modéliser des hypothèses judiciaires. On peut par exemple évaluer la vraisemblance d'un scénario à partir de multiples indices (géolocalisation, historique numérique, emploi du temps, etc.).

L'IA au service de la loyauté probatoire

La gendarmerie utilise aussi l'IA pour sécuriser la chaîne de preuve (authentification d'images, détection de deepfakes, analyse de cohérence documentaire).

Caroline Lequesne : *Pouvez-vous nous expliquer simplement quelques projets emblématiques comme GendVox, Janus ou les dispositifs de détection de deepfakes ?*
Christophe Torrisi : **Parole** : Le logiciel **PAROLE** est une plateforme d'aide à la transcription automatisée des interceptions téléphoniques, développée pour optimiser le traitement des fichiers audio dans le cadre des enquêtes judiciaires. Pour le moment, l'accès est réservé aux militaires APJ et OPJ affectés dans des unités de recherches et les MPF.
Janus : C'est un outil d'analyse de données visuelles et textuelles pour la recherche d'indices dans les enquêtes, notamment pour le traitement d'images ou de vidéos.
Détection de deepfakes : Nous utilisons des modèles comme **Authentik IA** pour analyser les signatures numériques des médias et détecter les altérations synthétiques. Ces outils sont essentiels pour authentifier les preuves numériques.
Mais aussi **ODIP,** ChatBot RH, PredNatinf, L'Agent, MirAI, Iaccueil, etc.
(→ à développer en fonction du temps dispo et des questions...)

Caroline Lequesne : *Vous insistez régulièrement sur l'idée que l'IA doit rester un assistant et non un décideur. Pourquoi cette distinction est-elle essentielle ?*

Christophe Torrisi : Nous pourrions disserter pendant des heures sur la place de l'IA par rapport à l'humain. Mais, au-delà des questions d'éthique, de transparence et de confiance, l'IA doit demeurer un assistant en matière de procédure pénale. La **responsabilité** pénale de l'enquêteur est **individuelle** et **inaliénable**. Un gendarme ou un officier de police judiciaire engage sa responsabilité pénale et disciplinaire sur ses actes et ses décisions.

L'IA ne peut pas être tenue pour responsable. Si l'IA commet une erreur, c'est l'humain qui en assume les conséquences. C'est pourquoi nous insistons sur l'**absence de substitution de la machine à l'humain**.

L'IA aide à traiter l'information, mais c'est l'enquêteur qui qualifie les faits, décide des suites à donner et présente l'affaire devant le magistrat.

Ces éléments sont rappelés dans la **charte Éthique IA** de la gendarmerie. (Confiance, Connaissance, Respect, Transparence, Loyauté et **Responsabilité**)

Caroline Lequesne : *Vous racontez un exemple frappant : celui d'une IA qui déduit l'âge d'une jeune fille simplement parce qu'elle est en classe de quatrième. Que nous apprend cet exemple sur les limites actuelles de ces technologies ?*

Christophe Torrisi : L'exemple que j'avais évoqué avec vous était l'illustration de l'illusion d'objectivité ou d'infaillibilité d'une IA.

Au cas d'espèce, dans le cadre de l'élaboration en interne d'un large modèle de langage (LLM) destiné à assister l'enquêteur pour la rédaction d'un PV de synthèse, une faille est détectée. (Exemple cité par GCA Boget à VivaTeck2025).

Voici le cas concret :

On a pris une procédure avec l'accord du magistrat. C'est un père qui se dispute avec sa fille, la veille au soir. La fille monte dans sa chambre en claquant la porte. Le lendemain, le père part travailler. Quand il revient, sa fille n'est pas là. Il décide de se rendre à la gendarmerie pour signaler la disparition inquiétante de sa fille. Il explique tout, qu'il s'est engueulé avec sa fille la veille au soir, que sa fille est en quatrième, qu'elle avait cours aujourd'hui, etc.

Tous ces éléments sont rentrés dans l'IA qui effectue un résumé extrêmement propre. Quand on le lit, on se dit que c'est très bien sauf que l'IA précise que la fille a 14 ans. Jamais dans la procédure, le père précise qu'elle a 14 ans. Il est juste dit que sa fille est scolarisée en classe de quatrième ! L'âge en droit, c'est quelque chose qui revêt une importance majeure (minorité pénale).

Pour éviter cet écueil, nous avons développé une doctrine claire :

- Protocole de vérification systématique des données sources (auditabilité, intégrité, traçabilité),
- Double lecture humaine des résultats produits par IA,
- Partenariat avec des experts académiques et juridiques dès la conception des outils.

Caroline Lequesne : *La souveraineté numérique est devenue un sujet majeur. Peut-on réellement parler d'autonomie stratégique lorsqu'une grande partie des modèles d'IA proviennent encore d'acteurs extra-européens ?*

Christophe Torrisi : Dans le domaine de la sécurité, la souveraineté, ou plutôt l'autonomie stratégique, est un enjeu fondamental. Car il n'existe peut-être pas de ministère aussi proche du citoyen que celui du ministère de l'Intérieur. Au sein de ce ministère, il s'agit d'assurer les protections collectives des personnes et des biens. Mais cette protection doit s'exercer avec le souci permanent d'un équilibre entre impératif de sécurité et respect des libertés individuelles.

Il est essentiel de maitriser les moyens qui participent à ces missions aujourd'hui régaliennes. Le risque est réel de voir progressivement des Big tech s'emparer de part de marché significative dans le champ régalien. **Il ne** s'agit donc pas d'être souverain en IA pour le plaisir de maitriser une technologie. **L'enjeu** est bien celui de la **souveraineté dans le champ d'activité de la sécurité**.

La souveraineté en IA se joue sur les infrastructures, les modèles et les données. L'internalisation d'un modèle d'IA générative au sein de ses SI ne suffit pas à affirmer que nous sommes souverains.

IV. PRÉPARER LES ORGANISATIONS À LA PROCHAINE DÉCENNIE

Finalement, la technologie n'est peut-être pas le principal défi. Le vrai sujet semble être la capacité collective à la comprendre et à la maîtriser.

Caroline Lequesne : *Vous avez participé à plusieurs réflexions sur la souveraineté et la gouvernance de l'IA. Quel est selon vous le plus grand défi des cinq prochaines années ?*

Christophe Torrisi : Le plus grand défi sera la **vitesse d'adaptation**. La technologie évolue plus vite que les lois, les formations et les processus organisationnels. Il faut créer des **cadres agiles** qui permettent d'innover sans perdre le contrôle. La Gendarmerie travaille à une gouvernance rigoureuse mais flexible, avec des comités d'éthique et de validation des usages

Caroline Lequesne : *Les organisations investissent beaucoup dans les outils. Investissent-elles suffisamment dans les compétences ?*
Christophe Torrisi : Non, c'est souvent le point faible. On achète des logiciels, mais on ne forme pas les utilisateurs à les utiliser de manière sécurisée et efficace. L'appréhension des outils peut constituer une charge mentale.

Il y a trois ans, lorsqu'il s'est agi de monter en puissance dans la compréhension de l'IA, la Gendarmerie a créé un MOOC national pour sensibiliser plus de **90 000 gendarmes** et publie la revue *CulturIA qui se poursuit désormais sous la forme d'une newsletter « Veille IA et Cybercriminalité ».* L'investissement dans le capital humain (formation continue, recrutement de profils hybrides tech/droit) est aussi important que l'investissement technologique.

Caroline Lequesne : *La gendarmerie a formé des dizaines de milliers de personnels à l'IA. Que peut en retenir le monde de l'entreprise et des administrations ?*
Christophe Torrisi : Je pense que nous devons rester humbles en toutes circonstances. On dit souvent que « **là où il y a la volonté, il y a un chemin** ». C'est fort de cet adage que des fondations ont été créées (Charte Éthique, coordonnateur national IA) et que des briques se sont progressivement empilées.
Notre modèle s'appuie notamment sur :
L'accessibilité : La formation doit être massive, continue et adaptée à tous les niveaux hiérarchiques.
L'interdisciplinarité : Former les techniciens au droit, et les juristes aux enjeux techniques.
L'éthique comme levier : Inscrire l'IA dans les valeurs de l'organisation pour gagner la confiance des personnels et conserver celle des citoyens.

Caroline Lequesne : *Faut-il désormais considérer la culture cyber comme une compétence de base au même titre que les compétences numériques ?*
Christophe Torrisi : Absolument. La culture cyber ne se limite pas à ne pas cliquer sur un lien suspect. Mais un saut qualitatif peut-être rapidement atteint si l'on retient que les trois piliers de la cybersécurité sont la sécurité des systèmes d'information, la lutte contre la cybercriminalité et la cyberdéfense.

Aucune connaissance technique n'est par ailleurs nécessaire pour assimiler les trois principes de la sécurité de l'information, à savoir la **confidentialité**, **l'intégrité** et la **disponibilité** des données.

Caroline Lequesne : *Si vous étiez aujourd'hui dirigeant d'une PME, directeur d'une collectivité ou responsable d'une administration, quelles seraient vos trois priorités dès demain matin ?*
Christophe Torrisi :
Cartographier les données sensibles et les actifs critiques (on ne protège bien que ce que l'on connaît.).
Former et sensibiliser massivement pour instaurer une culture du doute et de la vérification.
Élaborer un plan de continuité et de reprise d'activité.

CONCLUSION
Caroline Lequesne : Pour terminer, j'aimerais vous poser une question simple : dans un monde où l'on parle beaucoup d'intelligence artificielle, de cyberattaques et de désinformation, qu'est-ce qui vous rend malgré tout optimiste ?
Christophe Torrisi : Je suis optimiste parce que **l'IA est à la fois le glaive et le bouclier**. Les mêmes technologies qui créent des menaces permettent de les détecter, de les analyser et de les contrer à une échelle inédite. Je suis optimiste parce que la **coopération** s'intensifie, que ce soit à l'international, entre les forces de sécurité intérieure, entre secteurs public et privé. Et je suis optimiste parce que l'humain reste au centre du « jeu ». La technologie ne vaut que par ceux qui la maîtrisent.