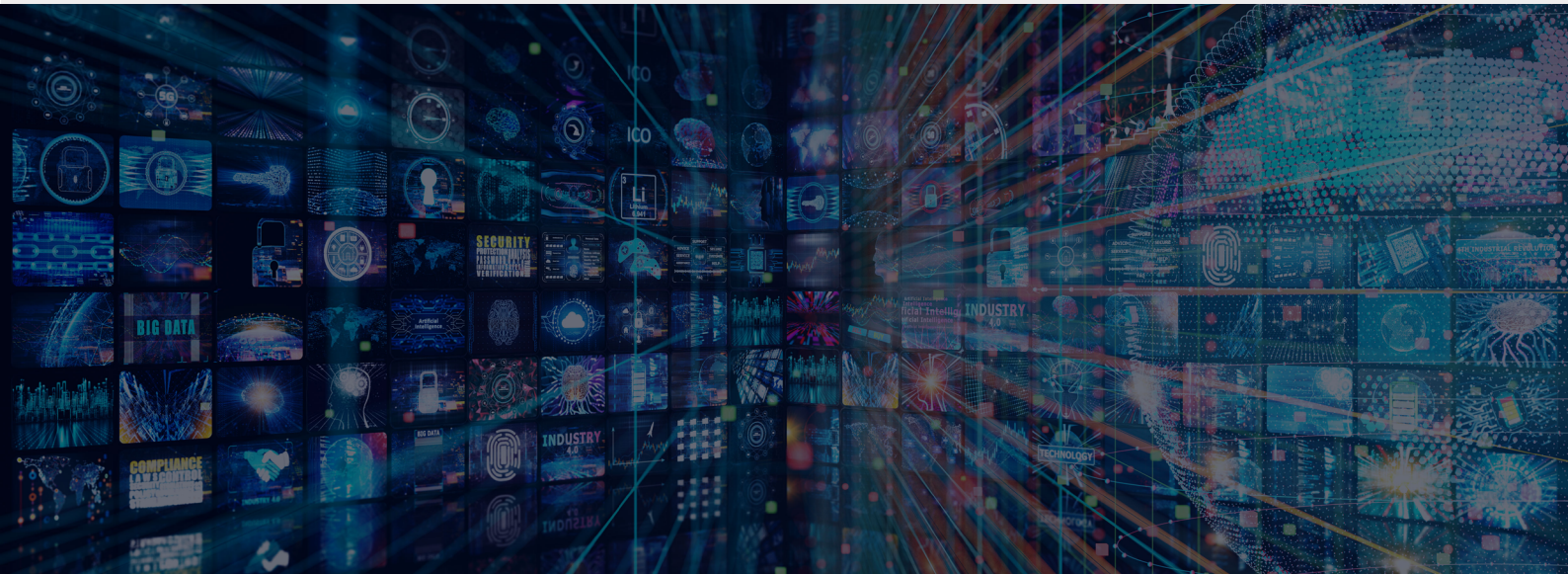
IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

OBSERVATOIRE
de l'information
et des stratégies
d'influence

CYBERSÉCURITÉ, LE FACTEUR HUMAIN EN EST-IL LE CENTRE DE GRAVITÉ ?

Bastian Dufilhol / Officier général en 2e section de l'armée de Terre, professeur à l'ESCP

Octobre 2025



PRÉSENTATION DE L'AUTEUR

Bastian Dufilhol / Officier général en 2e section de l'armée de Terre, professeur à l'ESCP

Officier général en 2e section de l'armée de Terre, Bastian Dufilhol est aujourd'hui investi dans l'enseignement supérieur (ESCP et Centre des hautes études militaires). Il est également en charge du développement des secteurs défense, régalien et industries de défense d'ANOZR WAY, *start up* française en cybersécurité. De 2011 à 2013, sous l'autorité du chef d'état-major de l'armée de Terre, il a coordonné le projet de simplification du fonctionnement de l'armée de Terre.
Saint-Cyrien, breveté de l'École de Guerre, il est ingénieur, diplômé de l'ESSEC et docteur en sciences politiques. Auditeur de l'institut des hautes études du ministère de l'Intérieur, il est l'auteur d'une thèse sur la résilience de l'État, mêlant politiques publiques, théorie des organisations et sociologie des crises.

PRÉSENTATION DE L'OBSERVATOIRE

L'Observatoire de l'information et des stratégies d'influence de l'IRIS se consacre à l'analyse approfondie des mécanismes de fabrication de l'information, des logiques médiatiques et des stratégies d'influence, dans un contexte international. Il explore comment l'information est produite, transcrite et diffusée dans les médias traditionnels, numériques et les réseaux sociaux, tout en examinant les dynamiques de pouvoir, les enjeux géopolitiques, les dilemmes éthiques et problématiques économiques liés à ces pratiques.

À l'ère du numérique, l'Observatoire vise à éclairer les relations complexes entre médias, opinion publique et sphères d'influence à travers le monde, en incluant une perspective stratégique. Il s'adresse aux décideurs, chercheurs et citoyens soucieux de mieux comprendre les enjeux globaux de l'information et de l'influence.

À travers ses travaux et ses initiatives, l'Observatoire se positionne comme une ressource de réflexions et d'analyses des stratégies d'influence et de désinformation, contribuant ainsi à un débat public éclairé et informé.

iris-france.org

@InstitutIRIS

@InstitutIRIS

institut_iris

IRIS

IRIS - Institut de relations internationales et stratégiques

En mai 2024, plusieurs assistants parlementaires européens ont été ciblés par une campagne d'ingénierie sociale particulièrement sophistiquée. Des cyberdélinquants ont utilisé de faux profils LinkedIn très bien construits pour entrer en relation avec ces collaborateurs, leur proposer des opportunités professionnelles valorisantes, et *in fine* les inciter à ouvrir des documents piégés ou à divulguer des informations sensibles. Un cas d'école avec un mode opératoire 100 % cognitif, une finalité entre enjeux politiques et économiques et une exploitation directe de l'empreinte numérique des cibles. La menace ne pénètre plus par une faille technique. Elle infiltre les esprits, les émotions, les habitudes quotidiennes. Le facteur humain est devenu le champ de bataille central. Et dans cette guerre silencieuse, la donnée personnelle est à la fois la munition et le butin.

La racine « cyber » provient du mot cybernétique qui a été formé en français en 1834 pour désigner la « science du gouvernement », à partir du grec *kubernêtiké*, signifiant « diriger, gouverner ». Le terme est repris en 1948, aux États-Unis, par le mathématicien Norman Wiener à l'origine de la cybernétique, science constituée par l'ensemble des théories relatives au contrôle, à la régulation et à la communication entre l'être vivant et la machine[1]. Avant même la naissance de ce que l'on appelle depuis 1984[2] l'espace cyber, le facteur humain, dans toute son acception, y occupe de manière consubstantielle une place centrale.

Alors que 80 % des attaques cyber réussies le sont aujourd'hui par le biais humain, **la menace s'est structurée dans un continuum cyber – numérique – informationnel – cognitif**, qu'elle soit d'origine institutionnelle à des fins de déstabilisation, qu'elle soit criminelle, ou bien même la combinaison des deux par *proxy*[3] agissant pour le compte d'États.

Bénéficiant d'un écosystème favorable à ce continuum, elle y adopte principalement le mode d'action de l'ingénierie sociale, reposant sur la captation d'informations et la capacité à influencer les comportements, qu'ils soient individuels, sous forme de pression par exemple, ou collectifs comme la manipulation de masse. Les données personnelles se sont alors transformées en matières premières. Dans ce contexte, le changement de paradigme réside dans le fait que le facteur humain est devenu le vecteur de la menace.

Se pose alors la question de savoir si la défense cyber en France et au sein des organisations qui la composent, probablement aujourd'hui encore trop segmentée et éparpillée, doit, elle aussi, s'inscrire dans ce continuum afin de nous protéger efficacement. En outre, pour les

[1] Solange Ghernaouti, *Cybersécurité : Analyser les risques, mettre en œuvre les solutions*, 7e éd. (Paris : Dunod, 2022).
[2] William Gibson est un écrivain américain, inspiré des contre-cultures des années 1970-80. Il a signé de nombreux romans de science-fiction visionnaires. Il évoque pour la toute première fois le *cyberspace* dans son livre *Neuromancien* en 1984.
[3] On entend par proxy dans le champ de la conflictualité une organisation ou un groupe agissant pour le compte d'un État sans lien effectif.

individus comme pour les organisations, l'enjeu semble être désormais la maîtrise de leur empreinte numérique afin de se prémunir de cette menace.

Un état des lieux sur les attaques par ingénierie sociale permet dans un premier temps de comprendre le poids du facteur humain et les notions de stratégies directe et indirecte. Dans un souci d'approche globale, il est nécessaire de compléter le constat par une analyse psychologique et comportementale de la menace. Par ailleurs, dans un champ d'affrontement devenu asymétrique, notamment pour des raisons juridiques, la donnée personnelle présente des singularités, une grande sensibilité, mais surtout elle est devenue l'unité de valeur. Fort de ces constats, il est possible d'esquisser les voies à explorer afin de structurer la défense cyber dans un continuum où la menace s'est, elle, déjà inscrite.

L'ATTAQUE PAR INGÉNIERIE SOCIALE EST DEVENUE LE MODE D'ACTION PRIVILÉGIÉ

En tout premier lieu, il convient d'analyser la *cyber kill chain*, chaîne de valeur de la menace cyber qui bénéficie de l'écosystème très favorable de l'hybridité particulièrement prononcée entre vies numériques personnelle et professionnelle. Des nombreux travaux de recherche et de l'expérience de la société ANOZR WAY[4], il ressort qu'elle se décompose en plusieurs étapes. En tout premier lieu, une organisation est ciblée pour l'intérêt qu'elle présente (espionnage, proxy[5], levier de déstabilisation…). La seconde étape consiste à identifier les personnes à haute valeur ajoutée : dirigeants, postes sensibles et toute personne présentant une surexposition cyber, comprenant l'exposition cyber comme la combinaison entre les vulnérabilités et la surface d'attaque résultant de son empreinte numérique. Une fois ces personnes identifiées, débute la collecte de données les concernant à partir du *clear*, du *deep* et du *dark web*[6]. Les cercles familial, amical et professionnel de ces individus sont aussi concernés, généralement à partir de technologies de *scrapping* comme les avatars sur les

[4] L'auteur de ces lignes est actuellement conseiller sécurité dans l'entreprise nommée.

[5] Un *proxy* est ici à considérer comme une entité intermédiaire entre une organisation et une cible.

[6] Le *clear web* correspond à toutes les pages indexées par les moteurs de recherche classiques, du type Google, Bing ou encore Baidu. Il englobe donc aussi bien Wikipedia et YouTube que les blogs, les sites d'e-commerce, les sites d'information… Le *deep web*, de son côté, correspond aux contenus qui ne sont pas indexés directement par les moteurs de recherche. Il comprend toutes les pages qui nécessitent une authentification : bases de données, parties non publiques des sites bancaires, relevés d'imposition, données médicales… Enfin, il existe une partie du web beaucoup plus difficile d'accès : il s'agit du *dark web.* Cette partie sombre d'internet porte bien son nom : il s'agit de réseaux superposés qui utilisent l'internet public, et qui ne sont accessibles que via des logiciels ou des configurations spécifiques. Aucun des sites présents n'est indexé, et pour les retrouver, il faut passer par des sous-réseaux tels que Tor, I2P, Freenet ou Zeronet. Les protocoles employés par ces sous-réseaux du dark web (les dark nets) garantissent a priori l'anonymat de ceux qui s'y rendent. Mais un manque de précaution peut entraîner une identification (au moins partielle) des utilisateurs et les mettre en danger : le dark web est aussi le terrain de jeu de criminels, qui y mènent des activités illégales (ventes et achats de données volées, d'armes, de substances ou contenus illicites, de logiciels de cyberattaques, etc.).

réseaux sociaux combinés à des robots qui pivotent sur chaque donnée afin d'en agréger de nouvelles, ceci jusqu'à épuisement des données indexables. Une fois la donnée rassemblée, il est possible d'établir l'empreinte numérique d'une personne ; cette dernière est analysée afin d'en dégager les vulnérabilités[7] et la surface d'attaque définissant l'exposition cyber. La dernière étape consiste en une exploitation de cette surface d'attaque en élaborant des scénarios adaptés aux vulnérabilités de la personne (usurpation de compte, *smsishing*, *spearfishing*, *MFA bypassing*…). Une forme de *« weaponisation[8] ».* L'étape clé est la collecte des données qui occupe une place centrale de cette chaîne de valeur.

Plusieurs cas viennent alors caractériser la menace et ses conséquences, permettant de comprendre le poids du facteur humain. Été 2024, des milliers de familles ukrainiennes ont fait l'objet d'attaques par ingénierie sociale, de déstabilisation et de fraudes bancaires à partir des noms et prénoms de soldats ukrainiens identifiés sur le front oriental. Deux ans plus tôt, en février – mars 2022, les troupes russes ont été géolocalisées à partir de l'utilisation d'applications de rencontre comme Tinder. À l'automne 2023, l'un des géants de la base industrielle et technologique de défense (BITD)[9] a fait l'objet, durant cinq mois, de fuites de données à partir de *ransomware*. Si pourtant les grands groupes de la BITD se donnent les moyens de se prémunir contre le risque cyber, le réseau de 4 000 sous-traitants ne dispose pas des mêmes moyens et se trouve être la cible d'attaques cyber selon une logique d'approche indirecte. À titre d'exemple, une PME[10] dans le secteur de l'aéronautique découvre, en janvier 2024, des ordinateurs professionnels infectés d'*infostealers*[11]. Il est alors bon de réaliser qu'un *infostealer* permet la récupération à distance de l'intégralité d'un disque dur, de l'historique de navigation internet/intranet et des données du trousseau. Après sensibilisation, plusieurs employés ont découvert que leurs PC personnels étaient également infectés. Un ordinateur personnel permettait à lui seul de retrouver 200 identifiants et mots de passe, dont certains à vocation professionnelle.

Début 2025, à partir de l'application Strava, les déplacements du président de la République française parviennent à être anticipés avec précision[12]. Deux mois plus tard, toujours par

[7] « Dans la législation, et la littérature en matière de cybersécurité, on retrouve trois termes qui sont employés comme des synonymes, mais qui en réalité ne le sont pas : vulnérabilité / cybermenace / risque. Plus l'exposition (numérique en l'occurrence) est grande, plus la vulnérabilité est grande ; inversement, plus la capacité de réponse est grande, moins la vulnérabilité est grande. Cela signifie que *vulnérabilité = exposition / capacité de réponse*. » (Dr Emilie Musso).

[8] Fabrication d'armes ou de vecteurs adaptés et employés par la menace afin d'attaquer.

[9] Le nom de l'entreprise ne peut être communiqué pour des raisons de confidentialité et de protection.

[10] *Ibid* 3

[11] Un *infostealer* est un terme d'informatique désignant une forme de logiciel malveillant créé dans le but de pénétrer les systèmes d'information et d'y voler des informations sensibles. Il peut notamment s'agir d'informations de connexion, d'informations financières ou d'autres données personnelles. On pourrait citer : *Redline, Vidar, RacoonStealer, Stealc, Trojan*.

[12] Les membres du groupement de sécurité de la présidence de la République (GSPR) utilisent leur application STRAVA© afin d'enregistrer, voire de publier, leurs performances en course à pied alors qu'ils effectuent les reconnaissances des déplacements à venir du président de la République.

Strava, les contours comme les accès de la très secrète base militaire de l'Île-Longue, abritant les sous-marins nucléaires lanceurs d'engins, sont dévoilés ; alors que la sensibilité du sujet est pourtant déjà soulevée lors de son utilisation par des unités militaires en Irak (2010), en Afghanistan (2011) et au Mali (2018), dévoilant les contours de bases opérationnelles avancées sur ces théâtres d'opérations. En juillet 2024, un test au sein d'un ministère régalien français permet de mettre en évidence, sur l'échantillon des vingt plus hauts fonctionnaires de ce ministère, un niveau d'exposition cyber critique. La compromission, en 2024, de l'adresse électronique *elysee.fr* d'Emmanuel Moulin, actuel Secrétaire général de la présidence de la République française, suffit elle aussi à confirmer que le sujet atteint le sommet de l'État. Ces deux exemples démontrent le fait contre-intuitif que les dirigeants sont les plus exposés en termes de vulnérabilité cyber.

Ce phénomène est confirmé à l'aune de ce dernier exemple, celui d'une femme, membre du comité exécutif d'une entreprise du CAC 40. Engagée dans une négociation en Asie du Sud-Est, elle reçoit une heure avant la réunion décisive un appel sur son téléphone mobile personnel : « Êtes-vous bien la mère de Julien et Marie[13] qui sont dans le lycée … dans le 15e à Paris ? Nous sommes à côté », et cela raccroche. Après avoir alerté le lycée et son mari, elle conduit sa négociation qui sera un échec.

LE BIAIS COGNITIF ET COMPORTEMENTAL EST UNE CLÉ DE COMPRÉHENSION INDISPENSABLE

L'attaque commence par une photo Instagram, une liste de contacts sur LinkedIn, un footing posté sur Strava. Chaque clic, chaque partage, chaque naïveté est exploité, recyclé, amplifié. C'est une stratégie d'étouffement invisible : on est scrappé, indexé, profilé puis retourné contre soi-même.

« Ce que la cybersécurité peine encore à comprendre, les attaquants l'ont déjà intégré : ils ne ciblent pas un système, mais des décisions, des vulnérabilités cognitives, des réflexes humains. Il ne s'agit plus seulement de défendre un système d'information. Il s'agit de reprendre le contrôle de nos propres récits, de notre exposition, de notre souveraineté mentale. Et pendant que les entreprises dressent des murailles autour de leurs serveurs, c'est un simple téléphone personnel qui ouvre la brèche ; une voix d'enfant, une question d'école, un silence

[13] Les prénoms ont été changés.

». C'est ainsi que Nathalie Granier, psychologue experte dans le champ de la cybersécurité, illustre la dimension comportementale et cognitive[14].

L'analyse comportementale est une discipline qui examine le comportement des utilisateurs ou des attaquants et dont l'objectif principal est d'anticiper des menaces potentielles et de renforcer les mesures de sécurité en conséquence. Cela revient à une forme de profilage[15]. Cette approche s'avère essentielle dans la caractérisation de la menace et sur l'identification des moyens de s'en prémunir. Dans ce nouveau champ de bataille, la pensée devient un vecteur d'intrusion.

Selon Nathalie Granier, « l'analyse comportementale va permettre de répondre à 3 grands sujets. Tout d'abord l'analyse du lieu du crime. En cyber, cela va consister à collecter des preuves physiques documentant la scène, car elles existent aussi dans cet espace : les identifiants de connexion, les journaux, les horaires de connexions, *etc.* L'analyste va ensuite corréler ces informations les unes avec les autres. La deuxième étape consistera à récupérer les documents. Enfin, pour réaliser le profilage, il est essentiel d'analyser minutieusement le comportement et les caractéristiques des cybercriminels afin de créer des profils qui peuvent aider à les identifier. Cette démarche vise à récupérer des informations sur les traits personnels, les caractéristiques sociales, les facteurs motivants qui vont aider ensuite les équipes techniques qui chercheront à répondre aux questions suivantes : qu'a pu faire l'adversaire ? Quels sont leurs objectifs ? Qui sont-ils ? Que vont-ils faire ensuite ? *In fine*, elle permet de détecter les menaces, et de répondre aux incidents, d'identifier des comportements anormaux, améliorer la défense. »

Outre la psychologie, d'autres disciplines telles que la géopolitique, la linguistique et la sociologie peuvent également jouer un rôle crucial dans cette analyse. Nathalie Granier souligne cependant que l'analyse comportementale présente des limites[16], de confidentialité, de biais cognitifs, de faux positifs, de manque de données et de méthodes.

---

[14] Propos recueillis en entretien, 27 mai 2025.

[15] Le profilage, selon la définition du RGPD, « est le traitement automatisé de données à caractère personnel qui consiste à utiliser ces données pour évaluer certains aspects de la personne concernée, et analyser ou prédire ses intérêts, son comportement et d'autres attributs. »

[16] Évoluant également chez ANOZR WAY, Nathalie Granier précise que l'analyse comportementale « se trouve souvent confrontée à une préoccupation majeure : **la confidentialité**. Leur principal outil de travail étant les données, il est essentiel de respecter les normes de confidentialité et de gérer correctement les informations sensibles afin d'éviter tout abus ou violation de la vie privée. Cela est particulièrement crucial lorsqu'il s'agit d'investigations sur l'ordinateur d'un employé, par exemple. Puis, le profiling en cybersécurité peut être entravé par divers **biais cognitifs** auxquels l'analyste peut être sujet, tels que le biais de conformité, d'ancrage, de représentativité et de confirmation. Ces biais peuvent influencer négativement la prise de décision et l'analyse en favorisant des conclusions préconçues ou partielles. Il est donc essentiel de reconnaître, comprendre et maîtriser ces biais pour assurer une évaluation objective et rigoureuse des menaces.
Enfin et surtout, l'analyste n'est pas à l'abri des faux positifs ou des faux négatifs. Nous ne pouvons garantir une attribution à 100%. Plusieurs facteurs expliquent cela, en premier lieu la complexité humaine. Les comportements humains sont souvent imprévisibles et influencés par de nombreux facteurs contextuels, sociologiques, culturels, émotionnels et psychologiques.

L'INSÉCURITÉ JURIDIQUE AUTOUR DU DROIT DE LA DONNÉE FRAGILISE LE CONTINUUM DE LA DÉFENSE

L'espace numérique est aujourd'hui un champ de conflictualité. On y mène une guerre ouverte entre États et les réseaux criminels s'y immiscent. Aux attaques de systèmes et à la captation massive de données, s'ajoutent les actions de manipulation. Les stratégies sont à l'image de la doctrine élaborée par le général Guerassimov[17] en 2020. Il y décrit les logiques de guerre informationnelle totale, de combat numérique, d'approche indirecte, de champs immatériels et de combats par proxy où l'innovation et la créativité doivent être stimulées à tous les échelons afin de déstabiliser l'adversaire dans tous les espaces et l'amener à agir systématiquement dans un contexte dégradé.

Dans ce contexte, les États de droit et démocratiques se retrouvent dans un combat asymétrique. Il s'agit de mener une guerre avec les règles du droit commun ; équation insoluble.

En effet, il existe aujourd'hui des vides juridiques autour du droit de la donnée, notamment personnelle, dans le *darkweb* en particulier. On peut alors se poser la question de « pourquoi » et « comment » sécuriser juridiquement la donnée et son exploitation dans toutes les couches de l'Internet afin de protéger les personnes et les organisations ayant fait l'objet de vol de données et exposées à des attaques ciblées. En dépit de l'absence de texte sur le sujet, le principe de précaution s'impose souvent aujourd'hui et conduit à une forme d'auto-blocage, en France en particulier. L'exploitation de la donnée du *darkweb* pourrait selon certains s'apparenter à une forme de recel ; mais dès lors qu'il s'agit de protéger les personnes et les biens, d'informer des personnes déjà attaquées ou menacées, est-ce vraiment contraire à l'esprit de la loi ? N'est-on pas dans une légitimité de l'action par sa finalité ? La question est posée par des experts qui se sont emparés du sujet dans le cadre d'un groupe de travail soutenu par la Chaire Cyber et souveraineté numérique de l'IHEDN ainsi que l'Alliance pour la Confiance numérique[18]. Ce groupe est co-dirigé par le Pr. Michel Séjean[19] et le Dr Emilie

Un autre élément est parfois **le manque de données** ou des données insuffisantes pour parvenir à une conclusion définitive. Troisièmement, les attaquants modifient constamment leurs **méthodes,** ce qui rend le travail de l'analyste très complexe. Enfin la **question des outils** utilisés peut également être soulevée. »

[17] Valeri Vassilievitch Guerassimov est général d'armée et chef de l'État-major des Forces armées de la Fédération de Russie depuis le 9 novembre 2012. Il est également le premier vice-ministre de la Défense.

[18] Créée en 2013, l'Agence pour la Confiance numérique (ACN) représente les entreprises du secteur de la confiance numérique, notamment celles de la cybersécurité, de l'identité numérique et de l'intelligence artificielle de confiance. Organisation professionnelle, elle regroupe des TPE, des PME, des start-ups et des grands groupes. L'originalité de ce collectif permet d'associer les capacités et compétences de chacun pour répondre à tous les défis liés à la confiance numérique.

[19] Michel Séjean est professeur à l'université Paris XIII et chercheur associé à l'IHEDN, spécialiste de droit de la cybersécurité et de droit comparé. Il est également directeur scientifique du Code de la cybersécurité édité par Dalloz. Il est aidé dans ses travaux par de nombreux experts, du droit (particulièrement la Dr Émilie Musso – experte française dans le droit de la donnée numérique), du monde professionnel, de différents ministères et de parlementaires.

Musso, et travaille à l'adoption d'une loi sur le sujet. Selon la Dr Émilie Musso[20], cette nouvelle règle « ne chercherait pas à contraindre davantage, mais au contraire à libérer et sécuriser tant les praticiens de l'*Open Source Intelligence* (OSINT) que ceux qui en sont l'objet, en écartant le risque lié au vide juridique qui aujourd'hui bien souvent paralyse l'action, qu'elle soit publique ou privée, face à une menace débridée et désinhibée.

De manière contre-intuitive, la Commission nationale de l'informatique et des libertés (CNIL) elle-même encourage la démarche alors qu'elle met en évidence dans un récent rapport[21] l'ampleur que prend le vol de données en France et la nécessité de muscler tous les champs de la protection cyber. Aussi, les récents textes européens en matière de cybersécurité impliquent, pour les respecter, de traiter des données issues de fuites de données. C'est le cas par exemple, d'un des règlements délégués complétant le règlement DORA, qui impose aux entités financières de détecter les fuites de données[22] ; le règlement DORA prescrit de traiter les données en sources ouvertes nécessaires aux impératifs de cybersécurité[23], d'obtenir des renseignements sur les cyberattaques, dont les vols de données,[24] et de surveiller[25] ces événements, ce qui implique de traiter des données issues de fuites de données. Quant à la directive NIS 2, elle impose notamment de mettre en place « des outils de cybersécurité pour détecter les cyberattaques »[26]. Puisque les vols de données sont une forme de cyberattaque, il convient au titre de cette directive de traiter les données issues de fuites de données, afin de détecter ces événements.

[20] Ibid 11

[21] En 2024, la CNIL a été notifiée de 5629 violations de données personnelles, soit 20% de plus qu'en 2023. Au-delà de cet accroissement notable, la tendance la plus préoccupante est celle d'une recrudescence de violations de très grande ampleur. En plus des violations sans précédent qui ont concerné les opérateurs du tiers payant, France Travail ou encore la société Free, la CNIL constate que le nombre de violations touchant plus d'un million de personnes a doublé en un an.
En réaction, la CNIL a fait de la cybersécurité un des 4 axes de son plan stratégique 2025-2028.
En pratique, son action se traduit par :

- L'accompagnement des organismes, en produisant des recommandations permettant de protéger les données personnelles au regard de l'évolution de la menace et de l'état de l'art ;
- Des contrôles sur la mise en œuvre des mesures de sécurité par les organismes ;
- L'information et la sensibilisation des particuliers à la cybersécurité pour les rendre acteurs de la protection de leurs données.

[22] Règlement délégué (UE) 2024/1774 de la commission du 13 mars 2024 complétant le règlement (UE) 2022/2554 du Parlement européen et du Conseil par des normes techniques de réglementation précisant les outils, méthodes, processus et politiques de gestion du risque lié aux TIC et le cadre simplifié de gestion du risque lié aux TIC (*RTS on ICT risk management framework*), art. 14, 1°, b) ; art. 34, i).

[23] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011, cons. 56 ; art. 25, 1°.

[24] *Ibid*., art. 3, 15°; art. 13, 1°.

[25] *Ibid*., art. 10, 3°.

[26] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), art. 29.

VERS UNE NÉCESSAIRE STRUCTURATION DE LA RÉPONSE DANS UN CONTINUUM DE LA SÛRETÉ[27]

Penser le cyberespace comme un objet « sociotechnique » invite à débusquer derrière l'ensemble des dispositifs technologiques qui le compose une dimension sociale et politique, et à le considérer comme un produit humain. On aurait tort d'imaginer que les solutions techniques permettront de faire face aux différentes échelles de menaces auxquelles les organisations, entreprises ou États doivent répondre dans un nouvel environnement. Le comportement des utilisateurs y est essentiel et doit être pris en compte, notamment leur empreinte et leur vulnérabilité numériques. L'analyse des questions de cybersécurité demanderait donc d'articuler de manière systématique les approches sociales, humaines et techniques[28]. La cybersécurité revêtant un aspect stratégique, elle devrait être appréhendée au plus haut de la direction d'une organisation[29]. Visions managériales, opérationnelles et technologiques devraient effectivement converger.

En observant la plupart des entreprises du CAC 40[30], les états-majors des armées occidentales[31], ou même les États, il n'existe pas vraiment d'approche globale[32], alors que le risque cyber est aujourd'hui la combinaison du risque numérique et du risque informationnel, contexte où le facteur humain est devenu le vecteur de la menace.

Ainsi, les pistes à explorer dans la structuration de la réponse pourraient être une implication et un appui forts des cadres dirigeants publics et privés, la transversalité de la cybersécurité,

27 Cette notion de continuum de la sûreté face aux risques humains, cyber et guerres d'influence, est évoquée et illustrée le 20 mai 2025 par Anne Tricaud (Head of Security – Airbus), le général (2S) Stéphane Dupont (directeur de la sûreté de NavalGroup), Chloé Debièvre (spécialiste en influence et lutte informationnelle) et Émilie Bonnefoy (Open Sezam) lors de leur intervention dans le cadre de l'émission RiskIntelMedia, animée par Yasmine Douadi.

28 Amaël Cattaruzza et Jérémy Buisson, *La dimension sociotechnique du cyberespace*, dans *La cybersécurité*, 2e édition, 2023, Armand Colin.

29 Comme bien des aspects, comme la simplification organisationnelle ou les processus de transformation, s'il n'existe pas un *sponsorship* fort, les efforts à déployer seront considérables pour des résultats modestes.

30 Lorsque l'on décortique en France l'organisation de la cybersécurité dans les entreprises du CAC 40, on trouve les fonctions suivantes, à différents niveaux de responsabilité : *chief information officer (CIO), chief technology officer (CTO), chief data officer (CDO), chief security officer (CSO), chief information security officer (CISO) et data protection officer (DPO)*. De nombreuses dimensions sont prises en compte, mais le facteur humain et les aspects informationnel-communicationnel en sont le grand absent.

31 Cette segmentation dans le secteur privé est aussi présente au sein de la plupart des armées occidentales, de l'OTAN, où de nombreuses fonctions agissent encore en silo, à l'image des différentes fonctions au sein d'un état-major interarmées : renseignement (J2), opérations (J3), systèmes d'information et de communication (J6), influence et action d'environnement (J9) auxquelles il faut ajouter la communication opérationnelle (COM OPS) relevant généralement directement du commandement et la lutte informatique d'influence (L2I) relevant quant à elle du niveau stratégique.

32 Il existe pourtant des politiques qui posent les bases d'une structuration comme le plan de sécurité (PSSI) et le plan d'amélioration continue de la sécurité (PACS) de l'ANSSI l'illustrent. Ces deux plans cherchent à structurer la réponse selon quatre piliers : gouvernance, protection, défense et résilience. Au sein de la gouvernance, l'ANSSI mentionne la gestion du facteur humain (sensibilisation et entraînements), mais les questions informationnelle et cognitive sont éludées.

le partage de l'information[33], le chaînage des champs numérique, informationnel et communicationnel, la prise en compte des facteurs humains dans toute leur acception et des capacités duales, afin de se protéger et agir dans ce continuum cyber – numérique – informationnel – cognitif, porteur d'un continuum de la sûreté.

Le facteur humain, central, est *in fine* le problème, mais aussi la solution.

[33] Lors du *Paris Cyber Summit* du 3 au 5 juin 2024, il a été soulevé la question du partage de l'information, au sein d'un État comme à l'international, entre public et privé, dans ce que l'on pourrait qualifier de « cercles de confiance ». Ce partage de l'information, encore insuffisant, pourrait être une première étape au décloisonnement. La directive NIS 2 invite les États membres de l'UE à renforcer ce partage.

L'expertise stratégique en toute indépendance

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

2 bis, rue Mercœur - 75011 PARIS / France
+ 33 (0) 1 53 27 60 60
contact@iris-france.org

iris-france.org

L'IRIS, association reconnue d'utilité publique, est l'un des principaux think tanks français spécialisés sur les questions géopolitiques et stratégiques. Il est le seul à présenter la singularité de regrouper un centre de recherche et un lieu d'enseignement délivrant des diplômes, *via* son école IRIS Sup', ce modèle contribuant à son attractivité nationale et internationale.

L'IRIS est organisé autour de quatre pôles d'activité : la recherche, la publication, la formation et l'organisation d'évènements.