Évolution des menaces de cybersécurité en 2025

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

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

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

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

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

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

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

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

La montée en puissance des acteurs de la menace

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

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

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

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

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

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

Des chaînes de dépendance devenues cibles stratégiques

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

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

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

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

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

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

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

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

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

Technologies émergentes : opportunités et nouvelles vulnérabilités

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

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

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

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

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

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

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

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

On pourrait explorer d'autres domaines émergents :

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

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

Le droit entre incertitudes et leviers de cybersécurité

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

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

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

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

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

Conclusion

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

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

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