PERSPECTIVES **STRATÉGIQUES**

LE REGARD DU COMITÉ
ESPACE & AÉRONAUTIQUE
DES JEUNES IHEDN
POUR AIRBUS DEFENCE AND SPACE

8 CONTRIBUTIONS
POUR ÉCLAIRER
LES DÉFIS DE DEMAIN

LES JEUNES IHEDN

AIRBUS
DEFENCE AND SPACE

PRÉAMBULE

Chers lecteurs,

En vos mains se trouve Perspectives Stratégiques, premier ouvrage de pensée stratégique du comité Aéronautique et Espace des Jeunes IHEDN, né d'un partenariat avec Airbus Defence and Space.

Nous avons voulu donner à des étudiants et jeunes professionnels l'opportunité de partager, à travers différents angles d'approche, leur vision sur la Cybersécurité et l'Espace, des thèmes devenus des enjeux de souveraineté très concrets. De plus, à l'heure de l'intelligence artificielle et des nouveaux risques qui lui sont associés, des questionnements concernant la coopération entre États sont notamment abordés au sein de cet ouvrage. Que ce soit d'un point de vue opérationnel, juridique, économique ou géopolitique, les rédacteurs construisent des analyses tournées vers l'avenir, interrogeant les choix qui s'offrent dès aujourd'hui à l'Europe pour construire son autonomie stratégique.

Le comité Aéronautique et Espace tient à remercier Airbus Defence and Space pour ce partenariat noué depuis plusieurs années, et en particulier Nicole Anschutz, qui a permis non seulement de faire découvrir les engagements du groupe à Élancourt, mais aussi de nouer un lien durable entre notre comité et un acteur majeur de la défense européenne.

Enfin, un grand merci à Métisse Clain, responsable publication au sein du comité Aéronautique et Espace des Jeunes IHEDN pour la supervision des articles et Chloé Goboyan pour la mise en page, ainsi qu'à tous les rédacteurs, sans qui cet ouvrage n'aurait pas été possible.

Il ne vous reste plus qu'à vous laisser porter par ces pages, et à vous interroger, à votre tour, sur les enjeux de l'Espace et de la Cybersécurité.

Comme le disait Antoine de Saint-Exupéry *: « Pour ce qui est de l'avenir, il ne s'agit pas de le prévoir, mais de le rendre possible ».* C'est dans cette dynamique que le comité Aéronautique et Espace des Jeunes IHEDN et ses rédacteurs vous invitent à réfléchir, avec eux, à cet avenir.

Bonne lecture !

Sancie Kergall-Gayet
Responsable du comité Aéronautique et Espace des Jeunes IHEDN

AVERTISSEMENT

Les textes publiés dans le présent ouvrage n'engagent que la responsabilité de leur auteur. Les idées ou opinions émises ne peuvent être considérées comme l'expression d'une position officielle.

SOMMAIRE

Rédigé par : Louise JOBIT

L'ESPACE, UN NOUVEL ENVIRONNEMENT AUX ENJEUX STRATÉGIQUES DE SOUVERAINETÉ

Le 4 octobre 1957 s'ouvre une nouvelle page pour l'humanité : la conquête de l'espace. Placée dans un contexte de bipolarité entre l'URSS et les États-Unis, la guerre froide a permis de grandes avancées, particulièrement dans le domaine de la course à l'espace. Ainsi, le premier vol spatial orbital de l'Histoire, effectué par le satellite soviétique *Spoutnik 1*, pose la première pierre d'un domaine infini qui ne demande qu'à être exploré. Les années qui suivirent furent riches en avancées, amenant l'être humain dans ce tout nouvel environnement.

Aujourd'hui, près de six décennies plus tard, nos connaissances du spatial n'ont cessé de croître, et notre relation à ce nouvel environnement a fortement évolué. Autrefois lieu de recherches et de découvertes, il est à présent devenu un nouveau terrain d'influence mondiale au sein duquel s'affrontent les grandes puissances. Les technologies spatiales se sont ainsi développées, passant de l'exploration scientifique des planètes à des usages davantage commerciaux (via, par exemple, les satellites de communication) ou militaires.

Nous exposerons dans un premier temps les avancées qu'a permises l'arrivée de l'Intelligence Artificielle (IA) générative dans le milieu spatial, ainsi que la nouvelle perception que les acteurs privés comme publics apportent à cet environnement. Dans un deuxième temps, nous nous intéresserons à la question de la géopolitique spatiale, avant d'opérer un focus particulier sur le cas européen. Enfin, nous ouvrirons notre réflexion à une analyse plus critique en nous questionnant sur l'avenir de l'espace face aux nouveaux enjeux dont il est le protagoniste.

L'intelligence artificielle et l'ouverture des possibles

L'Intelligence Artificielle (IA) n'est pas un outil récent. Employée pour la première fois en 1956 lors de la conférence de Dartmouth, qui marqua le début de la recherche scientifique dans ce domaine, elle n'a cessé d'évoluer et de se développer jusqu'à nos jours. Les dernières décennies ont été

particulièrement fructueuses en termes d'innovations, et l'apparition de l'IA générative en 2020 s'intègre pleinement dans cette dynamique.

Avec le développement du *New Space* depuis les années 2000, force est de constater que l'humanité se tourne de manière croissante vers l'espace, possédant dorénavant les moyens nécessaires pour partir à la découverte de ce nouvel environnement.

Ouvrant un champ des possibles infini dans un milieu que nous n'avons que trop rêvé de découvrir sans pour autant le pouvoir, il s'intègre à présent dans notre réalité. Se caractérisant par une démocratisation de l'accès à l'espace, une réduction des coûts et une participation accrue d'acteurs privés (tels que SpaceX ou Blue Origin), ce mouvement repose sur des bases d'agilité et d'innovation au sein desquelles l'IA occupe un rôle de plus en plus central.

Son utilisation permet de rendre les missions plus autonomes, économiques et innovantes, ouvrant ainsi la voie à des projets de datacenters orbitaux portés par des acteurs privés et publics, projets que nous aurions perçus comme futuristes il y a encore quelques années. Le *New Space* offre de nombreuses possibilités d'innovation et d'optimisation des moyens existants, mais l'usage de l'IA permet d'alléger certaines contraintes rencontrées auparavant, offrant une plus grande flexibilité d'action secondée par la machine. Toutefois, toutes ces avancées ont profondément transformé le milieu de la conquête spatiale et les enjeux géopolitiques associés, métamorphosant cet environnement en un terrain de rivalité économique, technologique et militaire entre les grandes puissances et les nouveaux acteurs.

Géopolitique spatiale

Au-delà des avancées réalisées dans le domaine de la recherche, l'espace est devenu un pivot des relations internationales mondiales, au sein desquelles la France s'impose comme l'un des leaders. Qu'il s'agisse du domaine militaire ou civil, l'espace est devenu un théâtre majeur des enjeux stratégiques mondiaux. Cela s'est traduit, en septembre 2019, par la création par le président de la République Emmanuel Macron d'un grand Commandement de l'espace au sein de l'Armée de l'air, devenue depuis l'Armée de l'air et de l'espace. Suivant cette trajectoire, la géopolitique ne se joue à présent plus seulement sur Terre : à l'avenir, certains conflits et guerres d'influence se dérouleront probablement au-dessus de nos têtes.

Actuellement, on observe une réorganisation des rapports de force entre les grandes puissances, marquée par de nouvelles ambitions, notamment de la part de la Chine. Celle-ci affiche une volonté hégémonique visant à devenir la première puissance spatiale d'ici 2045, en contournant les alliances occidentales telles que les accords Artemis. Cette stratégie comporte des risques majeurs, en particulier en matière de course à l'armement et de cyberattaques ciblant les infrastructures spatiales occidentales. Elle souligne également la diplomatie agressive de Pékin, qui propose des coopérations ciblées pour isoler les États-Unis et l'Europe.

Sur le continent asiatique également, la Russie tente de développer des systèmes d'armement spatiaux, tels que des satellites tueurs ou des lasers antisatellites. Cependant, son budget restreint et les sanctions occidentales réduisent le champ d'action de Moscou, rendant sa pérennité spatiale dépendante de ses partenariats avec la Chine.

L'Europe, quant à elle, reste guidée par une vision de souveraineté. Toutefois, bien qu'elle dispose du lanceur Ariane 6 et du système de positionnement Galileo, elle accuse un certain retard face aux mégaconstellations de ses concurrents et face à la réduction des coûts de lancement. De son côté, la France mise sur l'innovation (nanosatellites, IA, surveillance de l'espace) via le Centre National d'Études Spatiales (CNES) et le Commandement de l'Espace (CDE), tout en privilégiant des alliances ciblées avec des acteurs émergents comme les Émirats arabes unis et l'Inde.

Focus sur le cas européen

Le cas européen est complexe, car l'Union européenne se compose d'une multiplicité d'acteurs. Cependant, les nombreux désaccords entre les États membres, notamment sur les budgets et les priorités, fragilisent son autonomie face à des géants toujours plus compétitifs et déterminés à conserver leur position hégémonique. Entre héritage industriel, ambition d'autonomie et défis géopolitiques, l'Europe conserve un rôle clé dans la conquête spatiale. Elle s'appuie sur des programmes d'envergure (Galileo, Copernicus, Ariane 6), des agences nationales (CNES en France, DLR en Allemagne, ASI en Italie) et des industriels majeurs (Airbus Defence and Space, Thales Alenia Space, ArianeGroup) qui occupent une place centrale dans la défense des intérêts spatiaux européens.

Comme le montre l'évolution actuelle du monde, l'espace représente, au-delà des ressources qu'il recèle, un environnement central pour les relations internationales, ce qui en fait un espace stratégique à protéger afin de faire valoir les intérêts de chaque puissance. C'est dans cette optique que sont élaborés

de nombreux programmes de défense, à l'instar de la Stratégie spatiale de l'UE pour la sécurité et la défense, qui vise à réduire la dépendance envers les États-Unis et la Chine, à protéger les satellites contre les cyberattaques ou les missiles antisatellites (ASAT), et à coordonner les capacités spatiales des États membres.

L'Europe possède les capacités industrielles et technologiques nécessaires pour s'affirmer comme un acteur de premier plan dans cet ordre mondial en cours de restructuration. Cependant, son avenir dépendra avant tout de sa capacité à se rassembler et à coordonner ses forces pour s'affirmer face aux géants qui se dressent devant elle.

Le revers de la médaille

La conquête spatiale est en train de rebattre les cartes de l'ordre mondial établi depuis plusieurs décennies. Si, à l'origine, les avancées scientifiques et la coopération internationale étaient privilégiées dans ce nouvel environnement, c'était sans compter sur la nature belliqueuse de l'homme. Bien que les traités internationaux se soient multipliés et les relations bureaucratisées, les conflits récents en Ukraine ou les tensions en Iran nous prouvent que nous ne sommes pas à l'abri de nouvelles rivalités majeures. Alors que, lors des deux guerres mondiales, les soldats s'affrontaient de manière directe, les moyens actuels sont beaucoup plus indirects et destructeurs (drones autonomes) et se déploient sur des champs de bataille divers.

Le numérique, qui fait désormais partie intégrante de nos vies, constitue un nouveau terrain d'action capable de paralyser un pays. Ce fut le cas le 8 janvier 2026, lorsque les autorités iraniennes ont imposé un black-out numérique généralisé lors de manifestations nationales afin de limiter la diffusion d'informations. L'idée de conflits spatiaux, qui n'occupait autrefois que l'imaginaire des amateurs de science-fiction, pourrait bien devenir une réalité tangible. L'avenir des conflits se jouera sur des champs de bataille virtuels et spatiaux, ces deux secteurs étant étroitement liés.

Bien que théoriquement soumis au droit international, les rapports d'influence se déploient désormais au-dessus de nos têtes. Avec des satellites capables de cartographier la Terre ou de géolocaliser n'importe quel individu, les risques de détournement à des fins de surveillance ou d'espionnage international sont majeurs. Si certains satellites permettent d'aider les populations et les autorités en cartographiant des incendies ou des crues pour accélérer l'intervention des secours, qu'en

serait-il si ces mêmes outils étaient systématiquement utilisés pour surveiller des bases militaires et des centres de pouvoir ?

L'avènement du *New Space* et la privatisation de l'espace par des firmes commerciales nous poussent également à nous questionner sur la gouvernance de ce milieu de plus en plus concurrentiel. Ne risquons-nous pas, en investissant ce nouvel environnement vierge de toute influence humaine historique, de reproduire les vices et les erreurs commis sur Terre que nous tentons aujourd'hui de réparer ?

Conclusion

En somme, l'espace est devenu un pilier de souveraineté et de puissance dont l'importance ne cessera de croître dans les années à venir, une dynamique accélérée par les avancées de l'intelligence artificielle et l'essor du *New Space*. Sans basculer dans une paranoïa ou une défiance totale envers l'intelligence artificielle, il convient de rester lucide face aux risques qu'elle comporte. Si cette transformation rapide crée de nouvelles opportunités, elle engendre également d'importantes vulnérabilités.

L'espace n'est plus un environnement abstrait entourant la Terre ; il fait désormais partie intégrante de notre réalité quotidienne. Ainsi, la nécessité de préserver ce milieu devient primordiale. Conformément au droit international en vigueur, l'espace doit demeurer un terrain de coopération mondiale au sein duquel toute revendication de souveraineté sur l'espace extra-atmosphérique (y compris la Lune et les autres corps célestes) est prohibée (au-delà de l'espace de très haute altitude, ou THA, situé entre 20 et 100 km d'altitude).

Ce cadre juridique garantit également l'utilisation pacifique de l'espace et la responsabilité des États vis-à-vis de leurs activités privées, ce qui laisse toutefois apparaître des brèches exploitées par le *New Space*. L'usage de l'espace doit rester pacifique, tout en exigeant le déploiement d'une stratégie de souveraineté pour éviter de subir le diktat des autres puissances.

Notre ouverture sur ce nouvel environnement rebat totalement les cartes de l'ordre mondial. Les enjeux stratégiques soulevés par ce nouveau milieu laissent la porte ouverte à de nombreuses questions. Un choix collectif s'impose désormais : d'un côté, un espace militarisé et fragmenté ; de l'autre, un espace gouverné et coopératif. C'est aujourd'hui que cette décision doit être prise, et l'issue dépendra des choix immédiats en matière de régulation de l'IA, de coalitions et de doctrines stratégiques.

À propos de l'autrice : Après avoir effectué son lycée au Prytanée national militaire de La Flèche (1189E), Louise est actuellement étudiante en troisième année de sciences politiques à l'institut d'études politiques de Fontainebleau. Grâce au programme ERASMUS+, elle a pu suivre pendant une année les cours du master Public and cultural diplomacy à l'Università degli studi di Siena. Elle est également réserviste opérationnel pour le Service de Santé des Armées.

Rédigé par : Kimberley MERLET

QUELS MODÈLES D'ARCHITECTURE POUR LE RENSEIGNEMENT SPATIAL EUROPÉEN À L'ÈRE DE L'IA EMBARQUÉE D'ICI 2040 ?

L'exploitation des données issues des capacités spatiales occupe une place croissante dans la conduite des opérations militaires. Toutefois, les architectures actuelles, majoritairement fondées sur un traitement au sol, atteignent aujourd'hui leurs limites en matière de latence, de volume et de réactivité[1]. Cette tension s'explique notamment par la difficulté à produire rapidement un renseignement exploitable, les systèmes générant un grand volume de données peu ciblées qu'il est ensuite nécessaire de trier et d'analyser.

Dans ce contexte, l'intégration de l'intelligence artificielle directement à bord des systèmes spatiaux apparaît comme une évolution structurante. Elle permet notamment d'opérer un tri des données en amont, de détecter des anomalies et de prioriser les informations, déplaçant ainsi une partie critique du traitement et de la décision au plus près du capteur, et contribuant à accélérer et fluidifier la chaîne décisionnelle[2].

Ces transformations interrogent en profondeur les modèles d'organisation du renseignement spatial en Europe, en déplaçant la question de la souveraineté du seul accès à la donnée vers le contrôle de son traitement et de son interprétation, et ouvrent la voie à une reconfiguration possible de ses architectures à l'horizon 2040. Une dynamique qui s'inscrit d'ailleurs dans des initiatives déjà engagées à l'échelle européenne, à l'image du programme IRIS², qui vise à structurer des infrastructures spatiales sécurisées à usage gouvernemental, contribuant à la fois aux enjeux de sécurité et, dans une certaine mesure, de défense[3], bien que le renseignement demeure encore largement structuré à l'échelle nationale.

---

[1] « Au cœur de la transformation numérique », *Thales Alenia Space*, [en ligne], consulté en avril 2026. URL : https://www.thalesaleniaspace.com/fr/au-coeur-de-la-transformation-numerique

[2] « L'intelligence artificielle, un levier de supériorité stratégique pour les armées », *INAS France*, [en ligne], consulté en avril 2026. URL : https://inas-france.fr/lintelligence-artificielle-un-levier-de-superiorite-strategique-pour-les-armees/

[3] Règlement (UE) 2023/588 du Parlement européen et du Conseil du 15 mars 2023 établissant le programme de l'Union pour une connectivité sécurisée pour la période 2023-2027, Journal officiel de l'Union européenne, 17 mars 2023.

Variables

Cette étude prospective, suivant une méthodologie inspirée des travaux des Jeunes IHEDN, repose sur l'identification de deux variables à fort impact et à forte incertitude. Ces variables ont été retenues en raison de leur capacité à structurer les architectures de renseignement spatial et à produire des trajectoires contrastées. Bien que le degré d'intégration européenne puisse influencer le développement de l'IA embarquée, ces deux variables ne sont pas strictement dépendantes et peuvent évoluer selon des logiques distinctes, justifiant leur traitement séparé.

Degré d'intégration européenne du renseignement spatial

La première variable déterminant le futur des architectures spatiales intégrant l'IA est le degré d'intégration européenne du renseignement spatial, qui peut être envisagé selon deux orientations polarisées.

La première correspond à une fragmentation nationale. Celle-ci suppose un repli des États européens, caractérisé par une souveraineté forte des données et une absence de partage structuré. Dans cette configuration, les capacités de renseignement demeurent essentiellement nationales, reposant sur des architectures cloisonnées et faiblement interopérables, limitant ainsi la circulation et l'exploitation conjointe de l'information.

À l'inverse, la seconde orientation repose sur une intégration renforcée à l'échelle européenne. Elle se traduit par la mise en place d'une architecture commune, fondée sur la mutualisation des données, l'adoption de standards partagés et l'émergence de mécanismes de gouvernance collective. Une telle configuration permettrait d'améliorer l'interopérabilité des systèmes, de fluidifier le partage de l'information et de renforcer la capacité des États européens à produire un renseignement exploitable de manière coordonnée.

Niveau d'autonomie de l'IA embarquée

La seconde variable déterminante concerne le niveau d'autonomie de l'IA embarquée au sein des systèmes spatiaux.

Une IA limitée renvoie à des fonctions d'assistance, telles que le tri des données, le filtrage ou la détection d'anomalies simples, dans lesquelles la décision demeure entièrement humaine. Dans ce cadre, l'IA agit comme un outil d'aide à l'analyse, sans transformation majeure de la chaîne décisionnelle.

À l'inverse, une IA avancée désigne des systèmes capables d'analyser des flux de données complexes, d'identifier des schémas comportementaux et de générer des alertes en temps quasi réel. En réduisant significativement le temps entre détection et décision, elle contribue à transformer la chaîne de production du renseignement, en renforçant la réactivité et l'autonomie des systèmes.

Quatre scénarios d'évolution à l'horizon 2040

Une Europe fragmentée et une IA limitée

Année 2040. Les pays européens se replient sur eux-mêmes face à un environnement international instable, privilégiant la protection de leurs intérêts propres. Les capacités de renseignement spatial restent largement nationales, avec un faible niveau d'interconnexion. Dans ce contexte, le développement de l'IA embarquée demeure limité, en raison de priorités stratégiques divergentes et d'un manque d'investissements coordonnés. Les systèmes reposent principalement sur des fonctions d'assistance, ce qui contraint la capacité d'analyse et allonge les délais de réaction. Faute de coopération structurée, les États européens demeurent dépendants de capacités extérieures, notamment celles de leurs alliés au sein de l'OTAN, sans pour autant bénéficier d'un accès complet et autonome à ces ressources.

Europe fragmentée et IA avancée

Année 2040. Les pays européens évoluent dans une logique de fragmentation, mais font du développement technologique une priorité stratégique. Dans un contexte de compétition accrue, ils investissent massivement dans les technologies disruptives, notamment l'IA embarquée. Chaque État développe ses propres capacités, conduisant à une hétérogénéité des standards et des pratiques, source de frictions opérationnelles et de dépendances technologiques implicites. L'IA est utilisée de manière intensive pour compenser l'absence de coopération, permettant d'améliorer la réactivité et la capacité d'analyse. Cette dynamique favorise l'innovation, mais s'accompagne d'une fragmentation stratégique, limitant l'efficacité collective et rendant difficile toute coordination à l'échelle européenne.

Europe intégrée et IA limitée

Année 2040. Les États européens approfondissent leur coopération en matière de renseignement spatial, conduisant à la mise en place d'une architecture coordonnée reposant sur des standards communs, un partage structuré des données et une gouvernance collective. Dans un contexte de compétition stratégique accrue, cette intégration vise à renforcer la cohérence et l'autonomie des capacités européennes. Toutefois, afin de préserver la confiance entre États et de garantir un contrôle humain sur les décisions critiques, le développement de l'IA embarquée demeure volontairement encadré. Les systèmes privilégient ainsi des fonctions d'assistance, telles que le tri des données et la détection d'anomalies simples. Cette configuration favorise la stabilité et la coordination, mais peut limiter la réactivité face à des acteurs disposant de capacités technologiques plus avancées.

Europe intégrée et IA avancée

Année 2040. Les États européens mettent en place une architecture intégrée de renseignement spatial, fondée sur une forte mutualisation des données issues de sources publiques et privées, ainsi que sur des standards communs. Cette coopération permet le développement d'une IA embarquée avancée, capable d'analyser des flux de données multi-sources, d'identifier des schémas complexes et de générer des alertes en temps quasi réel. La réduction du délai entre détection et décision confère un avantage opérationnel majeur en matière de réactivité et de supériorité informationnelle. Toutefois, cette configuration soulève des enjeux accrus de gouvernance. La centralisation des données et l'automatisation partielle de l'analyse posent la question du contrôle des systèmes, de la répartition de la responsabilité entre États et du maintien d'une supervision humaine sur les décisions critiques.

Enseignements stratégiques

L'élaboration de ces scénarios met en évidence plusieurs enseignements structurants. Tout d'abord, l'avenir du renseignement spatial européen dépend de la capacité des États à dépasser la tension entre souveraineté nationale et intégration, dans un contexte de compétition stratégique accrue.

Ensuite, le développement de l'IA embarquée impose d'arbitrer entre performance technologique et maintien d'un contrôle humain sur les décisions critiques. Si elle constitue un levier d'autonomie

stratégique et de réduction des dépendances extra-européennes, son intégration ne peut être pensée de manière isolée.

Enfin, ces évolutions soulignent l'importance d'une gouvernance adaptée, reposant sur une coordination renforcée entre acteurs étatiques, industriels et privés, afin d'encadrer le développement et l'usage des systèmes automatisés.

À propos de l'autrice : Kimberley Merlet est spécialisée dans l'analyse des enjeux de défense et de sécurité spatiale. Titulaire d'un master en philosophie et d'un mastère spécialisé en défense et sécurité de l'espace, elle s'intéresse aux implications stratégiques des technologies émergentes. Elle est engagée au sein des Jeunes IHEDN, où elle contribue à la production éditoriale au sein du pôle communication et participe aux travaux du comité Aéronautique et Espace.

Rédigé par : Zoé NAMUR

SOPHIE ADENOT LANCÉE PAR SpaceX : ANATOMIE D'UNE DÉPENDANCE STRATÉGIQUE ET LES FONDATIONS D'UNE RÉPONSE EUROPÉENNE

Le 13 février 2026, Sophie Adenot s'envolait vers l'ISS à bord d'un vaisseau américain, depuis un sol américain, propulsé par une fusée américaine. Derrière la fierté tricolore se cache une dépendance structurelle que ni les discours ni les drapeaux ne sauraient effacer. Mais l'Europe n'est pas absente du jeu : elle construit pour la décennie qui vient avec une alliance de 22 nations, des industriels de rang mondial et des programmes d'infrastructure souveraine sans équivalent.

Cet article se propose d'analyser cette dépendance à travers trois prismes complémentaires : le constat opérationnel, l'écart technologique et industriel, et les enjeux géopolitiques qui en découlent. Mais il met aussi en lumière ce que l'Europe construit pour demain car si SpaceX domine le présent, l'ESA et ses partenaires industriels posent les jalons d'une souveraineté spatiale durable et cohérente avec les valeurs et les intérêts européens.

Le symptôme Adenot : une dépendance structurelle

Le 13 février 2026, la spationaute française Sophie Adenot s'est envolée vers l'ISS à bord du Crew Dragon Freedom de SpaceX, depuis Cap Canaveral, en Floride. Un départ historique pour la France et en même temps une image qui interroge : pourquoi une astronaute portant le drapeau tricolore part-elle depuis le sol américain, propulsée par une fusée américaine ?

Ce n'est pas une anomalie isolée. Depuis 2020, tous les astronautes européens ont décollé à bord de vaisseaux SpaceX : Thomas Pesquet (2021 Alpha), Matthias Maurer (2021 Cosmic Kiss), Samantha Cristoforetti (2022 Minerva), et désormais Sophie Adenot (2026 mission εpsilon). L'ESA forme et sélectionne ses astronautes, gère leurs expériences à bord, coordonne la science mais ne les lance pas. Elle dépend intégralement d'un opérateur privé américain pour accéder à l'espace habité.

Cette situation est le fruit d'un choix politique de 2009 : les États membres de l'ESA ont collectivement renoncé à développer un véhicule habité européen, jugeant le coût prohibitif et la rentabilité incertaine. À la même époque, SpaceX commençait le développement du Dragon. La NASA,

confrontée à l'arrêt du Space Shuttle en 2011, a externalisé le transport vers l'ISS ouvrant un marché que l'Europe n'a jamais tenté de conquérir. L'écart s'est creusé à une vitesse que personne n'avait anticipée.

La mission εpsilon de Sophie Adenot, dont le nom fait référence à l'infiniment petit en mathématiques et à la cinquième étoile la plus brillante d'une constellation incarne cette dualité. À bord de l'ISS, elle mène des expériences de premier plan : adaptation du corps à la microgravité, échographies assistées par réalité augmentée (EchoFinder), et des dizaines de protocoles scientifiques menés en coopération internationale. La science avance, ambitieuse et reconnue même si le lanceur n'est pas européen. Mais cette réalité ne saurait masquer la question structurelle qui demeure entière.

Falcon 9 vs Ariane 6 : deux visions de l'espace

L'écart capacitaire illustre deux approches radicalement différentes. SpaceX a fait de la réutilisabilité et de la cadence son modèle économique. L'Europe a poursuivi la logique du lanceur jetable, optimisée pour la fiabilité institutionnelle mais inadaptée à la compétition commerciale des années 2020. Il serait réducteur de résumer Ariane 6 à un retard. Cinq vols réussis en moins de 18 mois, deux configurations (A62 et A64 avec moteur Vinci réallumable), une montée en cadence réelle vers 2027.
Le problème n'est pas la qualité technique du lanceur, c'est l'inadéquation avec un marché que SpaceX a restructuré à sa vitesse. C'est un défi de modèle économique autant que technologique, et ArianeGroup en est pleinement conscient.

L'atout européen : un écosystème industriel de premier plan

Là où l'analyse s'arrête souvent au constat de retard, elle omet un fait fondamental : l'Europe dispose d'un tissu industriel spatial et de défense parmi les plus compétents et les plus diversifiés au monde. Aucun acteur unique, pas même SpaceX, ne couvre un spectre aussi large : propulsion, satellites, observation, navigation, cybersécurité, défense.

Industriel	Rôle spatial & défense	Poids mondial
ArianeGroup	Maître d'œuvre Ariane 6, lanceurs civils & militaires	1er lanceur institutionnel européen
Airbus Defence & Space	Satellites, observation Terre, Télécom, Stations sol, Modules ISS (Columbus), Exploration spatiale (JUICE, BepiColombo, Solar Orbiter, ExoMars avec Thales Alenia Space, Rosetta, VenusExpress, MarsExpress), Navigation avec Galileo 2e génération, EGNOS	Top 3 mondial fabricants satellites
Thales Alenia Space	Lunar Gateway (ESPRIT), surveillance	Maître d'œuvre module ESPRIT
Thales Group	Communications sécurisées, Cybersécurité spatiale, défense	Leader défense & sécurité européen
Dassault Aviation	Systèmes embarqués, Rafale (Intégration spatiale), drones	Aviation de combat souveraine française
Safran	Motorisation Vulcain & Vinci, navigation inertielle spatiale	Propulsion d'Ariane 6

Tableau 2 — Champions industriels européens du spatial & de la défense

La chaîne industrielle européenne couvre l'ensemble du spectre spatial : de la propulsion à la charge utile, de l'observation Terre aux télécommunications sécurisées, des lanceurs aux systèmes de navigation. C'est un atout collectif que peu de régions dans le monde peuvent revendiquer et qui constitue le socle sur lequel une souveraineté spatiale européenne peut réellement être bâtie. 22 États membres, des programmes sur plusieurs décennies, une légitimité multilatérale unique : voilà ce que SpaceX ne peut pas reproduire. Quand un opérateur privé américain subit une pression politique de Washington, l'ESA peut maintenir une trajectoire indépendante.

C'est précisément ce que signifie la souveraineté et c'est ce que l'ESA construit patiemment pour la décennie qui vient :

› **Galileo :** 28+ satellites opérationnels, précision supérieure au GPS — navigation souveraine pleinement déployée.

› **Copernicus :** plus grand programme d'observation de la Terre au monde, données ouvertes accessibles à tous.

› **IRIS² :** future constellation souveraine (6 Mds€, déploiement 2029–2030), conçue comme alternative gouvernementale à Starlink.

› **Lunar Gateway :** Thales Alenia Space maître d'œuvre du module ESPRIT — l'Europe vise la Lune et au-delà.

Les enjeux géopolitiques de la dépendance spatiale

La souveraineté spatiale repose sur trois piliers interdépendants, tous fragilisés : l'accès indépendant à l'espace (le vol habité dépend entièrement de SpaceX), l'autonomie décisionnelle (les délais et charges utiles sont soumis à des décisions américaines), et le contrôle des données et des infrastructures (navigation, observation, communication).

L'exemple le plus frappant est la bataille des constellations en orbite basse. Starlink dépasse 9 300 satellites actifs fin 2025, sa démonstration d'utilité militaire en Ukraine a radicalement changé la perception des décideurs du monde entier. L'Europe répond avec IRIS², mais avec plusieurs années de retard sur un marché que Starlink a déjà structuré à son avantage. Un paradoxe révélateur illustre cette situation : Arianespace lance des satellites Amazon Kuiper (18 contrats sécurisés) pour financer le lanceur qui devra demain défendre la constellation européenne souveraine.

Ce paradoxe n'est pas qu'économique : il traduit une tension profonde entre les urgences du court terme financer Ariane 6 via des lancements commerciaux et les exigences du long terme, bâtir une infrastructure spatiale qui ne dépende pas des décisions prises à Seattle ou à Hawthorne. Trancher cette tension est précisément le rôle des États membres de l'ESA, réunis en Conseil ministériel.

Conclusion : Reprendre la clé du pas de tir

La mission de Sophie Adenot est une réussite humaine et scientifique indiscutable. Mais derrière la fierté nationale, elle révèle une réalité que l'Europe ne peut plus différer : la dépendance spatiale n'est

pas un détail technique, c'est une question de puissance et d'autonomie stratégique. SpaceX domine le présent, c'est un fait. Mais l'Europe dispose des cerveaux, des industriels, des programmes et du cadre politique pour construire une souveraineté durable. Ce qui lui manque encore, c'est l'urgence stratégique collective.

Trois leviers s'imposent avant 2027 : investir massivement dans la cadence et la réutilisabilité d'Ariane 6, en s'appuyant sur ArianeGroup et Safran pour la prochaine génération de lanceurs ; accélérer IRIS² pour une infrastructure de connectivité souveraine opérationnelle avant 2030 ; et ouvrir sérieusement le dossier du transport humain européen non plus comme un horizon lointain, mais comme un objectif stratégique de décennie, mobilisant Airbus, Thales, Dassault et l'ensemble de l'écosystème.

Le départ de Sophie Adenot depuis Cape Canaveral ne sera peut-être pas le dernier. Mais il devrait être le dernier que l'Europe accepte sans en tirer les conséquences politiques et industrielles qui s'imposent. L'espace n'est pas qu'une frontière scientifique : c'est un espace de puissance, d'infrastructure et d'autonomie. Et pour l'instant, l'Europe y est locataire. Mais elle construit sa propre maison, satellite après satellite, lancement après lancement.

À propos de l'autrice : Étudiante en deuxième année de Relations Internationales à L'ILERI, Zoé Namur s'intéresse particulièrement aux prochains grands défis géopolitiques extra-atmosphériques. Son domaine d'étude se concentre sur les enjeux de pouvoir et de souveraineté liés à la compétition étatique, à la privatisation de l'espace et au vide juridique international. Dans le cadre de son cursus, elle a rédigé un article de recherche sur le secteur spatial afin d'analyser les dynamiques géopolitiques de ce domaine en pleine évolution, au cœur des ambitions des grandes puissances mondiales.

Rédigé par : Fériel TAKLIT

LA MISE EN PLACE D'UNE CONSTELLATION EUROPÉENNE SOUVERAINE, CONDITION INDISPENSABLE À L'AUTONOMIE STRATÉGIQUE FACE AUX PUISSANCES EXTRA-EUROPÉENNES

Le 24 février 2022, au premier jour de l'invasion russe de l'Ukraine, des cyberattaques coordonnées neutralisaient les terminaux du réseau satellitaire KA-SAT, avec pour objectif de paralyser les communications militaires ukrainiennes. Face à cela, le 26 février 2022, Elon Musk active son service internet par satellites, nommé Starlink, afin d'assurer la continuité des télécommunications. Ainsi, cette aide ne vient pas d'un satellite européen mais d'un réseau de la société privée américaine SpaceX. Quelques semaines plus tard, Elon Musk reconnaissait avoir refusé d'activer sa couverture au-dessus de la Crimée pour empêcher les drones ukrainiens de détruire la flotte de Moscou. Cette décision unilatérale d'un chef d'entreprise privé américain sur des opérations militaires aux portes de l'Union européenne, sans mandat ni contrôle européen, peut poser question. En d'autres termes, elle montre la vulnérabilité stratégique européenne sur son territoire.

Ce constat révèle une vulnérabilité structurelle : pendant que les États-Unis, la Chine et la Russie ont fait de la maîtrise orbitale un attribut constitutif de leur souveraineté, l'Europe demeure dépourvue d'architecture militaire spatiale cohérente pour être un contrepoids efficace et redouté. Ainsi, sans constellation souveraine, l'Europe peut-elle encore prétendre à une autonomie stratégique crédible face aux puissances extra-européennes ?

Cet article soutiendra que la construction d'une constellation militaire souveraine européenne est une nécessité à la fois technologique, opérationnelle et juridique. La première partie consiste en une analyse de la militarisation de l'espace, avant de voir les prémices d'une constellation européenne souveraine

La militarisation de l'espace

L'espace, nouveau terrain de démonstration de puissance

L'espace est devenu au XXI^{e} siècle le théâtre où s'exercent les rapports de force entre grandes puissances. Accentué par les récents conflits avec la guerre en Ukraine, ou encore la guerre en Iran,

l'espace devient un atout stratégique au service du militaire. En février 2026, deux engins spatiaux russes hautement secrets, Luch/Olymp-et-2, ont intercepté les communications d'au moins une douzaine de satellites européens importants. Cette menace russe atteste d'une conviction partagée par tous, celle de la supériorité orbitale qui conditionne désormais la supériorité opérationnelle terrestre, maritime et aérienne.

Ainsi, l'espace n'est plus un sanctuaire scientifique pour aller simplement étudier la Lune ou des orbites autour, mais devient un domaine de compétition stratégique à part entière dans le domaine militaire. Cette militarisation se manifeste par des menaces concrètes sur le territoire européen. En janvier 2023, le satellite chinois de renseignement TJS-14 s'est positionné en plein milieu des constellations des pays européens, notamment les satellites militaires français dénommés Syracuse, dans le but de collecter des informations. Depuis 2022, un bulletin d'alerte de l'Agence européenne de sécurité aérienne révèle que, depuis le début de l'invasion de l'Ukraine, l'armée russe ne cesse de brouiller les signaux GNSS[4] de navigation par satellite, perturbant le GPS[5] et Galileo, non seulement en zone de conflit, mais aussi dans les pays voisins comme la Pologne, en mer Baltique, à l'est de la Finlande, en mer Noire, ou encore en Méditerranée orientale.

Par ailleurs, la cheffe de la marine suédoise concernant la mer Baltique évoque une navigation fantôme de plus en plus importante des navires civils suédois qui désactivent leur système AIS[6] à cause des interférences, rendant ainsi leur identification et leur suivi plus complexes et augmentant les risques d'accident. Enfin, la guerre des douze jours opposant l'Iran, Israël et les États-Unis, en juin 2025, montre que les États européens ont suivi les événements quasi exclusivement via des renseignements américains et israéliens. L'Europe n'avait pas de capacité autonome d'évaluation en temps réel de la situation dans une zone qui est directement liée à ses intérêts vitaux, notamment en matière d'énergie.

[4] GNSS : Le Système mondial de navigation par satellite (GNSS) désigne une constellation de satellites fournissant des signaux depuis l'espace, lesquels transmettent des données de positionnement et de synchronisation.

[5] GPS : Le Système de positionnement mondial (GPS, Global Positioning System) désigne un système américain de radionavigation basé dans l'espace pour un usage de données de localisation en temps réel, 24 heures sur 24, destiné à un usage civil et militaire.

[6] AIS : Automatic Identification System (AIS), désigne un outil et une aide à la navigation pour les navires afin de leur éviter des collisions graves.

La domination des mégaconstellations, source de dépendance structurelle

Les États-Unis disposent de l'architecture spatiale militaire la plus complète et la plus aboutie au monde. Le GPS, opérationnel depuis 1978 et modernisé en continu, ainsi que la *United States Space Force*, créée en 2019, opèrent des dizaines de satellites de renseignement électromagnétique, de communications résistantes au brouillage, d'imagerie sub-métrique et d'alerte. À cela s'ajoute, au-delà des capacités gouvernementales, Starlink de SpaceX avec, en mars 2026, plus de 10 000 satellites actifs en orbite basse dont l'usage militaire opérationnel a fait ses preuves en Ukraine.

La Russie maintient un arsenal orbital structuré autour de GLONASS, son système de navigation souverain intégré à l'ensemble de ses systèmes d'armes, complété par la constellation de renseignement électronique Liana et les satellites d'alerte avancée Tundra, opérationnels depuis 2015. Par ailleurs, la Chine est aussi un acteur majeur : elle a réussi à bâtir en deux décennies une architecture spatiale militaire capable de rivaliser avec les États-Unis. La constellation BeiDou, au service des forces armées, est opérationnelle depuis 2020 avec 35 satellites, de même que la série Yaogan, qui compte plusieurs dizaines de satellites d'imagerie haute résolution et de renseignement électromagnétique. Enfin, un nouvel acteur émerge : c'est l'Inde. En 2019, le test ASAT[7] relevant de l'opération *Mission Shakti* a démontré qu'une puissance régionale peut désormais se doter d'un accès orbital.

Face à cet arsenal orbital, les armées européennes demeurent structurellement dépendantes du GPS américain pour la navigation et la synchronisation de leurs systèmes d'armes, mais également pour d'autres systèmes comme la détection balistique, le guidage de précision et la surveillance orbitale. En effet, le commissaire européen à la Défense, Andrius Kubilius, a affirmé que les États membres doivent encore obtenir l'autorisation des États-Unis pour partager certaines données sur les menaces spatiales, une situation qu'il qualifie « d'obstacle à notre sécurité » et « d'obstacle à notre indépendance dans l'espace ».

[7] Anti Satellite Weapons (ASAT), désigne l'envoie d'un missile pour détruire un satellite en plein Espace, ou éblouir ou on endommager un satellite sans explosion.

L'inadaptation du droit spatial international

La vulnérabilité européenne comporte une dimension juridique fondamentale. En effet, l'espace demeure l'un des domaines les moins normés du droit international. Le seul texte fondateur est le Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique de 1967, élaboré dans un contexte de guerre froide. Il consacre la liberté d'exploration (article I), la non-appropriation nationale (article II) et prohibe les armes de destruction massive en orbite (article IV). Ces principes conservent leur valeur, mais le Traité demeure inadapté aux réalités contemporaines sur trois points cruciaux.

Premièrement, il est muet sur les armes ASAT non nucléaires. Or, quand un satellite est détruit, cela provoque des milliers de débris qui peuvent détruire d'autres satellites ou des stations spatiales (notamment ennemis) et provoquer un risque de conflits militaires. En effet, la destruction de satellites autres que ceux initialement visés multiplie le risque de perturbation du fonctionnement du GPS (terre, mer, aérien), d'Internet, ainsi que des communications militaires, et expose la population à un risque grave sans précédent de perdre l'accès à l'espace et à des crises militaires incontrôlables.

La Chine a détruit son satellite Fengyun-1C en 2007, générant plus de 3 000 débris, et la Russie a conduit un test similaire en 2021, causant 1 500 fragments qui menacent directement les occupants de la Station spatiale internationale. Les systèmes antisatellites (ASAT) reposant sur des capacités d'interception cinétique se développent ainsi dans un vide normatif, en l'absence de tout régime de sanction et de mécanisme de contrôle.

Deuxièmement, la Convention sur la responsabilité internationale de 1972 instaure une responsabilité absolue pour les dommages en surface, mais seulement une responsabilité pour faute en orbite. Cela revient à dire que si un test ASAT étranger détruit un satellite européen, l'Europe devrait rapporter une preuve causale quasi impossible à établir. Enfin, aucun texte ne régule les mégaconstellations commerciales privées ni leur double usage (*dual-use*) civilo-militaire.

L'affaire Cosmos-2553 illustre cette impunité normative. Ce satellite russe, lancé en février 2022, est soupçonné par la Space Force américaine d'être lié à un programme d'arme nucléaire antisatellite, ce qui constitue une violation directe de l'article IV du Traité de 1967. Lorsque les États-Unis ont soumis une

résolution à l'ONU réaffirmant ces obligations, la Russie a été le seul État à voter contre. Aucune conséquence n'a suivi. Cela témoigne bien d'un vide juridique que l'Europe doit combler, pour prétendre à une autonomie stratégique crédible, par une initiative normative internationale qu'elle serait la mieux placée pour porter.

Les prémices d'une constellation spatiale européenne souveraine

Les acquis européens et leurs insuffisances

L'Europe dispose d'acquis spatiaux réels. Galileo, avec ses 30 satellites opérationnels, offre une précision civile supérieure au GPS et intègre un PRS[8], un service chiffré destiné à un usage gouvernemental et militaire. Copernicus, avec ses satellites Sentinel, est un système permettant l'observation et la surveillance de la Terre en temps réel pour la gestion de crise et la sécurité. Ces acquis sont réels mais leur limite est structurelle, car ils ont été conçus pour répondre à un besoin civil, avec une infime composante militaire insuffisante pour un usage de combat à haute intensité. Galileo est un système de positionnement et non une constellation de commandement, et Copernicus fournit des images, et non des transmissions de données en ciblage en temps réel. L'Europe possède des briques spatiales de qualité, mais elle ne dispose pas d'une architecture militaire orbitale intégrée.

L'implantation d'IRIS² dans le décor spatial européen

Le programme IRIS² représente une avancée qualitative majeure. Porté par le consortium SpaceRise réunissant Airbus Defence & Space, Thales Alenia Space, SES, Eutelsat, Hispasat, Telesat et la Commission européenne, dont le contrat a été signé en 2024 pour un budget de 10,6 milliards d'euros, IRIS² prévoit un déploiement de 282 satellites en orbites basses (LEO) et moyennes (MEO), avec une opérationnalité fixée pour 2030. En octobre 2025, Thales Alenia Space a reçu un contrat de plus de 400 millions d'euros pour les technologies embarquées, en collaboration avec Airbus pour les plateformes, confirmant ainsi qu'IRIS² est désormais en phase d'exécution industrielle.

IRIS² redéfinit le futur des télécommunications européennes. Cette nouvelle constellation satellitaire vise à offrir une connectivité souveraine, sécurisée, résiliente et accessible partout, même dans

[8] Le service public réglementé du système Galileo (PRS, Public Regulated Service), désigne un système destiné à fournir des services de positionnement et de synchronisation mais uniquement aux utilisateurs autorisés par les autorités publiques pour des applications sensibles.

les zones blanches. Ce projet vise à mettre en place des communications sécurisées dans des domaines clés comme la défense, le réseau diplomatique européen, la gestion des crises et la surveillance, mais aussi un accès commercial à internet. Ce projet se distingue des mégaconstellations commerciales étrangères, car il bénéficie d'une exigence de souveraineté des données, d'une cybersécurité renforcée et d'une résilience face aux menaces spatiales.

Sa propulsion active et ses systèmes d'évitement automatisés sont conformes à la Charte Zéro Débris de l'ESA. Avec 282 satellites, ce projet permet de maintenir une constellation maîtrisée plutôt que de subir la surpopulation orbitale américaine ou chinoise, dont la gestion génère des risques croissants d'interférences et de débris. Sa résilience repose sur le durcissement des plateformes contre les impulsions électromagnétiques, une manœuvrabilité accrue face aux menaces et une redondance multiorbite assurant la continuité du service. Il faut cependant nommer sa limite : IRIS² est un système de connectivité gouvernementale sécurisée, et non une constellation militaire dédiée au combat à haute intensité. Même ainsi, IRIS² réduira significativement la dépendance des États membres aux infrastructures étrangères et améliorera leur résilience communicationnelle en temps de crise, démontrant une avancée décisive et un point de départ indispensable à l'autonomie spatiale européenne.

Vers une doctrine spatiale intégrée entre ambition et risque de fragmentation

IRIS² doit s'inscrire dans une architecture plus large. Le commissaire européen à la Défense, Andrius Kubilius, a appelé à la création d'un commandement spatial européen « virtuel », avec pour objectif de mutualiser les capacités spatiales en temps de crise.

Ce projet s'inscrit dans le futur bouclier spatial européen, qui est l'un des quatre projets phares de défense de la Commission européenne, reposant ainsi sur GOVSATCOM pour les communications gouvernementales communes sécurisées, IRIS² pour la connectivité sécurisée, des capacités renforcées de protection contre le brouillage et l'utilisation des services européens de navigation et d'observation. L'Europe doit développer une capacité autonome de *Space Domain Awareness* (SDA), c'est-à-dire avoir une connaissance approfondie de l'espace, incluant les phénomènes naturels et les activités humaines qui s'y déroulent.

Concrètement, cela revient à avoir la capacité de détecter, identifier, surveiller, caractériser et attribuer les objets et menaces en orbite sans dépendre des données américaines, et d'investir dans des

contremesures non cinétiques (cyberdéfense spatiale ou brouillage défensif) permettant de neutraliser des menaces sans générer de débris.

Cette ambition institutionnelle se heurte néanmoins à un risque structurel que l'actualité illustre avec clarté. En effet, l'Allemagne a annoncé en mars 2026 la mise en place d'un programme national de 100 satellites militaires, développé avec des industriels nationaux pour 10 milliards d'euros, en parallèle d'IRIS². S'y ajoutent le projet d'abandon du programme franco-allemand d'avion de patrouille maritime au profit du Boeing P-8 Poseidon américain, la stagnation du projet européen du Système de combat aérien du futur (SCAF), ou encore l'Italie qui étudie également la mise en place d'un réseau de satellites LEO à usage militaire et civil. Même si la Commission a rappelé les avantages de l'approche mutualisée, ces rappels resteront sans effet tant que la coopération spatiale reposera sur la seule bonne volonté politique.

Conclusion

L'Europe n'est pas absente du domaine spatial, comme l'attestent les systèmes européens Galileo et Copernicus. Mais elle y est encore stratégiquement vulnérable sur le plan militaire. Ses acquis spatiaux sont civils, ses dépendances militaires sont extra-européennes, et le cadre juridique international qui devrait la protéger est en réalité inadapté aux réalités actuelles face à une compétition spatiale de haute intensité.

Cependant, IRIS² représente un tournant majeur dans cette volonté d'asseoir son autonomie spatiale stratégique. L'Europe doit désormais assumer une ambition plus large, telle qu'un commandement spatial unifié, une capacité souveraine de surveillance et de défense orbitale, et une initiative normative internationale visant à encadrer le spatial. Ces trois chantiers sont les conditions *sine qua non* pour une Europe qui entend devenir un acteur crédible dans le domaine spatial militaire.

À propos de l'autrice : Fériel Taklit est juriste en droit des affaires, diplômée de l'Université Paris 1 Panthéon-Sorbonne, de l'Université de Montpellier et d'Em Lyon Business School. Elle a travaillé au sein du groupe Thales sur des projets industriels et contractuels liés au secteur de la défense.

Rédigé par : Hugo HILAIRE

L'ARCHITECTURE EUROPÉENNE POUR L'ALERTE PRÉCOCE : UNE FAILLE CRITIQUE DE LA DÉFENSE COLLECTIVE

Le 2 mars, depuis la base de l'Ile Longue à Brest, où sont déployés les sous-marins nucléaires lanceurs d'engins, le président de la République a annoncé une augmentation du nombre de têtes nucléaires composant l'arsenal français, tout en réaffirmant que la France ne renoncerait pas à l'emploi de la dissuasion si ses « intérêts vitaux » venaient à être menacés.

Si cette annonce constitue indéniablement un tournant majeur dans la posture nucléaire française, elle soulève néanmoins plusieurs interrogations. En effet, si l'effort doctrinal et capacitaire vise clairement à renforcer la crédibilité de la riposte, il pose en creux la question de la capacité de la France, et plus largement de l'Europe à se prémunir efficacement contre une attaque initiale. En d'autres termes, se pose la question de savoir si l'Europe, dispose aujourd'hui des capacités nécessaires pour assurer une protection effective des territoires et de ses intérêts stratégiques.

Aujourd'hui les tensions augment de jour en jour, la portée des missiles s'allongent, leur puissance augmente et leur utilisation semble s'affranchir de toute considération éthique. C'est dans ce contexte que la problématique de l'alerte précoce (early warning) acquiert dès lors une pertinence stratégique accrue.

L'alerte précoce se définit comme l'ensemble des capacités permettant la détection précoce du lancement d'un missile, notamment par l'acquisition de sa signature thermique lors de la phase propulsive, son identification rapide par la discrimination fiable entre menaces et objets non menaçants fondée sur des critères tels que la signature infrarouge, la forme, la taille et l'origine du lancement, ainsi que la transmission immédiate et sécurisée de ces informations vers les centres de commandement et de contrôle (C2) afin de garantir une prise de décision en temps opportun.

Une fois la menace détectée et caractérisée, l'architecture d'alerte précoce comprend également des fonctions de suivi continu (tracking), consistant à surveiller l'évolution de la position, de la vitesse et de la trajectoire du missile tout au long de son vol afin d'estimer sa zone d'impact probable. Ces données collectées conditionnent enfin la phase d'interception, qui repose sur le déploiement de contremesures destinées à neutraliser la menace avant l'impact, et dont l'efficacité dépend étroitement de la précision et de la persistance du suivi. Au-delà de la défense immédiate, l'alerte précoce contribue plus largement à la compréhension et à l'anticipation des menaces, tout en jouant un rôle central dans l'attribution de la responsabilité d'une attaque potentielle.

Des capacités terrestres européennes comme base crédible de l'architecture d'alerte précoce

L'efficacité maximale de l'alerte précoce repose sur une intégration étroite des infrastructures spatiales et terrestres. En effet, la composante spatiale offre une capacité de détection plus précoce ainsi qu'une vision globale des théâtres de lancement. Les capteurs infrarouges déployés en orbite constituent à cet égard un maillon essentiel, en permettant d'identifier les menaces avant leur acquisition par les radars au sol, en particulier face aux vecteurs hypersoniques tels que les planeurs hypersoniques (HGV) et les missiles de croisière hypersoniques (HCM).

À bord des satellites, ces capteurs infrarouges détectent les lancements en captant la signature thermique des missiles durant leur phase propulsive, permettant une détection rapide et à grande échelle. Les radars terrestres, fixes ou mobiles, assurent ensuite le suivi des missiles balistiques lors des phases intermédiaire et terminale, tandis que les radars à portée au-delà de l'horizon contribuent à la détection des missiles de croisière évoluant à basse et moyenne altitude. Actuellement, l'Europe dispose de capacités terrestres de défense aérienne et antimissile ayant atteint un niveau de maturité technologique et opérationnelle lui permettant de se positionner à un niveau comparable à celui des capacités américaines au sein de l'OTAN.

En effet, les capacités européennes de défense aérienne et antimissile de détection et d'interception reposent sur un socle industriel et technologique diversifié, articulé autour de plusieurs systèmes terrestres complémentaires. Le programme franco-italien SAMP/T, développé par Eurosam et récemment décliné en version *Next Generation,* décrit par le président Macron comme le meilleur système

de défense sol-air au monde[9], constitue la capacité la plus avancée, offrant une défense contre les aéronefs, les missiles balistiques et, désormais, les menaces hypersoniques manœuvrantes.

À un niveau intermédiaire, l'IRIS-T SLM de Diehl Defence apporte une capacité mobile de défense aérienne de moyenne portée, efficace contre les drones, les aéronefs et les missiles de croisière grâce à un radar performant et à des intercepteurs modernes.

Enfin, des systèmes plus anciens mais toujours pertinents comme le Crotale NG de Thales assurent des fonctions de surveillance, d'identification ami-ennemi et d'engagement de cibles multiples à courte portée. Ensemble, ces capacités illustrent une défense multicouche européenne, encore hétérogène, mais reposant sur une base industrielle robuste. Or, malgré l'existence de ressources, l'Europe affiche aujourd'hui un déficit significatif de capacités spatiales dédiées à l'alerte précoce, limitant son autonomie dans l'évaluation des menaces balistiques.

Au sein de l'OTAN, les États-Unis demeurent à ce stade les seuls fournisseurs d'early warning fondée sur des moyens spatiaux et assuré par le système infrarouge spatial (Space-Based Infrared System, SBIRS). Ce dispositif repose sur une constellation de satellites et de charges utiles équipées de capteurs infrarouges déployés en orbite géostationnaire (GEO) et en orbite hautement elliptique (HEO), complétée par des radars terrestres. Cette constellation offre à la fois une surveillance globale des théâtres de lancement et un suivi précis de cibles individuelles.

Vers un développement ad hoc des capacités spatiales d'alerte précoce

Dans un contexte géopolitique marqué par des fissures et fragmentations au sein du cercle otanien, l'Europe est contrainte de réagir pour renforcer sa défense collective face à cette dépendance capacitaire. À cet égard, le Général Rougier a récemment rappelé que la défense aérienne redevenait une priorité absolue pour les pays européens[10]. Effectivement, l'Europe met actuellement en place son propre système d'alerte précoce autonome afin de renforcer la défense contre les missiles balistiques et les nouvelles menaces hypersoniques. Cette prise de conscience, tardive mais tangible des lacunes de la composante spatiale s'est d'abord inscrite dans une logique souveraine, illustrée par des initiatives

[9] « Défense : Le système sol-air SAMP/T est-il vraiment « le meilleur au monde », comme le dit Macron ? », *20 minutes*, [en ligne]. URL : https://www.20minutes.fr/societe/4196245-20260115-defense-systeme-sol-air-samp-vraiment-meilleur-monde-comme-dit-macron

[10] « Général Alexis Rougier | Supériorité stratégique et très haute altitude », *Chaire Grands Enjeux Stratégiques Contemporains*, [en ligne]. URL : https://www.youtube.com/watch?v=uvMCZQEmN38

nationales telles que les démonstrateurs Spirale (2009–2011) ou le nanosatellite allemand Ernest12U, opérationnel depuis 2025, avant de s'élargir progressivement à des programmes développés à l'échelle de l'Union européenne (UE).

Lancé en 2019 dans le cadre de la coopération structurée permanente (PESCO), le programme TWISTER constitue le principal effort européen en matière de défense antimissile intégrée reposant sur des capacités spatiales. Piloté par la France avec la participation de plusieurs États membres, il vise à développer à l'horizon 2030 une capacité européenne d'alerte précoce spatiale, complétée par des intercepteurs endo-atmosphériques capables de faire face à un large spectre de menaces. Les projets ODIN's EYE et ODIN's EYE II, financés par le Fonds européen de la défense (EDF), constituent le pilier spatial de TWISTER et s'inscrivent dans le développement d'une architecture européenne d'alerte précoce complète.

Dans ce cadre, la France et l'Allemagne ont signé, le 15 octobre 2025, une lettre d'intention lançant l'initiative JEWEL (Joint Early Warning for a European Lookout), appelée à devenir l'élément structurant de ces efforts. Celle-ci prévoit le déploiement de satellites géostationnaires interopérables capables d'assurer une surveillance continue des lancements de missiles, avec pour objectif l'atteinte d'une capacité opérationnelle initiale au début des années 2030. Selon les estimations de l'International Institute for Strategic Studies (IISS), le développement de deux satellites d'alerte avancée en orbite géostationnaire (GEO) représenterait un coût d'environ 3,2 milliards de dollars et permettrait d'établir une capacité européenne minimale et indépendante de détection, destinée à compléter le système américain SBIRS.

Toutefois, afin de disposer d'une couverture autonome et persistante, capable de détecter et de qualifier des lancements régionaux tout en conservant une résilience face aux pressions dans le domaine contrespatial, l'IISS préconise le déploiement d'au moins quatre satellites GEO d'alerte avancée, pour un coût total estimé à 6,4 milliards de dollars[11]. Or, une architecture efficace d'alerte avancée antimissile repose sur une approche multi-orbites, combinant des satellites en GEO, en orbite hautement elliptique (HEO) et en orbite basse (LEO), afin d'assurer simultanément une couverture globale, une redondance accrue et une précision élevée de détection. Le recours à un unique régime orbital exposerait en revanche le système à des vulnérabilités structurelles et à une sensibilité accrue aux menaces systémiques et aux actions contre-spatiales.

[11] Alexandre K. Bollfrass, Annemiek Dols, Erin Pobjie et Ester Sabatino, « Advancing European Military Capacity in Space », *IISS*, [en ligne]. URL : https://www.iiss.org/research-paper/2026/03/advancing-european-military-capacity-in-space/

Par ailleurs, en mars 2026, lors du salon BEDEX à Bruxelles, Thales a dévoilé le projet Skydefender, un système intégré de défense aérienne et antimissile multi-couches et multi domaines, visant à assurer une protection globale contre l'ensemble des menaces aériennes. Au cœur de cette architecture, Thales Alenia Space développe une capacité d'alerte précoce depuis l'orbite géostationnaire, reposant sur des satellites équipés de capteurs infrarouges capables de détecter les lancements de missiles et d'en localiser précisément l'origine avant leur entrée dans le champ des radars terrestres[12]. Cette initiative, faisant suite à la présentation du projet Michelangelo Dome par Leonardo, illustre l'implication croissante des industriels dans le développement de capacités orbitales destinées à renforcer la défense collective européenne.

Conclusion

Dans le contexte sécuritaire actuel, les nations européennes ne peuvent plus se permettre de dépendre d'acteurs extérieurs pour leur architecture d'anticipation et de gestion des menaces. L'Europe se trouve aujourd'hui à un point de bascule stratégique. Loin de constituer une faiblesse, cette situation crée une fenêtre d'opportunité pour clarifier les priorités et engager une réaction structurante. Par ses caractéristiques opérationnelles, la composante spatiale s'impose désormais comme un pilier incontournable de la défense collective européenne, l'espace s'imposant à la fois comme première ligne d'attaque et première ligne de défense. L'UE et des États Membres tels que la France et l'Allemagne ont amorcé cette réaction stratégique.

Les programmes et initiatives en cours apparaissent encourageants et s'inscrivent dans une dynamique visant à l'émergence progressive d'une architecture européenne de défense aérienne plus cohérente et pleinement opérationnelle. L'Europe dispose donc d'une réelle opportunité pour réduire sa dépendance stratégique, notamment par le développement de capacité spatiales, voire d'une constellation multi-orbitale dédiée à l'alerte avancée, venant compléter les capacités terrestres de détection et d'interception.

Plusieurs voies s'offrent à cet effet aux États européens, qu'il s'agisse de programmes menés au niveau de l'UE, de coopérations bilatérales, ou encore d'initiatives portées par l'Agence spatiale européenne (ESA), à l'image du programme European Resilience from Space (ERS). Cette opportunité

[12] « Thales launches SkyDefender: the integral air and missile defence dome with Artificial Intelligence », *Thales*, [en ligne]. URL : https://www.thalesgroup.com/en/news-centre/press-releases/thales-launches-skydefender-integral-air-and-missile-defence-dome

repose sur un écosystème spatial européen en pleine dynamique, caractérisé par l'engagement croissant des industriels, la disponibilité d'une expertise technique reconnue au sein de l'ESA, et des investissements nationaux soutenus dans le secteur spatial et de défense. Le principal défi réside désormais dans la capacité des États à dépasser les rivalités politiques, industrielles et doctrinales qui ont entravé des projets européens récents, tels que le SCAF ou l'initiative European Sky Shield, condition pourtant indispensable à l'émergence d'une architecture européenne crédible et cohérente de défense aérienne et antimissile.

À propos de l'auteur : Titulaire d'un Master en « Relations internationales : nouveaux enjeux et gestion de crise » de Sciences Po Toulouse et de l'Université Complutense de Madrid, Hugo s'est spécialisé dans les politiques internationales de sécurité et de défense. Il a consacré son mémoire à la coopération UE-OTAN dans le domaine des politiques spatiales de défense. Il poursuit actuellement un Master de spécialisation en études européennes à l'Institut d'Études Européennes de Bruxelles. Il a également effectué un stage au sein de l'Agence spatiale européenne (ESA), où il a contribué à l'analyse de la sécurité spatiale et des politiques européennes.

Rédigé par : Charles CHIKANY

LA CITADELLE CYBER 2040 : FORGER LA SOUVERAINETÉ EUROPÉENNE À L'ÉPREUVE DE L'ASYMÉTRIE

Mythos et GPT-5.5 Cyber, à peine sortis, font voler en éclats les délais d'exploitation des vulnérabilités. Deux ans avant l'apparition de ChatGPT en 2022, neuf mois après, 16 heures aujourd'hui, et probablement sous l'heure demain selon les estimations qui circulent dans les analyses stratégiques. L'Europe et la France au premier rang encaissent en miroir une vague d'attaques sans précédent le ministère de l'Intérieur visé par une intrusion majeure dans la nuit du 11 au 12 décembre 2025, 12 millions à l'ANTS en avril 2026, l'attaque DDoS de NoName057 contre La Poste fin 2025, sans parler des fuites à répétition côté privé. Le Premier ministre français reconnaît trois vols de données par jour sur les systèmes d'information de l'État. L'Autorité bancaire européenne et la BCE convoquent en urgence les superviseurs financiers face à Mythos. La cybermenace cesse d'être un risque informatique pour devenir un risque macro-économique systémique.

Au Forum InCyber 2026, Vincent Strubel, directeur général de l'ANSSI, le résume sans détour : « le décalage évident, croissant, entre d'une part un monde politique qui n'en finit pas de se durcir et puis d'autre part un monde numérique qui n'est pas à la hauteur de ces circonstances ». L'Europe a longtemps cru pouvoir compenser son retard capacitaire par la régulation : RGPD, NIS2, DORA, Cyber Resilience Act. Cette doctrine atteint ses limites. Comment l'Union peut-elle, à l'horizon 2040, basculer d'une souveraineté numérique de papier, centrée sur la conformité réglementaire et la localisation des serveurs, vers une souveraineté capacitaire fondée sur la maîtrise des couches matérielles, logicielles, cognitives et humaines de la résilience cyber ?

À partir d'une matrice prospective (cf. Figure 1), nous défendons le scénario de la citadelle décomplexée, qui s'appuie sur quatre fondations indissociables : les fondations physiques (I), la souveraineté de la donnée (II), le triptyque algorithmique et cognitif (III), et la résilience humaine et écosystémique (IV).

Reprendre la main sur les fondations physiques

Aucune citadelle ne tient sur le sable d'autrui. La protection des réseaux critiques commence par la couche dont on parle le moins : le matériel. Câbles, routeurs, pare-feu, silicium, terres rares. Ces

fondations restent l'angle mort de la souveraineté européenne, parce qu'elles relèvent de cycles industriels longs, peu compatibles avec le tempo politique et réglementaire.

L'asymétrie capitalistique des équipements réseaux

42 % des communications 5G européennes transitent par des équipements de fournisseurs à haut risque, comme la commissaire Henna Virkkunen le rappelait au Parlement européen en février 2025. La boîte à outils 5G de l'UE et les obligations de NIS2 sur la chaîne d'approvisionnement offrent déjà un cadre de restriction des fournisseurs à risque, encore faut-il l'activer. Les marchés publics européens représentent près de 14 % du PIB de l'UE : un levier capacitaire massif, sous-exploité.

Recherche, écosystème, capital : la vraie ligne de fracture

La recherche cyber européenne tient son rang, et la chaîne académique produit. Le blocage est en aval, dans l'industrialisation et le financement de la croissance. En 2025, la cybersécurité mondiale a attiré 13,97 milliards de dollars de capital-risque, dont près des trois quarts captés par des startups américaines. Les startups européennes ont levé environ 2,7 milliards d'euros sur la même année, soit un dixième de la masse américaine, alors que l'Union pèse près d'un quart du PIB mondial. Plusieurs jeunes pousses sont rachetées ou perdent leurs talents avant d'atteindre la masse critique nécessaire à une consolidation autonome.

Les grands groupes européens de défense, télécoms et services devraient favoriser l’investissement dans les startups et ETI cyber, acheter leurs technologies et de leurs ouvrir des marchés.

La bataille sous-marine : l'angle mort capacitaire

98 % du trafic intercontinental transite par approximativement 570 câbles sous-marins. En quinze ans, les hyperscalers américains (Google, Meta, Microsoft, Amazon) ont pris le contrôle d'environ 71 % de la capacité internationale, et plus de 90 % sur la route transatlantique. Le câble Dunant, entre les États-Unis et la France, appartient à Google, Orange opérant uniquement l'atterrissage côté français. En novembre 2024, les câbles BCS East-West Interlink et C-Lion1 sont sectionnés en Baltique. La réaction européenne s'est durcie : dans la nuit du 15 au 16 janvier 2025, lors de la mission OTAN Baltic Sentry, un avion de patrouille Atlantique 2 français est verrouillé par le radar d'une batterie russe S400 depuis Kaliningrad, soit l'avant-dernier stade avant le tir.

Les réactions industrielles émergent. En 2024, l'État français rachète 80 % d'Alcatel Submarine Networks, l'un des leaders mondiaux de la conception, fabrication, pose et maintenance de câbles sousmarins, vendu à Nokia en 2015. Un Plan d'action européen sur la sécurité des câbles, présenté en février 2025 par la Commission, dote treize projets d'intérêt européen de 347 millions d'euros.

Verticalisation matérielle : la dépendance physique de la chaîne de production

La sécurité d'un système d'information ne se limite pas au logiciel : elle commence par le matériel. Une compromission matérielle (firmware infecté, sous-composant piégé) peut rester invisible aux outils logiciels. L'opération israélienne contre les pagers du Hezbollah au Liban, avec près de 3 000 appareils piégés a rappelé qu'une chaîne d'approvisionnement compromise constitue un vecteur d'attaque réel et difficilement détectable a posteriori.

Cette dépendance physique se décline à trois étages : 85 % des capacités mondiales de séparation des terres rares concentrées en Chine ; NVIDIA détient l'état de l'art GPU sous condition des contrôles à l'export américain ; les fonderies sub-5 nm sont concentrées à Taïwan (TSMC) et en Corée (Samsung). Sans GPU souverains et sans accès stable au silicium avancé, IA défensive autonome, cloud et cryptographie post-quantique massive ne sont possibles à l'échelle continentale.

En réaction, la France a engagé en mai 2026 son Plan national de résilience « Terres rares et aimants permanents », qui vise 100 % des besoins européens en terres rares lourdes d'ici 2030, doté d'un fonds de 2 milliards d'euros. L'European Chips Act (43 milliards d'euros) accompagne le mouvement. Parmi les premières initiatives CPU/GPU souveraines, SiPearl avec son CPU Rhea, Kalray. Une fonderie avancée européenne d'ici le début des années 2030 pourrait conditionner la viabilité d'une cyberdéfense matériellement souveraine.

Maîtriser les fondations matérielles ne suffit pas, encore faut-il prolonger cette maîtrise sur les données qui y circulent.

Souveraineté de la donnée : sortir de l'extraterritorialité subie

La souveraineté de la donnée ne concerne pas uniquement sa localisation. Se pose la question de la liberté décisionnelle : pouvoir choisir, arbitrer, basculer ses systèmes sans dépendre d'autorisations extérieures.

Le « cloud de confiance » et les limites de l'isolation juridique

Le diagnostic posé par la Cour des comptes le 31 octobre 2025 appelle au pragmatisme. La Cour conclut « [qu'il] n'existe pas d'inventaire interministériel formalisé des données sensibles à héberger de manière souveraine », alors même que « la collecte en masse de données est un enjeu majeur pour les grandes puissances afin, notamment, de développer leurs capacités en intelligence artificielle ». Les hyperscalers américains détiennent environ 95 % du marché du cloud européen alors que des acteurs européens existent mais ils sont insuffisamment sollicités face à des solutions américaines clé en main qui captent les budgets cyber par effet de gamme et de force commerciale.

La section 702 du Foreign Intelligence Surveillance Act (FISA) permet aux agences de renseignement américaines de collecter, sans mandat individuel, les communications électroniques de personnes étrangères dès lors qu'elles transitent par des fournisseurs domiciliés aux États-Unis. La loi RISAA d'avril 2024 a prorogé le dispositif jusqu'en 2026 et élargi son champ aux prestataires de cloud et datacenters.

Le Cloud Act (2018) oblige les fournisseurs américains à transmettre les données qu'ils détiennent, où qu'elles soient stockées dans le monde, sur réquisition judiciaire américaine.

Vincent Strubel résumait au Forum InCyber 2026 la double menace cumulative : « la captation de nos données au titre du droit à portée extraterritoriale d'où qu'ils viennent, ou la coupure brutale de service au titre de ce même droit ». Le risque d'interruption, désigné couramment par le terme « kill switch », est sorti du scénario théorique pour devenir un paramètre opérationnel à intégrer dans la conception des systèmes critiques.

L'épisode Nicolas Guillou, juge français à la Cour pénale internationale sanctionné par l'administration américaine en 2025, donne une portée concrète à cette dépendance. Comptes bancaires bloqués, remboursements d'assurance santé inaccessibles, services Microsoft suspendus, accès numériques coupés. Un magistrat français exerçant un mandat international se retrouve déconnecté de ses outils professionnels et privés par la décision unilatérale d'une puissance étrangère. L'extraterritorialité a quitté le terrain du risque théorique pour celui de l'instrument d'influence.

Les offres de « cloud de confiance » construites sur technologies américaines sous licence garantissent une isolation juridique tant que l'application extraterritoriale du droit américain reste cantonnée aux opérateurs. Si elle venait à s'étendre aux licences logicielles elles-mêmes, l'autonomie juridique mise en avant par ces offres en sortirait fragilisée. Le cas du Health Data Hub illustre les limites de l'effectivité des recommandations administratives en matière de souveraineté des données. Malgré

les alertes répétées de la CNIL dès 2020 et un long parcours contentieux, la plateforme est restée hébergée sur Microsoft Azure pendant près de cinq ans. Ce n'est que le 23 avril 2026 qu'elle a annoncé sa migration vers Scaleway, filiale du groupe Iliad. Le transfert vers cette nouvelle infrastructure est prévu pour la fin de l'année 2026 ou le début de l'année 2027.

Vers une bascule capacitaire : la France comme déclencheur européen

La séquence d'attaques 2025-2026 a accéléré la décision politique. Le séminaire de la Direction interministérielle du numérique (DINUM) du 8 avril 2026 a annoncé une sortie progressive de Windows pour Linux dans l'administration centrale, la migration de 80 000 agents de la Caisse nationale d'assurance maladie vers les solutions souveraines Tchap, Visio et FranceTransfert, et l'obligation pour chaque ministère de formaliser d'ici l'automne 2026 son plan de réduction des dépendances extra-européennes.

Le plan d'action présenté par le Premier ministre Sébastien Lecornu le 30 avril 2026 a complété ce dispositif : déblocage de 200 millions d'euros d'urgence (modernisation applicative, capacités de détection, cryptographie post-quantique), fusion de la DINUM et de la Direction interministérielle de la transformation publique en une autorité numérique de l'État rattachée au Premier ministre, affectation des amendes CNIL à un fonds de modernisation des systèmes d'information publics, et fixation d'un seuil minimal de 5 % des budgets numériques de chaque ministère consacrés à la cybersécurité dès 2027.

À l'échelle européenne, le sommet de Berlin sur la souveraineté numérique de mi-novembre 2025 a porté 18 initiatives concrètes, dont l'alliance Mistral-SAP et l'accélération du déploiement d'IRIS² pour la connectivité satellitaire, illustrant un mode de coopération inter-États structuré sur projets, sans intégration verticale.

Edge souverain et logique d'investissement

Le traitement décentralisé des données, au plus près des utilisateurs et des capteurs, présente un double bénéfice : la réduction de la surface d'attaque concentrée et la diminution de la dépendance aux hyperscalers centralisés.

En contrepartie, il introduit de nouveaux défis (multiplication des points d'entrée, hétérogénéité des firmwares, complexité de maintenance) qui exigent une discipline de sécurité renforcée tout au long de la chaîne d'approvisionnement.

Le projet European Edge Continuum, démontré pour la première fois en environnement opérationnel au Mobile World Congress de Barcelone le 2 mars 2026, marque une avancée structurante. Il fédère, dans le cadre de l'IPCEI-CIS, les edge clouds de plusieurs opérateurs de télécommunications à travers un point d'accès unique. Pour les usages de défense, une architecture souveraine ne peut toutefois faire l'économie d'un volet centralisé : les applications militaires qui réclament de la masse computationnelle (renseignement d'images, IA d'aide à la décision, simulation) ne peuvent reposer sur le seul edge.

Les deux architectures, distribuée et centralisée, sont complémentaires. Reste à les rendre européennes. Le cas Mythos illustre l'urgence stratégique. En effet, Anthropic ne diffuse pas son modèle frontière au public et le partage seulement avec une poignée de grandes entreprises américaines et avec l'administration américaine, le temps que les éditeurs corrigent les vulnérabilités découvertes. Les banques européennes attendent un accès qui n'est pas garanti. D'ici 5 ans, accéder à un modèle de cette catégorie sera un acte de souveraineté à part entière.

L'Europe ne peut espérer reconquérir son cloud par la régulation seule. Le Cyber Resilience Act, DORA et NIS2 sont nécessaires, mais insuffisants. Trois leviers complémentaires sont indispensables. D'abord, la commande publique européenne préférentielle, qui mobilise un volume de marchés représentant près de 14 % du PIB de l'Union. Ensuite, un écosystème dense de fonds d'investissement privés européens, indépendants entre eux et distincts des dispositifs d'aide publique de la Commission, capables de financer en série les startups et ETI cyber depuis l'amorçage jusqu'à la croissance. Enfin, une doctrine de coopération technologique sélective, qui préserve l'interopérabilité avec les alliés tout en garantissant l'étanchéité des briques critiques européennes : cryptographie, identité numérique, données stratégiques.

Maîtriser les couches matérielles et la donnée n'est qu'un préalable. La résilience cyber se joue désormais en temps réel, dans la course algorithmique entre attaque et défense.

Anticiper, détecter, contre-attaquer : le triptyque algorithmique et cognitif

La résilience cyber de 2040 se gagnera autant dans l'algorithme que dans le câble. Trois fronts simultanés la structurent : la profondeur du renseignement sur la menace, la guerre cognitive industrialisée par l'intelligence artificielle, la rupture cryptographique liée au calcul quantique.

Renseignement cyber souverain : profondeur de télémétrie et coopération inter-CSIRTs

La Cyber Threat Intelligence (CTI) mondiale est dominée par une poignée d'acteurs américains qui disposent d'une très grande profondeur de télémétrie : Mandiant (filiale Google), CrowdStrike, Microsoft Threat Intelligence, et Cloudflare, possédant près de 20 % du trafic web mondial. Aucun acteur européen ne dispose à ce jour d'une concentration de capteurs et de données d'incidents comparable.

L'Europe possède pourtant des briques solides, mais fragmentées. Orange Cyberdefense et Sekoia offrent des services de CTI sectorielle, Filigran porte la solution open source OpenCTI utilisée dans plusieurs administrations européennes, HarfangLab développe une solution EDR souveraine,

Synacktiv conduit des missions offensives et de réponse à incident. Bitdefender (Roumanie) et WithSecure (Finlande) complètent un tissu cloisonné.

L'enjeu doctrinal consiste à compléter la logique de conformité, structurée par NIS2 et le Cyber Resilience Act, par une logique de défense proactive. Deux approches émergent : l'External Attack Surface Management (EASM), qui cartographie en continu les actifs exposés depuis le point de vue d'un attaquant, et le Continuous Threat Exposure Management (CTEM), qui priorise les vulnérabilités selon leur exploitabilité réelle.

Le réseau européen des CSIRTs, établi dès 2016 par la directive NIS et consolidé par NIS2, fonctionne sous le secrétariat d'ENISA et coordonne déjà l'échange d'informations entre les CSIRTs des États membres, en lien avec CERT-EU pour les institutions européennes. Le réseau opérationnel EUCyCLONe rassemble les autorités nationales de gestion de crise, et le Cyber Blueprint révisé en juin 2025, a été testé lors de l'exercice BlueOLEx 2025. L'EU Cybersecurity Reserve, dotée de 36 millions d'euros et opérée par ENISA depuis août 2025, mobilise des prestataires de confiance en cas de crise transfrontalière. L'enjeu est à la densification des données : volume et qualité des indicateurs partagés, vitesse de circulation des techniques observées et télémétrie.

La guerre cognitive : l'ingénierie sociale industrialisée par l'IA

L'industrialisation de la manipulation informationnelle par l'IA générative est l'une des transformations les plus rapides du paysage de menace. Le nombre de vidéos deepfake détectées dans le monde est passé d'environ 15 000 en 2019 à plus de 95 000 en 2023, soit une progression de 550 % en quatre ans, avec une projection à 8 millions à fin 2025. Le coût des fraudes par contenus synthétiques en

2025 atteint 863 millions d'euros pour les organisations victimes. Le cas du groupe Arup à Hong Kong, en février 2024, fait référence : 25 millions de dollars détournés à la suite d'une visioconférence frauduleuse mettant en scène un deepfake du directeur financier.

La France dispose d'un atout institutionnel particulier. VIGINUM, service à compétence nationale créé le 13 juillet 2021 sous le SGDSN, bénéficie d'un cadre juridique particulier qui autorise le traitement automatisé de données publiques pour détecter et caractériser les ingérences numériques étrangères. Son activité 2024 a permis de détecter entre 250 et 300 phénomènes par an, parmi lesquels les campagnes pro-russes Matriochka et Portal Kombat, ou les 43 manœuvres informationnelles ciblant les Jeux olympiques et paralympiques de Paris en 2024. En février 2025, VIGINUM a publié un rapport détaillé sur la manipulation observée autour de l'élection présidentielle roumaine.

La défense cognitive ne se gagnera pas par la course technologique au détecteur de deepfakes, structurellement perdue face à des générateurs adversaires qui s'améliorent en symétrie, ni par une certification généralisée de l'information. Trois leviers la portent : la sensibilisation et l'éducation citoyennes au doute méthodique et à la vérification des sources, la robustesse des doctrines institutionnelles de communication de crise, et la disponibilité d'outils européens d'analyse des contenus synthétiques fondés sur des modèles d'IA souverains. Chaque État européen organise à sa façon sa capacité de détection ; la coopération européenne se construit par échange d'analyses.

La menace quantique : Harvest Now, Decrypt Later

Des acteurs étatiques aspirent aujourd'hui massivement les données chiffrées européennes (communications diplomatiques, transactions financières, données de santé, secrets industriels, communications militaires interceptées sur câbles sous-marins) dans l'hypothèse de pouvoir les déchiffrer ultérieurement avec un ordinateur quantique tolérant aux erreurs. Cette stratégie d'aspiration différée, dite « Harvest Now, Decrypt Later », transforme toute donnée chiffrée aujourd'hui avec une durée de vie utile supérieure à 10 ans en actif déjà compromis.

Le directeur général de l'ANSSI a précisé le calendrier le 8 octobre 2025 : « il ne sera pas raisonnable d'acheter des produits qui n'intègrent pas de la cryptographie post-quantique après 2030 ». Les algorithmes RSA-2048 et ECC-256 sont considérés par le NIST comme exposés à compter de cette même échéance. L'ANSSI estime un « Q-Day » réaliste à 2035, date à laquelle un ordinateur quantique suffisamment puissant pourrait casser les chiffrements asymétriques en usage courant.

L'industrie européenne se positionne. Thales a lancé son chiffreur réseau MISTRAL post-quantique à l'European Cyber Week de Rennes en novembre 2025, avec une disponibilité commerciale prévue en juin 2026. L'équipement, certifié EAL4+ et conforme aux référentiels ANSSI, utilise l'algorithme MLKEM standardisé par le NIST en août 2024 et délivre un débit de 4 fois 10 gigabits par seconde. La Commission européenne déploie en parallèle l'initiative EuroQCI, qui combine cryptographie postquantique et distribution quantique de clé (QKD) terrestre et spatiale via la constellation IRIS².

La trajectoire de migration ne peut se résumer à une transposition mécanique des standards internationaux. La cryptographie post-quantique européenne devrait s'engager dans les processus de standardisation pour faire valoir ses propres choix techniques, en privilégiant l'interopérabilité et la robustesse vérifiables plutôt que la singularité de principe. Une trajectoire claire de migration des opérateurs d'importance vitale, alignée avec les recommandations de l'ANSSI et de ses équivalents européens, permettrait de tenir l'horizon 2030 sans rupture opérationnelle.

IA défensive : la course à l'augmentation opérationnelle

L'effondrement temporel des délais d'exploitation, évoqué en introduction, referme la fenêtre de réaction humaine. Le rapport 2026 de CrowdStrike indique un temps moyen de progression latérale d'attaquant tombé à 29 minutes en 2025, soit une accélération de 65 % par rapport à 2024 (48 minutes), avec un record observé à 27 secondes. Les superviseurs financiers, François-Louis Michaud (ABE), Christine Lagarde (BCE), Andrew Bailey (Bank of England), Jamie Dimon (JP Morgan) et David Solomon (Goldman Sachs) ont tous, en avril 2026, classé Mythos parmi leurs priorités bien que son accès ne soit pas garanti. Les systèmes legacy bancaires étant parfois vieux de plusieurs décennies, la souveraineté algorithmique devient un enjeu de stabilité financière.

Deux extrêmes doivent être écartés. Le « tout-IA », dénoncé par Vincent Strubel (« tout miser sur l'IA serait une erreur »), conduirait à déléguer des décisions critiques à des systèmes dont la traçabilité reste imparfaite. À l'inverse, le refus de l'IA défensive, par méfiance ou excès de prudence réglementaire, placerait l'Europe en infériorité opérationnelle structurelle. La position d'équilibre consiste à intégrer l'IA dans les outils défensifs au moins aussi vite que les attaquants l'intègrent dans leurs offensives, tout en préservant la supervision humaine sur les décisions structurantes : escalade, déconnexion d'un opérateur d'importance vitale, riposte. Il ne s'agit pas de déléguer mais d'augmenter opérationnellement les praticiens.

La cyberdéfense de 2040 reposera sur les modèles entraînés en 2030 : les choix d'investissement faits aujourd'hui sont structurants. Le défi n'est pas tant de réguler l'IA que de la produire à un niveau compétitif.

La résilience humaine et écosystémique : encaisser, repartir, retenir

La maîtrise des couches algorithmiques et cognitives ne dispense pas d'une stratégie de résilience humaine et écosystémique, qui repose sur trois leviers indissociables. Mieux vaut partir du principe que la frontière finira par céder. La résilience ne se mesure plus à l'absence d'attaque, mais à la capacité à maintenir la mission sous attaque, à reconstruire vite et à conserver les compétences qui rendent cela possible.

Le mode dégradé et la résilience cyber-physique

Le mode dégradé désigne la capacité d'un système critique à fonctionner avec moins, sous attaque ou en cas de compromission profonde. Dans l'énergie, basculer en commande locale manuelle des postes électriques en cas de compromission des SCADA (*Système de contrôle et d'acquisition de données*). Dans la santé, assurer la continuité des soins sans système d'information hospitalier nominal. Dans la défense, maintenir la chaîne opérationnelle sans connexion réseau permanente. La variante « air-gap » consiste à déconnecter de manière contrôlée et réversible un système critique en quelques minutes, le temps d'isoler une intrusion et de purger les segments compromis.

Pour illustrer ces propos, l'attaque subie par Jaguar Land Rover le 31 août 2025 a paralysé la production sur l'ensemble de ses sites mondiaux pendant près de six semaines, perturbant plus de 5 000 entreprises de la chaîne d'approvisionnement et coûtant environ 1,9 milliard de livres à l'économie britannique. L'attaque DDoS subie par le groupe La Poste entre le 22 décembre 2025 et le 5 janvier 2026 illustre une résilience effective.

Revendiquée par le groupe pro-russe NoName057 et prise en charge par la DGSI, elle a culminé à 366 gigabits par seconde et 3,5 milliards de paquets par seconde, sans permettre d'intrusion ni de fuite. Le groupe a livré 180 millions de colis pendant l'incident. Comme l'a résumé Philippe Bertrand, directeur de la sécurité globale du groupe : « quels que soient les moyens mis en place, aucune organisation ne peut empêcher les cyberattaques. Tout l'enjeu consiste à avoir les moyens d'y faire face ».

La force de réaction rapide : pompiers du cyber et exercices interarmées

La France dispose d'une architecture de réponse à incident articulée autour de plusieurs piliers : l'ANSSI et le CERT-FR pour les opérateurs d'importance vitale (OIV) et entités essentielles au sens de NIS2 ; les prestataires PRIS qualifiés (Synacktiv, HarfangLab, Wavestone) ; le COMCYBER, appuyé par sa Réserve dont la LPM 20242030 prévoit la montée en puissance jusqu'à 1 000 cybercombattants d'active ; le dispositif 17Cyber pour le grand public et les PME. À l'échelle européenne, le CSIRTs Network, EU-CyCLONe et l'EU Cybersecurity Reserve constituent un cadre opérationnel commun. Le volet militaire mérite une attention particulière.

L'intégration systématique du volet cyber et guerre électronique aux exercices interarmées majeurs (Orion 2026, Cyber Coalition de l'OTAN, Locked Shields conduit chaque année à Tallinn) conditionne la capacité réelle des forces à opérer sous menace cyber multidomaines. La résilience cyber militaire se forge par la simulation grandeur nature, sous tension opérationnelle, dans un environnement reproduisant les couplages cyber-physiqueinformationnel des conflits contemporains. La montée en puissance de la composante européenne de l'EU Cybersecurity Reserve, en lien étroit avec les structures nationales de réponse à incident, accroîtrait la capacité projetable face à une compromission systémique transfrontalière.

Capital humain et écosystème

La pénurie de talents cyber est documentée à toutes les échelles. La France compte environ 15 000 postes vacants selon Wavestone en 2025. À l'échelle mondiale, l'ISC2 évalue à 2,8 millions le déficit dans son Cybersecurity Workforce Study 2024. L'Observatoire des métiers de la cybersécurité ANSSI/AFPA/DGEFP relève en 2025 que 47 % des offres exigent un niveau Bac+5, et que les femmes ne représentent que 11 % des effectifs.

Le constat dépasse l'aspect quantitatif. La pénurie est aussi qualitative : les processus de recrutement, en privilégiant les filtres formels (diplôme initial, mots-clés du curriculum vitae, certifications), recrutent parfois des profils moins opérationnels que les candidats atypiques qu'ils écartent. Les autodidactes, les profils en reconversion venus de l'administration système, du droit, des sciences humaines ou de l'industrie, et les passionnés issus des compétitions de type Capture The Flag ou de plateformes telles qu'Hackropole apportent une diversité de regards précieuse à un métier dont la complexité dépasse largement le périmètre technique.

À cette pénurie s'ajoute une fragilité culturelle propre à l'écosystème européen. En France, un premier échec continue d'entraîner des conséquences bancaires, fiscales et réputationnelles qui pénalisent toute nouvelle tentative, tandis que la Silicon Valley considère souvent l'expérience acquise comme un atout. Cette défiance à l'égard des parcours non linéaires freine aussi bien les fondateurs que les investisseurs et alimente la fuite des talents.

Quatre leviers se dessinent. Le premier consiste à élargir les critères de sélection au-delà du seul diplôme initial, en valorisant les parcours non-linéaires, les contributions open source et les profils en reconversion.

Le deuxième consiste à massifier la réserve opérationnelle de cyberdéfense (RCD française et ses équivalents allemand KdoCIR, italien CIOC, britannique Cyber Force Reserves) par des conventions employeurs élargies, un statut fiscal incitatif et des passerelles formalisées entre réserve militaire et autorités civiles compétentes lors de crises majeures, sur le modèle des médecins militaires détachés au profit du secteur civil pendant la crise sanitaire.

Le troisième consiste à construire des écosystèmes nationaux qui dialoguent à l'échelle européenne, par la coopération transfrontalière, le réinvestissement des fonds privés dans les startups cyber du continent et l'achat préférentiel européen lorsque l'offre existe. Il s'agit de dupliquer dans chaque État membre une dynamique de coalition entre services publics, grands groupes et PME/ETI, au service d'une filière cyber souveraine et intégrée.

Le quatrième tient à la fidélisation par la mission, le projet et la compétence démontrée. L'écart salarial avec les États-Unis est réel, mais la rétention se joue surtout sur l'autonomie d'action, les objectifs de la mission et les perspectives non-linéaires. Accepter qu'un parcours non-linéaire soit un actif et non un défaut : telle est la condition culturelle d'un capital humain durable.

Conclusion

La souveraineté cyber européenne à l'horizon 2040 ne se mesurera pas à la localisation des serveurs, ni au volume de pages réglementaires produites. Elle se mesurera à la liberté décisionnelle : la capacité à choisir, arbitrer, basculer et reconstruire ses systèmes sans dépendre d'autorisations extérieures. Cette liberté repose sur quatre fondations indissociables : maîtrise capacitaire de la couche physique, souveraineté de la donnée, supériorité algorithmique sous supervision humaine, capital humain et écosystémique.

Le scénario de la citadelle décomplexée s'oppose au statu quo dormant et au continent sous pression sans céder à l'illusion d'une autarcie technologique. Il se construit par quatre déplacements : passer d'une logique normative à une logique capacitaire d'investissement, par l'activation effective de la commande publique européenne préférentielle ; faire émerger un écosystème dense de fonds d'investissement privés européens, indépendants entre eux, capables de financer en série les startups et ETI cyber ; structurer la coopération inter-États sur projets industriels concrets, à l'image du European Edge Continuum ou du Plan d'action européen sur la sécurité des câbles ; valoriser le risque entrepreneurial, le parcours non-linéaire et la compétence vérifiable comme actifs structurants.

La frontière numérique sera franchie : la question n'est plus de savoir comment l'empêcher, mais comment la tenir, l'encaisser et la reconstruire, seul lorsqu'il le faut, avec les alliés lorsque cela est possible. Cette discipline, à la fois industrielle, doctrinale et humaine, est la condition de la liberté d'action européenne pour la décennie qui s'ouvre.

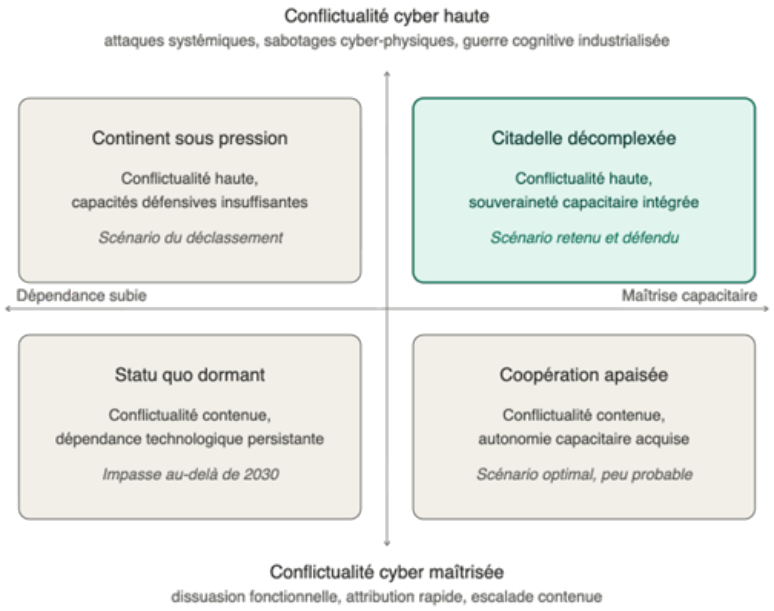

Figure 1 - Matrice prospective de la souveraineté cyber européenne à l'horizon 2040

À propos de l'auteur : Étudiant ingénieur en dernière année spécialisé en cybersécurité, Charles a réalisé un stage de cinq mois à l'ANSSI et est également auditeur du 153e cycle Jeunes de l'IHEDN. Il effectue actuellement son stage de fin d'études en cybersécurité dans une entreprise de la BITD.

Rédigé par : Lydie PÉRUSIN

VULNÉRABILITÉ DE LA SUPPLY CHAIN : QUELS RISQUES POUR LES CONSTRUCTEURS AÉRONAUTIQUES ?

600 %. C'est la hausse estimée des cyberattaques visant le secteur aéronautique en 2025[13]. Un chiffre qui, à lui seul, résume un basculement stratégique : la filière n'est plus ciblée uniquement pour ses grands groupes, mais pour l'ensemble de l'écosystème qui les fait fonctionner. Les attaques ne cherchent plus seulement à voler des données sensibles, elles cherchent désormais à déstabiliser, paralyser, désorganiser.

La *supply chain* ? C'est-à-dire l'ensemble des fournisseurs, sous-traitants, partenaires logistiques et prestataires numériques qui concourent à la fabrication et à la livraison d'un aéronef, est devenue la cible privilégiée de cette nouvelle génération d'attaques. Dans l'aéronautique, cette chaîne est d'une complexité rare : un avion résulte de l'assemblage de plusieurs dizaines de milliers de composants, produits par des acteurs dispersés aux quatre coins du monde.

Cette réalité pose une question centrale : dans quelle mesure la vulnérabilité croissante de la *supply chain* remet-elle en cause la souveraineté des entreprises de la base industrielle et technologique de défense (BITD), et comment les acteurs du secteur peuvent-ils y répondre ?

Une supply chain structurellement vulnérable

Plus une chaîne d'approvisionnement est longue et diversifiée, plus elle repose sur des interfaces multiples, des prestataires aux profils variés et des niveaux de maturité en cybersécurité hétérogènes. Or, dans un environnement aussi interconnecté que celui de l'industrie aéronautique, il suffit d'un seul maillon faible pour compromettre l'ensemble d'un système. C'est précisément ce que révèle l'attaque ayant visé le logiciel MUSE de Collins Aerospace (groupe RTX) en septembre 2025. En perturbant les systèmes d'enregistrement et d'embarquement de plusieurs aéroports européens, cette attaque a contraint des terminaux entiers à revenir à des procédures manuelles, générant des annulations en

[13] Allianz, Baromètre des risques aéronautiques 2025.

cascade et une désorganisation opérationnelle à Bruxelles, Berlin, Dublin et Londres[14]. Cet épisode illustre une évolution fondamentale de la menace : on ne parle plus seulement de vol de données sensibles, mais de risque systémique. Une cyberattaque ciblant un prestataire tiers peut désormais produire des effets en cascade sur l'ensemble d'un écosystème industriel.

Les grands industriels du secteur de la défense et de l'aérospatiale recensent chaque année des dizaines de milliers de vulnérabilités au sein de leurs systèmes d'information. Ces chiffres, aussi vertigineux soient-ils, ne reflètent que les failles détectées en interne. Ils ne disent rien des vulnérabilités potentielles chez les milliers de sous-traitants qui gravitent autour de ces groupes, et dont le niveau de sécurité informatique reste, pour beaucoup, très en deçà des standards exigés au sommet de la chaîne. La vulnérabilité de la *supply chain* ne constitue pas seulement un risque opérationnel. Elle touche, plus profondément, à la souveraineté industrielle et numérique des acteurs de la BITD. Car, dans le secteur de la défense aéronautique, la maîtrise des flux, des données, des logiciels embarqués et des systèmes de communication est un enjeu stratégique de premier ordre.

La dépendance envers des prestataires étrangers aggrave encore cette fragilité. Une étude du Cigref publiée en 2025 révèle que 80 % des dépenses liées aux logiciels et services de stockage de données à usage professionnel en Europe sont effectuées auprès d'entreprises américaines[15]. Dans ce contexte, une panne, une attaque ou une simple décision commerciale d'un acteur extra-européen peut mettre en difficulté des pans entiers de la production industrielle française ou européenne. La question n'est donc plus seulement de savoir comment protéger un groupe aéronautique, mais comment préserver la continuité d'un écosystème complet face à des dépendances numériques structurelles.

Construire une souveraineté fondée sur la maîtrise des risques cyber

Sécuriser intégralement une *supply chain* de 12 000 fournisseurs est une ambition illusoire. Aucun groupe industriel, quelle que soit sa taille, ne dispose des ressources humaines, financières et techniques suffisantes pour auditer en permanence l'ensemble des acteurs de sa chaîne. Les différences de maturité

[14] Jérôme Renoux, « Cyber-résilience : protéger les voyages aériens des chaos estivaux », *Le Journal du* Net, [en ligne]. URL : https://www.journaldunet.com/cybersecurite/1545859-cyber-resilience-proteger-les-voyages-aeriens-des-chaos-estivaux/

[15] Cigref, étude sur les dépendances numériques européennes, 2025 ; Léa Deseille, « La France lance son Observatoire de la souveraineté numérique », *ToutеL'Europe*, [en ligne]. URL : https://www.touteleurope.eu/l-ue-dans-le-monde/la-france-lance-son-observatoire-de-la-souveraineté-numerique-pour-renforcer-l-independance-technologique-europeenne/

cyber entre un grand sous-traitant de rang 1 et une PME de rang 3 ou 4 sont considérables et souvent impossibles à combler dans des délais raisonnables.

C'est pourquoi l'enjeu doit être reformulé. Il ne s'agit pas de supprimer toute vulnérabilité, ce qui est impossible, mais d'identifier les maillons les plus critiques, de réduire les dépendances les plus exposées et de renforcer la capacité à réagir vite en cas d'incident. Cette logique est celle de la résilience : la capacité d'un système à continuer de fonctionner malgré une perturbation, à absorber le choc, puis à se rétablir[16].

L'approche dite *zero trust* s'inscrit directement dans cette logique. Son principe : ne faire confiance par défaut à aucun utilisateur, aucun appareil, aucune requête, même à l'intérieur du réseau interne. Chaque demande d'accès est vérifiée, chaque connexion est contrôlée. Dans un environnement où les interfaces entre fournisseurs, sous-traitants et donneurs d'ordre se sont multipliées, cette architecture devient une réponse adaptée à la complexité des menaces actuelles[17].

Depuis plusieurs années, le cadre réglementaire européen pousse les acteurs industriels à élever leur niveau d'exigence en matière de cybersécurité. La directive NIS2, adoptée en 2022 et transposée dans la majorité des États membres depuis mars 2025, renforce les obligations applicables aux secteurs critiques : mise en place de mesures de gestion du risque cyber, obligation de déclarer tout incident significatif dans un délai de 24 à 72 heures, et réalisation d'audits réguliers de conformité[18].

En France, ce mouvement se prolonge avec le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, en voie d'adoption à l'Assemblée nationale[1819]. Ces textes ne sont pas de simples obligations administratives et politiques : ils constituent un socle commun de sécurité collective, dont la portée dépasse chaque entreprise prise individuellement. Accompagner

---

[16] « Réglementation en matière de cybersécurité dans l'UE en 2025 : comprendre NIS2, DORA et ISO 27001 », *bconnex*, [en ligne]. URL : https://bconnex.com/articles/reglementation-en-matiere-de-cybersecurite-dans-lue-en-2025-comprendre-nis2-dora-et-iso-27001/

[17] Larousse, définition de la résilience : « Capacité d'un système à continuer à fonctionner, même en cas de panne. »

[18] *Journal du Net*, op. cit. ; « Compagnies aériennes et cybersécurité : êtes-vous prêts face aux nouvelles menaces ? », *Thales*, [en ligne].

[18] « ORION 26 : les cybercombattants des armées à la manœuvre », *Ministère des Armées et des Anciens Combattants*, [en ligne]. URL : https://www.defense.gouv.fr/comcyber/orion-26-cybercombattants-armees-manoeuvre

[19] Contrat de 250 millions d'euros sur huit ans, conduit par ADS et Neverhack. « Airbus décroche un contrat pour former les "cyber commandants' des forces armées", *Capital*, [en ligne]. URL : https://www.capital.fr/entreprises-marches/defense-airbus-decroche-un-contrat-pour-former-les-cyber-combattants-des-forces-armees-1516043

ses fournisseurs dans cette montée en conformité est désormais une responsabilité que les grands maîtres d'œuvre du secteur de la défense ne peuvent plus déléguer.

La réponse opérationnelle s'articules autour de plusieurs axes complémentaires. D'abord, la formation et la montée en compétences des cybercombattants : en juillet 2025, Airbus a décroché un contrat de 250 millions d'euros sur huit ans avec le ministère des Armées pour former et entraîner les experts en cyberdéfense au sein du COMCYBER de Rennes, en co-traitance avec Neverhack[8]. Ce centre d'entraînement permet de simuler des scénarios d'attaque-défense en conditions réalistes, et de préparer les opérateurs à réagir sous pression.

Au-delà de la formation, c'est la pratique régulière de la simulation qui s'impose comme un pilier de la résilience. L'exercice interarmées ORION 26, organisé par le COMCYBER, illustre cette démarche : en mettant des unités en situation réelle de cyberattaque dans un contexte de haute intensité, il permet de tester la robustesse des systèmes, d'identifier les failles dans les protocoles de réaction et d'améliorer la coordination avec les dispositifs otaniens[11]. Ces exercices valent autant pour la défense nationale que pour les grands industriels : face à des attaques de plus en plus sophistiquées, la préparation ne peut plus reposer sur le seul déploiement technologique.

Conclusion

La *supply chain* est devenue l'un des terrains d'affrontement les plus actifs du cyberespace. Pour des acteurs comme Airbus Defence and Space, dont les activités croisent à la fois les enjeux industriels, défensifs et souverains, la sécurisation de cette chaîne n'est plus une question technique parmi d'autres : c'est un impératif stratégique.

La sécurisation totale est, et restera, une illusion. Ce qui est en revanche possible, et nécessaire, c'est de construire une résilience durable, qui passe par : l'identification des maillons critiques, la réduction des dépendances les plus exposées, l'imposition de standards contractuels aux fournisseurs, l'anticipation des crises par la simulation et une réaction rapide quand l'attaque survient. En parallèle, la réduction de la dépendance numérique envers les acteurs extra-européens, portée notamment par

l'Observatoire de la souveraineté numérique lancé en janvier 2026, ouvre une voie structurelle vers davantage d'autonomie stratégique[20].

En définitive, la souveraineté ne se mesure plus à la capacité de tout contrôler. Elle se mesure désormais à la capacité d'absorber les chocs, de rebondir et de ne jamais perdre la main sur ses vulnérabilités essentielles. Dans un contexte de haute intensité et de tensions géopolitiques durables, c'est cette résilience maîtrisée qui constitue la véritable puissance industrielle.

« Nous ne pouvons plus construire des systèmes comme si rien ne pouvait y pénétrer. Un adversaire déterminé entrera toujours. Développer des systèmes résilients capables de se reconfigurer est devenu un impératif. » - Général d'armée Thierry Burkhard, alors chef d'état-major de l'armée de Terre, CyberCercle, mai 2021

À propos de l'autrice : Lydie Pérusin est étudiante en master 2 de Relations internationales, parcours Sécurité-Défense, à l'Université Catholique de Lille. Membre du Comité Aéronautique et Espace, elle rédige actuellement un mémoire consacré aux enjeux stratégiques de l'aéronautique française à l'horizon 2050 dans le cadre d'une guerre de haute intensité et souhaite à terme s'engager au sein des forces armées.

[20] Assemblée nationale, projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (dossier DLR5L17N50731), 2025. ; Léa Deseille, « La France lance son Observatoire de la souveraineté numérique pour renforcer l'indépendance technologique européenne », *ToutеL'Europe*, [en ligne]. URL : https://www.touteleurope.eu/l-ue-dans-le-monde/la-france-lance-son-observatoire-de-la-souverainete-numerique-pour-renforcer-l-independance-technologique-europeenne/

Rédigé par : Yona EL FASSY

LE DROIT PÉNAL DES AFFAIRES COMME LEVIER STRATÉGIQUE DE RÉSILIENCE FACE À L'IMMATÉRIALITÉ DE LA MENACE CYBER

Face à la montée en puissance des cybermenaces systémiques visant les industries de défense, la présente étude analyse le rôle du droit pénal des affaires comme levier stratégique de résilience. À travers l'examen du bloc de légalité cyber formé par la directive NIS 2, la Part-IS et le cadre OIV issu de la LPM 2024-2030, il est démontré que la conformité réglementaire constitue désormais une obligation pénale de résultat engageant personnellement les dirigeants. L'étude aborde ensuite les défis d'imputation propres à l'IA offensive et les tensions probatoires inhérentes au secret de la défense nationale, avant de proposer une doctrine de conformité proactive — fondée sur l'audit documenté, la gouvernance algorithmique du SOC et la préparation opérationnelle à l'état de nécessité — permettant de transformer le risque pénal en bouclier de défense. Il en résulte que le droit pénal, traditionnellement répressif, peut être retourné en instrument d'anticipation stratégique au service de la souveraineté industrielle et nationale.

L'époque où la cybermenace se limitait à un « bruit de fond » numérique est définitivement révolue. La menace est désormais protéiforme et systémique : elle émane d'États-nations pratiquant l'espionnage industriel à grande échelle ou de groupes cyberterroristes visant à paralyser les capacités de défense européennes. Dans ce théâtre d'ombres, la cybersécurité n'est plus un simple défi technique ; elle est le socle de la résilience nationale.

Pourtant, la conformité réglementaire est souvent perçue comme un carcan administratif fastidieux, une liste de cases à cocher déconnectée du terrain. Cette vision est une erreur stratégique. Sous l'impulsion de la directive NIS 2 (décembre 2022) et de la Part-IS (règlements (UE) 2023/203 et (UE) 2022/1645), le cadre normatif s'est durci pour devenir un véritable impératif de souveraineté. Ces textes ne sont pas de simples contraintes : ils dessinent un nouveau régime de responsabilité où la négligence numérique est traitée avec la même sévérité qu'une trahison ou une mise en danger de la vie d'autrui. Pour les industriels, respecter ces normes n'est plus une question d'audit, mais une question de survie opérationnelle et juridique. La conformité devient alors une arme de défense : elle transforme le droit pénal, traditionnellement répressif et intervenant a posteriori, en un levier stratégique de résilience a priori. Dès lors, une question centrale émerge : comment le droit pénal peut-il se muer en un bouclier

capable d'anticiper les attaques, de protéger les dirigeants et de sanctuariser la reconstruction d'un géant industriel face à l'immatérialité du risque cyber ?

Si le corpus normatif NIS 2/Part-IS a érigé la cybersécurité en obligation pénale de résultat engageant personnellement les dirigeants (Partie I), les industriels doivent maîtriser l'arsenal répressif des STAD (système de traitement automatisé de données) face à l'IA offensive pour transformer la judiciarisation en arme (Partie II), afin de démontrer in fine que le droit pénal peut être retourné en levier proactif de résilience (Partie III).

L'expansion de la responsabilité pénale : de la sécurité des vols (safety) à la « cyber safety »

Cette partie analyse la transformation progressive de la conformité technique en un impératif de survie pénale. Sera d'abord examiné le bloc de légalité cyber (1.1) composé de NIS 2 et de la Part-IS, renforcé par le cadre OIV (Opérateur d'Importance Vitale) de la Loi de Programmation Militaire, avant d'aborder la responsabilité des dirigeants (1.2) face au verrouillage des délégations de pouvoirs. Sera enfin analysée la cristallisation de la mise en danger d'autrui (1.3) par l'assimilation de la cybersécurité à la sécurité des vols.

Le bloc de légalité cyber : NIS 2, Part-IS et cadre OIV/LPM comme normes de référence pénale

La question de l'articulation entre conformité réglementaire et responsabilité pénale ne peut être abordée sans identifier avec précision les textes qui constituent désormais le standard de conduite opposable aux industriels. Ces instruments forment un « bloc de légalité cyber » au sens où ils définissent ce qu'est une diligence normale en matière de sécurité des systèmes d'information : leur méconnaissance suffit à caractériser la faute pénale, sans qu'il soit besoin de démontrer une intention coupable au sens strict.

La directive NIS 2 (directive (UE) 2022/2555 du 14 décembre 2022) constitue le pivot de ce dispositif. Elle impose aux entités essentielles du secteur de la défense une obligation de gestion des risques cyber incluant la sécurité de la chaîne d'approvisionnement (art. 21, § 2, point d), la gestion des incidents, la continuité des activités et la sécurité des ressources humaines. Sur le plan pénal, le mécanisme est plus subtil : le manquement aux mesures imposées par NIS 2 constitue une faute caractérisée au sens de l'article 121-3, alinéa 4, du Code pénal, dès lors que ce manquement a exposé autrui à un risque d’une

particulière gravité que l'auteur ne pouvait ignorer. La jurisprudence (CA Chambéry, 13 janvier 2010, n°009/00389 ; JurisData n°2010-001453) précise que la faute caractérisée suppose une imprudence d'une gravité telle que son auteur ne pouvait en ignorer le risque. La responsabilité pénale de la personne morale peut en outre être engagée par capillarité via la supply chain : une imprudence caractérisée dans la sélection ou le contrôle d'un sous-traitant de rang 2 ou 3 peut suffire à exposer la société-tête, la directive imposant que la sécurité de la chaîne d'approvisionnement soit traitée comme une composante à part entière de la gestion des risques (Lepage, 2022, p. 45).

La Part-IS (règlement délégué (UE) 2022/1645 du 14 juillet 2022 et règlement d'exécution (UE) 2023/203 du 27 octobre 2022), instrument de l'Agence européenne de la sécurité aérienne (EASA, 2024), constitue la pièce maîtresse du dispositif. En liant juridiquement la cybersécurité à la sécurité des vols, elle opère une translation conceptuelle fondamentale : les standards de sécurité des systèmes d'information aéronautiques deviennent des « obligations particulières de sécurité prévues par la loi ou le règlement » au sens de l'article 223-1 du Code pénal.

Cette qualification repose sur un double ancrage normatif qui la verrouille : vers le haut, la Part-IS tire sa force obligatoire du droit primaire de l'Union et du règlement de base (UE) n°2018/1139 du 4 juillet 2018, lui conférant une valeur supérieure à la loi nationale ordinaire en vertu du principe de primauté consacré par l'article 88-1 de la Constitution et de son applicabilité directe au sens de l'article 288 TFUE, sans transposition nationale préalable ; vers le bas, elle se traduit par des obligations précises et directement opposables, l'article 5 du règlement d'exécution (UE) 2023/203 imposant explicitement que les mesures de sécurité informatique ne compromettent pas la sécurité des vols.

Comme le souligne Quéméner (2023), l'article 223-1 n'exige pas que la norme soit d'origine française ; il exige qu'elle soit contraignante et précise. Ces deux conditions étant réunies, le bit corrompu qui compromet un système de navigation embarqué n'est plus une abstraction technique, mais la violation d'une obligation de sécurité aussi directement opposable que l'obligation de vérifier l'état des trains d'atterrissage avant un vol. Leur méconnaissance délibérée est dès lors susceptible de constituer non seulement une faute caractérisée au sens de l'article 121-3, mais également une mise en danger délibérée d'autrui, infraction intentionnelle punissable d'un an d'emprisonnement et de 15 000 euros d'amende.

Les dates d'application respectives ne constituent pas un délai de grâce, mais une période d'adaptation dont l'inexploitation serait elle-même constitutive d'une faute caractérisée (Laux, 2023). Le cadre OIV issu de la loi n°2023-703 du 1er août 2023 relative à la programmation militaire pour les années

2024 à 2030 (LPM 2024-2030) complète ce socle normatif en imposant des obligations de résilience opérationnelle spécifiques aux opérateurs d'importance vitale.

En vertu des articles L. 23212 et suivants du Code de la défense, tels que renforcés par la LPM 2024-2030, les OIV sont astreints à des tests de détection et de résilience de leurs systèmes d'information critiques, réalisés sous l'autorité et le contrôle de l'ANSSI. L'absence de ces tests, ou leur réalisation purement formelle, peut être qualifiée d'imprudence majeure en cas de sinistre cyber, dans la mesure où le législateur a expressément consacré ces obligations comme composante de la diligence requise des OIV. Ainsi, les tests de résilience imposés par la LPM 2024-2030 ne constituent pas seulement une obligation professionnelle ou formelle : ils matérialisent, avant tout sinistre, la diligence que le juge pénal sera amené à apprécier a posteriori.

L'imbrication de ces instruments produit un effet cumulatif : NIS 2 établit le standard général de gestion des risques, la Part-IS verrouille la qualification pénale en assimilant la cybersécurité aéronautique à une obligation de sécurité de résultat, et le cadre OIV/LPM impose des obligations de résilience opérationnelle spécifiques dont le non-respect aggrave l'exposition pénale. Ensemble, ils transforment la conformité réglementaire d'une contrainte administrative en un impératif de survie pénale.

La responsabilité des dirigeants sous NIS 2 : la délégation de pouvoirs à l'épreuve du verrouillage légal

La directive NIS 2 introduit une rupture fondamentale avec la pratique antérieure en matière de gouvernance de la cybersécurité : elle « verrouille » la responsabilité personnelle des organes de direction, interdisant de fait le recours à la délégation de pouvoirs comme mécanisme d'exonération totale. L'article 20 de la directive impose en effet aux organes de direction des entités essentielles et importants d’approuver personnellement les mesures de gestion des risques cyber visées à l'article 21, d’en superviser la mise en œuvre et d'être tenus responsables en cas de manquement. Cette disposition est inédite dans sa portée : elle crée une obligation de compétence à la charge du dirigeant, qui ne peut plus se réfugier derrière son ignorance technique pour s'exonérer (Cabinet Dreyfus, 2024).

En droit pénal français, la délégation de pouvoirs constitue, depuis les arrêts fondateurs de la Chambre criminelle (Crim., 11 mars 1993, Bull. crim. n°112 ; Crim., 30 oct. 1996, Bull. crim. n°379), un mécanisme d'exonération de la responsabilité pénale du chef d'entreprise, sous réserve que la délégation soit précise, qu'elle soit conférée à un délégataire disposant de la compétence, de l'autorité

et des moyens nécessaires à l'exercice de sa mission. Sous NIS 2, ce mécanisme n'est pas supprimé, mais il est profondément reconfiguré : si le CEO peut déléguer l'exécution des mesures de cybersécurité au RSSI (Responsable de la Sécurité des Systèmes d'Information), il ne peut pas déléguer l'obligation d'approbation et de supervision que lui impose l'article 20 de la directive. En d'autres termes, la délégation peut produire un effet exonératoire sur l'exécution, mais non sur la gouvernance stratégique de la cybersécurité, qui demeure personnellement attachée au dirigeant.

La question de la délégation en cascade (PDG → DSI → RSSI) mérite ici un examen approfondi. Chaque maillon de la chaîne peut faire l'objet d'une délégation valide pour l'exécution des mesures techniques, sous réserve des conditions classiques de compétence, d'autorité et de moyens posées par la jurisprudence. Mais le « verrouillage » de l'article 20 de la directive NIS 2 demeure intacte à chaque niveau : ni le DSI ni le RSSI ne peuvent absorber la responsabilité d'approbation stratégique qui incombe personnellement au PDG. En cas de défaillance, le juge remontera nécessairement jusqu'au décideur qui a validé ou refusé les budgets et orientations de cybersécurité, quelle que soit la longueur de la chaîne de délégation. Dreyer (2022) souligne à cet égard que la distinction entre auteur matériel et auteur moral, fondamentale en droit pénal général, prend ici une acuité particulière : le dirigeant qui refuse les budgets nécessaires à la sécurité informatique est l'auteur moral d'une imprudence dont le RSSI ne peut assumer seul la charge pénale.

La jurisprudence de la Chambre criminelle du 27 octobre 2009 (n°09-82.346) ajoute une dimension supplémentaire en posant une présomption d'intentionnalité pour les infractions aux systèmes de traitement automatisé de données. Si cette jurisprudence vise principalement les auteurs d'intrusions, son raisonnement — la présomption d'intentionnalité déduite de la connaissance de l'obligation — nourrit symétriquement la caractérisation de la faute du dirigeant qui, informé de ses obligations légales par NIS 2, choisit délibérément de ne pas y satisfaire. La frontière entre la négligence grave et le dol éventuel est particulièrement ténue lorsque le dirigeant a été explicitement averti des risques et des obligations par ses équipes techniques.

Le risque de mise en danger d'autrui (art. 223-1 C. pén.) : la consécration pénale de la « cyber safety »

L'article 223-1 du Code pénal sanctionne d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'exposer directement autrui à un risque immédiat de mort ou de blessures de nature à entraîner une mutilation ou une infirmité permanente par la violation manifestement délibérée d'une obligation

particulière de prudence ou de sécurité imposée par la loi ou le règlement. L'entrée en vigueur progressive de la Part-IS (EASA, 2024) confère à cette disposition une portée radicalement nouvelle pour le secteur aéronautique : les standards de cybersécurité qu'elle impose pourraient devenir ipso facto des « obligations particulières de sécurité imposées par le règlement » au sens de l'article 223-1, produisant ainsi la jonction juridique entre la sécurité des systèmes d'information et la sécurité des vols.

Pour vérifier que la Part-IS satisfait la première condition de l'article 223-1, il convient de démontrer pourquoi ses dispositions constituent bien des obligations « particulières » au sens de la jurisprudence pénale française. La Chambre criminelle exige que l'obligation soit précise, identifiable et directement applicable — non une norme de comportement générale.

L'article 5 du règlement d'exécution (UE) 2023/203 répond à cette exigence en imposant explicitement que les mesures de sécurité informatique ne compromettent pas la sécurité des vols : il s'agit d'une obligation précise, dont la violation est objectivement constatable, portant sur un risque clairement identifié pour des personnes physiques déterminées (passagers, équipages).

La doctrine (Quéméner, 2023) confirme que des règlements européens sectoriels d'application directe peuvent constituer de telles obligations particulières, dès lors qu'ils prescrivent un comportement précis dont la méconnaissance est susceptible d'exposer des personnes à un risque concret.

On opère ainsi ce que l'on peut appeler une matérialisation pénale de l'immatériel : le bit corrompu, la faille dans un système embarqué ou l'intrusion dans un réseau de contrôle sont juridiquement assimilés à une pièce mécanique défectueuse sciemment laissée en service. L'immatériel (le code informatique) doit être traité avec la même rigueur de sécurité que le matériel (le composant physique).

Pour que la qualification de mise en danger délibérée d'autrui soit retenue, la jurisprudence exige la réunion de trois éléments cumulatifs : une obligation particulière de sécurité imposée par la loi ou le règlement, une violation manifestement délibérée de cette obligation, et l'exposition directe d'autrui à un risque immédiat de mort ou de blessures graves. La Part-IS satisfait la première condition dans les conditions qui viennent d'être exposées ; la seconde sera caractérisée dès lors que le manquement résulte d'un choix conscient de l'opérateur — refus d'appliquer une mise à jour de sécurité connue, maintien en service d'un système dont la vulnérabilité a été documentée par un audit — et non d'une simple erreur technique imprévisible.

Quéméner et Charpenel (2022) soulignent que la qualification délibérée est facilement établie lorsque l'opérateur a été préalablement informé de la vulnérabilité, par exemple via les alertes de l'ANSSI

(Panorama de la cybermenace 2023) ou les rapports d'audit internes. La troisième condition — l'exposition directe à un risque immédiat — est celle qui distingue la mise en danger de la simple imprudence. Dans le contexte d'un système de navigation compromis par une cyberattaque sur un aéronef en service, cette condition est sans difficulté caractérisée. Pour les systèmes de production ou desimulation, en revanche, l'immédiateté du risque devra être démontrée par un lien de causalité direct entre la défaillance informatique et le danger pour des personnes physiques : la paralysie d'un ERP administratif ne saurait satisfaire cette condition, faute de lien direct avec un risque corporel immédiat.

C'est pourquoi la cartographie des systèmes critiques, imposée par l'article 4 du règlement délégué (UE) 2022/1645, constitue à la fois une obligation réglementaire et un outil de gestion préventive du risque pénal : elle permet à l'industriel d'identifier, en amont de toute crises, les systèmes dont la compromission est susceptible d'engager la qualification de l'article 223.

L'arsenal répressif face à l'agression des réseaux : les STAD et l'IA offensive

Face aux agressions systémiques, le droit pénal sert de bouclier répressif pour l'industriel. Sera détaillée la qualification de STAD renforcée par la LPM 2024-2030 (II.1), puis analysé le défi de l'imputation face à l'IA offensive (II.2). Sera enfin traitée la « guerre des preuves » (II.3), où la nécessité de poursuivre l'attaquant se heurte à la protection du secret de la défense nationale.

La qualification de STAD des infrastructures critiques et la LPM 2024-2030

Un grand groupe industriel de la défense et de l'aérospatiale n'est pas seulement un sujet potentiel de responsabilité pénale ; il est avant tout, et structurellement, une cible privilégiée de la criminalité informatique d'État et des groupes cyberterroristes. Pour que la victime puisse espérer une réponse pénale efficace, encore faut-il maîtriser avec précision les qualifications applicables à ces atteintes, leurs éléments constitutifs et les conditions dans lesquelles la preuve peut être légalement administrée. Le régime des atteintes aux systèmes de traitement automatisé de données (STAD), codifié aux articles 323-1 à 323-7 du Code pénal, constitue le socle répressif de cette protection. L'article 323-1 punit l'accès ou le maintien frauduleux dans tout ou partie d'un système, qu'il soit ou non suivi d'une altération ou d'une extraction de données ; l'article 323-2 sanctionne les entraves au fonctionnement du système ; l'article 323-3 vise les suppressions et modifications frauduleuses de données.

S'agissant de l'élément moral, la Chambre criminelle (Crim., 27 oct. 2009, n°09-82.346) a bien posé une présomption d'intentionnalité. La constatation de la violation, sans motif légitime et en connaissance de cause, d'une des interdictions visées par l'article 323-3-1 implique l'intention coupable requise par l'article 121-3 du Code pénal. Cette présomption est particulièrement opérante dans le contexte des intrusions dans les systèmes d'un tel groupe : dès lors que l'attaquant a sciemment contourné les barrières de sécurité (pare-feux, authentifications multifactorielles, segmentations réseau), la connaissance du caractère protégé du système est présumée, et l'intention coupable avec elle. Cette présomption dispense souvent le parquet de devoir démontrer positivement l'intention malveillante, allégeant considérablement la charge probatoire dans les dossiers d'intrusion complexes (Quéméner, 2023).

Toutefois, il est important de rappeler que les prérogatives de l'ANSSI et le régime OIV relèvent du droit administratif — plus précisément d'une police administrative spéciale — et non du droit pénal. L'ANSSI intervient en tant qu'autorité administrative sur le fondement des articles L. 2321-2 et suivants du Code de la défense ; ses constats techniques et rapports d'intervention constituent des actes administratifs. C'est la passerelle entre ces deux ordres qui fait l'intérêt de la LPM 2024-2030 pour le sujet : les constatations techniques opérées par l'ANSSI dans le cadre administratif alimentent ensuite la procédure judiciaire pénale comme éléments de preuve.

En cas d'attaque visant un OIV, l'ANSSI peut accéder aux systèmes affectés pour caractériser la menace et collecter les preuves numériques permettant d'identifier les auteurs, preuves qui transitent ensuite vers le parquet ou le juge d'instruction par la voie du signalement prévu à l'article L. 2321-2-1 du Code de la défense. Cette articulation de l'administratif vers le pénal externalise une partie du travail d'investigation auprès d'une autorité dotée des compétences techniques et des habilitations de sécurité nécessaires, résolvant partiellement le problème de la collecte de preuves en environnement classifié développé en II.3.

La LPM 2024-2030 opère par ailleurs une aggravation substantielle des infractions STAD lorsqu'elles visent des OIV. En vertu du régime instauré par l'article L. 1332-1 du Code de la défense, la simple pénétration du système d'information d'un OIV est considérée comme portant une atteinte directe à la souveraineté nationale. Cette présomption de gravité produit deux effets juridiques distincts. D'une part, les circonstances aggravantes prévues à l'article 323-4-1 du Code pénal portent les peines à dix ans d'emprisonnement et 300 000 euros d'amende. D'autre part, elle facilite le recours aux techniques

spéciales d'enquête, notamment les perquisitions informatiques et les interceptions de données, en justifiant le recours à la procédure applicable à la criminalité organisée.

Une limite structurelle du régime STAD mérite enfin d'être soulignée. La qualification d'accès frauduleux suppose que le système soit effectivement protégé par des mesures de sécurité que l'attaquant a sciemment contournées. La jurisprudence dite « Bluetouff » (Crim., 20 mai 2015, n°1481.336) illustre cette exigence : la Chambre criminelle a précisé qu'un système accessible sans authentification préalable ne saurait être considéré comme suffisamment « protégé » pour caractériser l'infraction de l'article 323-1. Si l'entreprise n'a pas mis en place les mesures imposées par NIS 2, la Part-IS et la LPM, elle court le risque paradoxal que ses propres défaillances sécuritaires fragilisent la qualification pénale des intrusions dont elle est victime. Cette circularité renforce la thèse centrale de la présente étude : la conformité réglementaire proactive est conjointement un devoir légal, un bouclier pénal pour les dirigeants, et un prérequis à l'efficacité de la réponse pénale en cas d'agression.

L'IA offensive et le défi d'imputation (actus reus et mens rea)

Lorsqu'une attaque est orchestrée par un algorithme auto-adaptatif — malware polymorphe ou agent offensif de type APT piloté par machine learning —, la qualification pénale se heurte à une difficulté structurelle qu'il importe de ne pas surestimer : l'humain reste présent en amont, puisque quelqu'un a conçu l'outil, l'a entraîné et l'a délibérément déclenché. Ce qui se produit est une dislocation temporelle et causale entre l'intention initiale de l'assaillant et les effets concrets produits par la machine au moment de l'exécution, ce que l'on peut qualifier « [d'écran] algorithmique ».

Le vrai problème juridique est celui de l'articulation entre mens rea et actus reus. Prenons l'exemple concret d'un malware polymorphe déployé contre l'entreprise pour cibler le seul système de gestion des accès à un site de production majeur : l'IA, autonomisée une fois déclenchée, exfiltre en réalité des plans de conception classifiés non visés, propage l'attaque aux systèmes embarqués d'un sous-traitant et efface des données de maintenance. Le juge doit alors déterminer si ces effets non anticipés relevaient : du dol général (l'attaquant avait précisément voulu ces conséquences) ; du dol éventuel (il avait accepté le risque qu'elles surviennent) ou d'une simple imprudence consciente. Si les capacités d'exfiltration généralisée du malware étaient documentées et connues de l'opérateur avant le déploiement, le dol éventuel est caractérisé : l'attaquant avait accepté les conséquences prévisibles de son outil. Si ces capacités résultaient d'une évolution autonome de l'algorithme, imprévisible même pour

son concepteur, seule l'imprudence consciente peut être retenue. La distinction est déterminante, car elle conditionne directement la qualification pénale retenue et la sévérité de la sanction.

Ainsi, comme le souligne Caprioli (2022), le droit pénal devra évoluer vers une conception élargie de l'imputabilité englobant les effets structurellement prévisibles d'un système autonome déployé à des fins offensives. La tripartition concepteur / entraîneur / opérateur proposée par Bensoussan (2023), sans traduction formelle dans le Code pénal à ce jour, trouve néanmoins un écho dans le règlement européen sur l'IA (règlement (UE) 2024/1689 du 13 juin 2024, dit AI Act), qui distingue précisément le fournisseur, le déployeur et l'utilisateur avec des régimes de responsabilité différenciés (art. 16 à 29). Cette passerelle est précieuse : le concepteur du malware engagera sa responsabilité au titre de la complicité par fourniture de moyens (art. 121-7, al. 2, C. pén.) ; le déployeur assumera les conséquences prévisibles du déploiement au titre de la faute caractérisée (comme défini en 1.1) si les dérives étaient objectivement anticipables pour un opérateur raisonnable connaissant les capacités de l'outil.

Cependant, sur le terrain du droit positif, le recours à une analogie avec la responsabilité des « chefs de file » se heurte au principe de légalité criminelle (art. 111-3 C. pén.), qui interdit toute extension in malam partem. La prévisibilité objective des effets constituant l'élément-clé de l'imputation, le juge pourra en imputer la responsabilité à celui qui a choisi de déployer l'outil dès lors que ces dérives étaient objectivement prévisibles pour un opérateur raisonnable.

La « guerre des preuves » et le secret de la défense nationale

Pour obtenir la condamnation d'un attaquant, l'entreprise doit produire les preuves de l'intrusion — typiquement les journaux du SOC —, mais ces données révèlent simultanément l'architecture précise de ses réseaux de défense. Le procès risque ainsi de constituer une « seconde attaque », exposant publiquement les secrets techniques du constructeur. C'est ici qu'intervient le régime du secret de la défense nationale, dont le fondement textuel précis mérite d'être rappelé.

Ce régime repose sur la loi n°98-567 du 8 juillet 1998, codifiée aux articles L. 2312-1 à L. 2312-8 du Code de la défense, qui a institué la Commission consultative du secret de la défense nationale (CSDN). Lorsqu'une juridiction a besoin d'accéder à des documents classifiés dans le cadre d'une instruction, le juge ne peut les saisir directement ; il saisit la CSDN, qui rend un avis consultatif dans un délai de deux mois. C'est ensuite le ministre compétent — et non le Premier ministre — dont relève le document classifié qui décide de le déclassifier ou non, conformément aux modifications introduites par la loi

n°2009-928 du 29 juillet 2009. La politique générale de classification, quant à elle, relève du Premier ministre via le SGDSN, sur le fondement du décret n°2019-190 du 13 mars 2019 portant règlement général de la protection des informations classifiées, ce qui explique la confusion fréquente entre les deux niveaux d'intervention.

La constitutionnalité de ce dispositif a été expressément reconnue par le Conseil constitutionnel dans sa décision n°2011-192 QPC du 10 novembre 2011, qui a néanmoins posé l'exigence d'une conciliation équilibrée entre la protection des intérêts fondamentaux de la Nation et le droit à un recours juridictionnel effectif. Sur le plan européen, la CEDH a admis dans l'arrêt Jasper c. Royaume-Uni (16 février 2000, req. n°27052/95) que de telles restrictions probatoires pouvaient être compatibles avec l'article 6 de la Convention garantissant le droit à un procès équitable, à condition qu'elles soient strictement nécessaires et compensées par des garanties procédurales adéquates. Jean-Jacques Urvoas, Professeur de droit public et ancien garde des Sceaux (2023), précise à cet égard quelles peuvent être ces garanties compensatoires : recours à des experts habilités secret-défense, communication partielle de documents expurgés, ou encore intervention d'un juge ad hoc habilité à consulter les éléments classifiés sans les verser au débat contradictoire ; autant de voies permettant de préserver l’équilibre entre secret et équité procédurale exigé par l'article 6, § 1, CEDH.

Le secret de la défense nationale est ainsi une arme à double tranchant pour l'industriel en tant que partie civile : si la classification des journaux du SOC protège l'architecture réseau, elle prive en parallèle le juge des éléments nécessaires à la reconstitution de la chaîne causale de l'attaque et à la condamnation de l'auteur. Une voie médiane existe cependant, celle de l'anonymisation ou de la sanitisation des journaux techniques : des éléments probants peuvent être fournis sans exposer l'architecture complète, en occultant les adresses IP internes, les noms des systèmes critiques et les topologies réseau sensibles, tout en conservant les horodatages, les signatures de l'intrusion et les flux d'exfiltration constitutifs de l’infraction. Cette stratégie probatoire doit être anticipée dès la phase opérationnelle, bien avant toute procédure judiciaire. Le secret de la défense nationale et l'écran algorithmique identifié en II.2 se combinent en effet pour former une double barrière à la judiciarisation, dont l'entreprise doit mesurer les effets dès la conception de son dispositif de réponse aux incidents.

La stratégie de résilience : vers une conformité pénale proactive

La résilience de l'entreprise repose sur une conformité proactive transformant le risque pénal en levier de défense. Sera examiné comment l'audit de sécurité (III.1) constitue un bouclier probatoire, avant

d'aborder la responsabilité algorithmique du SOC (III.2). Sera enfin analysé l'usage de l'état de nécessité (III.3) comme fait justificatif permettant de légitimer les mesures d'urgence vitales lors d'une crise majeure.

L'audit de sécurité comme preuve d'absence de faute : le bouclier pénal

L'audit de sécurité régulier, imposé par la Part-IS (règlement d'exécution (UE) 2023/203), doit être instrumentalisé comme un bouclier pénal et non un simple outil de conformité administrative. La logique est celle de la preuve négative de faute : en documentant scrupuleusement le respect de l'état de l'art technologique, l'entreprise se constitue, avant tout incident, les éléments probatoires permettant d'écarter la faute caractérisée dont on a vu au II.2 que l'écran algorithmique complexifie l'établissement. La Chambre criminelle a en effet posé, dans son arrêt du 5 septembre 2000 (n°99- 82.301), que la faute caractérisée suppose une imprudence d'une gravité telle que l'auteur ne pouvait en ignorer le risque, ce qui signifie, a contrario, que la démonstration d'une conformité rigoureuse et documentée aux standards en vigueur neutralise cet élément constitutif. Et comme le soulignait Michèle-Laure Rassat (2017), puisque l'absence de faute ne se présume pas, c'est la raison pour laquelle ces audits documentés viennent servir de preuve.

Les tests de résilience opérationnelle imposés aux OIV par les articles L. 2321-2 et suivants du Code de la défense, renforcés par la LPM 2024-2030 et mis en œuvre sous l'autorité de l'ANSSI, constituent à cet égard une preuve de diligence opposable en cas de procès : ils matérialisent l'effort proactif d'identification et de correction des vulnérabilités, et s'inscrivent dans la logique de ce que la doctrine appelle la compliance défensive. La Part-IS impose par ailleurs, en son article 4 du règlement délégué (UE) 2022/1645, une cartographie des systèmes critiques et une évaluation périodique des risques dont la documentation constitue une pièce maîtresse du dossier de défense pénal.

Cette logique probatoire doit impérativement se prolonger dans la relation contractuelle avec les sous-traitants. Puisque la directive NIS 2, en son article 21, impose la sécurité de la chaîne d'approvisionnement comme composante des mesures de gestion des risques, alors la disparition de la faute peut produire un effet exonératoire. En effet, la diligence admet, par extension, la répartition contractuelle des responsabilités. Cependant, elle doit être réalisée sous différentes conditions : elle doit être précise, conférée à un cocontractant compétent et doté des moyens nécessaires. L'insertion de clauses d'audit et d'obligations de cybersécurité dans les contrats de sous-traitance de rang 2 et 3 permet

ainsi de transférer ou de partager la charge du risque pénal tout en renforçant la posture globale de sécurité, le tout en cohérence avec l'article L. 2321-3 du Code de la défense, qui impose aux OIV de contrôler la sécurité de leurs systèmes d'information critiques, y compris dans leur chaîne de valeur.

La gouvernance de l'IA de défense (SOC) et la responsabilité algorithmique

Les systèmes de détection automatisés du Security Operations Center utilisent l'IA pour bloquer les menaces en temps réel, mais cette automatisation défensive génère elle-même un risque pénal autonome qu'il y a lieu de maîtriser. Un « faux positif » algorithmique pourrait conduire à la déconnexion brute d'un système de navigation, d'un réseau de production ou d'une infrastructure critique, causant des dommages collatéraux susceptibles d'être qualifiés pénalement. Deux qualifications méritent d'être envisagées.

En premier lieu, si la déconnexion provoque un danger pour des personnes, l'article 223-1 du Code pénal sur la mise en danger délibérée d'autrui pourrait être mobilisé, dès lors que le fonctionnement de l'IA de défense constitue une violation d'une obligation particulière de sécurité — notamment celles découlant de la Part-IS, dont l'article 5 du règlement d'exécution (UE) 2023/203 impose que les mesures de sécurité informatique ne compromettent pas la sécurité des vols. En second lieu, si la déconnexion affecte les systèmes d'un tiers (un sous-traitant, un partenaire institutionnel), la qualification d'entrave au fonctionnement d'un STAD (art. 323-2 C. pén.) pourrait être retenue à l'encontre de l'OIV lui-même, victime devenue auteur par l'effet de son propre dispositif défensif.

Pour prévenir ce « risque de la réponse », la gouvernance de l'IA de défense doit garantir le maintien d'un contrôle humain effectif et traçable sur les décisions algorithmiques les plus critiques. La tripartition évoquée au II.2 pour l'attaquant se retourne ici contre l'OIV lui-même : en tant que concepteur, entraîneur et opérateur de son propre SOC, l'entreprise concentre les trois strates de responsabilité que le droit pénal cherchera à identifier en cas de dommage collatéral algorithmique. Cette exigence rejoint celle posée par l'article 14 de l'AI Act (règlement (UE) 2024/1689 du 13 juin 2024), qui impose une surveillance humaine renforcée (« human oversight ») pour les systèmes d'IA classés à haut risque, une journalisation automatique des décisions et une évaluation de conformité préalable au déploiement. La conformité à l'article 14 de l'AI Act constitue ainsi une preuve de diligence au sens de l'article 121- 3 du Code pénal, ce qui crée une incitation directe à documenter rigoureusement chaque décision algorithmique critique.

La reconstruction et l'état de nécessité (art. 122-7 C. pén.)

En cas de cyberattaque majeure paralysant les réseaux critiques d'un OIV, la direction pourrait se trouver contrainte d'accomplir des actes techniquement illicites : interception de communications, traitement de données personnelles sans base légale, accès à des systèmes tiers pour endiguer la propagation de l'attaque. L'article 122-7 du Code pénal offre ici un fait justificatif dont la portée, si elle est d'interprétation stricte, n'en est pas moins réelle : de jurisprudence constante de la Cour de cassation, l'état de nécessité se définit comme la situation dans laquelle une personne, pour sauvegarder un intérêt supérieur, n'a d'autre ressource que d'accomplir un acte défendu par la loi pénale, cet intérêt supérieur devant s'apprécier de façon objective, c'est-à-dire comme tel par tous. Or, la protection des capacités de défense nationales portées par un OIV (systèmes embarqués, programmes souverains, chaîne logistique de défense européenne) satisfait sans difficulté à cette condition d'objectivité : la sauvegarde de la souveraineté nationale et de l'intégrité des forces armées constitue précisément l'intérêt supérieur que nul ne saurait contester, et dont l'atteinte justifie, sous conditions, de déroger momentanément à l'ordre légal ordinaire.

Les conditions posées par l'article 122-7 (danger actuel ou imminent, nécessité impérieuse de l'acte, proportionnalité) trouvent par ailleurs un écho saisissant dans la jurisprudence administrative récente. Dans l'arrêt d'assemblée Ligue des droits de l'homme (CE, ass., 1er avril 2025, n°494511), le Conseil d'État a admis qu'une mesure dérogatoire aux droits fondamentaux pouvait être légalement édictée en situation de péril imminent, tout en exigeant qu'elle soit strictement proportionnée, provisoire et subsidiaire par rapport à toute alternative licite disponible. Transposé par analogie au fait justificatif pénal, cet enseignement impose aux industriels une discipline probatoire rigoureuse : chaque acte d'urgence accompli devra avoir été documenté en temps réel comme nécessaire, limité dans sa durée et conditionné à l'impossibilité de recourir à un moyen moins attentatoire ; ce qui signifie concrètement que la cellule de crise devra produire, dès la phase opérationnelle, les traces de la délibération ayant conduit à écarter toute alternative licite avant d'accomplir l'acte dérogatoire.

Cette convergence entre le fait justificatif pénal et la jurisprudence administrative n'est pas fortuite : elle reflète une logique commune aux deux ordres, que la théorie des circonstances exceptionnelles forgée par le Conseil d'État dans les arrêts Heyriès (CE, 28 juin 1918) et Dame Dol et Laurent (CE, 28 février 1919) a théorisée bien avant le droit pénal. Selon cette théorie, l'existence d'un péril grave et imminent justifie des dérogations temporaires à l'ordre légal ordinaire, à condition que la mesure soit strictement nécessaire et proportionnée. Le Conseil d'État a confirmé la vitalité de ce principe en

temps de paix dans l'ordonnance Syndicat Jeunes Médecins (CE, ord., 22 mars 2020), à l'occasion de la crise sanitaire, avant que l'arrêt d'assemblée Ligue des droits de l'homme (CE, ass., 1er avril 2025) n'en précise les conditions actuelles avec une exigence accrue de subsidiarité. Transposée au cas d'un acteur industriel, cette convergence doctrinale signifie que les actes dérogatoires accomplis en réponse à une cyberattaque majeure visant un OIV bénéficient d'une double légitimation : celle du fait justificatif pénal de l'article 122-7, et celle d'une tradition jurisprudentielle administrative constante reconnaissant la nécessité de déroger momentanément à l'ordre légal face à un péril objectif menaçant des intérêts supérieurs de la Nation.

C'est en ce sens que l'état de nécessité, loin d'être une échappatoire invoquée opportunément après les faits, peut devenir un instrument de résilience stratégique anticipé, à condition d'être préparé comme tel. Michèle-Laure Rassat (2017) et Emmanuel Dreyer (2022) s'accordent pour rappeler que le danger doit être objectivement caractérisé et non simplement redouté, et que la nécessité de l'acte — condition la plus délicate — ne se présume pas mais se démontre. Cela signifie qu'une doctrine interne de gestion de crise cyber, formalisée avant toute attaque et articulant les seuils de déclenchement des mesures d'urgence, leurs conditions de proportionnalité et leur durée maximale, constituerait non seulement un outil opérationnel, mais la preuve anticipée que l'état de nécessité, le jour où il serait invoqué, reposait sur une appréciation objective et raisonnée de l'intérêt supérieur de la Nation et non sur la seule réaction hâtive d'un état-major sous pression.

Conclusion

Le présent travail aura démontré que le droit pénal des affaires, loin de se réduire à un arsenal répressif intervenant après la catastrophe, constitue pour un grand groupe industriel de la défense et de l'aérospatiale un levier de résilience stratégique à triple détente.

En premier lieu, le bloc de légalité cyber formé par NIS 2, la Part-IS et le cadre OIV/LPM a définitivement effacé la frontière entre conformité technique et obligation pénale de résultat. Le dirigeant qui ignore ou sous-finance la cybersécurité de son organisation ne commet plus une simple négligence managériale ; il s'expose à une mise en cause pénale personnelle que la délégation de pouvoirs ne peut qu'atténuer, non absorber. La « matérialisation pénale de l'immatériel » opérée par la Part-IS, en assimilant le bit corrompu à la pièce défectueuse, constitue une révolution silencieuse dont les premiers contentieux n'ont pas encore révélé la pleine portée.

En deuxième lieu, la maîtrise des qualifications STAD, de l'écran algorithmique et de la stratégie probatoire face au secret de la défense nationale transforme le statut de l'entreprise de victime passive en acteur judiciaire actif. Cette circularité révèle une vérité plus profonde : dans le droit pénal cyber, la victime et le prévenu potentiel ne font souvent qu'un, ce qui fait de la conformité un impératif défensif à double face.

En troisième lieu, la conformité proactive, l'audit documenté, la gouvernance de l'IA défensive et la préparation opérationnelle à l'état de nécessité transforment le droit pénal d'un risque subi en un bouclier construit. L'entreprise qui documente sa diligence, structure ses délégations et anticipe ses faits justificatifs avant toute crise dispose d'un avantage décisif devant le juge.

Les évolutions législatives à venir ne feront qu'accentuer cette dynamique. La transposition de NIS 2 en droit français, dont le délai a expiré en octobre 2024, impose l'adoption de mesures nationales d'application, parmi lesquelles des décrets qui préciseront les obligations sectorielles et les sanctions pénales associées. La montée en puissance de l'AI Act, dont les dispositions relatives aux systèmes à haut risque deviennent pleinement applicables en août 2026, créera de nouvelles obligations de documentation algorithmique dont le non-respect sera susceptible d'alimenter la qualification de faute caractérisée. Enfin, l'évolution de la jurisprudence sur l'imputation algorithmique, que Caprioli (2022) préconise, dessinera progressivement les contours d'une responsabilité pénale adaptée à l'era de l'autonomie des systèmes. Pour un tel acteur industriel, anticiper ces évolutions plutôt que les subir est, désormais, une obligation stratégique autant que juridique.

Remerciements

Je tiens à adresser mes sincères et chaleureux remerciements à Gautier-Edouard FILARDO, Enseignant-Chercheur à l'Efrei, pour son accompagnement précieux, ses conseils avisés et son soutien constant tout au long de l'élaboration de ce travail. Sa disponibilité, sa rigueur intellectuelle et son expertise ont été d'une aide déterminante dans la conduite de cette réflexion. Qu'il trouve ici l'expression de ma profonde gratitude.

À propos de l'autrice : Après avoir découvert le milieu aéronautique au cours de sa licence de droit à Paris-Panthéon-Assas via l'association Les Ailes d'Assas, Yona cultive depuis un profond intérêt pour ce secteur. Afin d'en maîtriser davantage les enjeux réglementaires et économiques, elle a passé son BIA avant de rejoindre un Master de droit pénal des affaires. Aujourd'hui, elle a à cœur de lier les deux secteurs qui la passionnent : la compliance et l'aviation.