Le mot du Président

Chers membres et amis de l'association AED/SNC-IHEDN,

C'est avec un grand plaisir que je vous présente le neuvième numéro du bulletin Athéna. Ce bulletin est consacré des travaux intensifs et prospectifs réalisés par les comités de la 4e session nationale de l'IHEDN, 2024-2025. Cette session, intitulée *La France face aux ruptures stratégiques,* a permis de dresser un tableau détaillé des défis auxquels notre pays devra faire face dans les années à venir.

Les comités de la 61e session *Armement et économie de défense* (AED) et la 7e session *Souveraineté numérique et cybersécurité* (SNC) ont mené des analyses approfondies dans leurs domaines respectifs.

Pour les comités AED, les thèmes abordés incluent les transferts de technologies, les ressources en économie de guerre, le domaine spatial et l'intelligence économique. Ces sujets sont cruciaux pour assurer la sécurité et la compétitivité de la France dans un contexte international en constante évolution.

De son côté, les comités SNC se sont penchés sur des sujets d'une importance capitale pour notre avenir numérique, tels que l'ordinateur quantique, les opportunités du numérique et de l'IA, le développement numérique souverain, la cohésion nationale informationnelle, et d'autres innovations technologiques qui redéfiniront notre manière de vivre et de travailler.

Les synthèses des rapports présentés dans ce bulletin proposent des recommandations concrètes et actionnables pour faire face à ces ruptures stratégiques. Certaines de ces recommandations ont déjà été partagées lors de la communication Lundis de l'HEDN du 30 juin dernier, intitulée Les travaux de comité, contribution de l'IHEDN à la stratégie nationale.

Je tiens à remercier chaleureusement tous les membres des comités AED et SNC pour leur engagement, leur expertise et leur dévouement. Leur travail est essentiel pour préparer la France aux défis de demain et pour renforcer notre souveraineté et notre sécurité.

Je vous invite à lire attentivement ce bulletin et à vous approprier les recommandations qui y sont formulées. Ensemble, nous pouvons contribuer à bâtir une France plus résiliente et mieux préparée aux ruptures stratégiques qui nous attendent.

Très amicalement,

Géraud BRUN, Président de l'association AED/SNC-IHEDN

N'hésitez pas à faire part de vos réactions/commentaires/observations sur les articles de ce numéro et continuez à proposer des articles qui constitueront la matière des prochains numéros, en les envoyant à bulletin.athena@aed-ihedn.fr

L'association 3AED/IHEDN n'entend donner ni approbation ni improbation aux opinions émises dans les articles de ce Bulletin d'Athéna : ces opinions doivent être considérées comme propres à leurs auteurs.

Sommaire

Ce numéro est consacré aux rapports des quatre comités de la 61e session AED et des quatre comités de la septième session SNC de l'IHEDN. *Voir page 5*

Vie de l'association

Le dîner d'accueil des participants à la 62e session nationale AED, dîner qui constitue une des grandes traditions de notre se déroulera au Sénat le jeudi 6 novembre prochain. Jeune, moins jeunes, anciens, n'hésitaient pas à vous inscrire (inscriptions ouvertes sur notre site Web).

Messages de la rédaction

Chères auditrices/lectrices, chers auditeurs/lecteurs,

Plusieurs lecteurs souhaitent disposer d'informations sur les programmes d'armement. La rédaction fait donc appel aux responsables de ces programmes, qu'ils soient de la DGA, des armées et/ou de l'industrie, pour proposer des articles répondant à ce souhait, en restant bien sûr dans le cadre des informations ouvertes !

Gérard Dugard & Patrick Michon

Rendez-vous d'Athéna

L'association 3AED-IHEDN propose un rendez-vous mensuel autour de conférences qui permettent d'approfondir des questions en lien avec les thématiques d'économie de défense, d'armement, d'innovation et de géopolitique, avec des spécialistes reconnus dans leur domaine.
Nommé "Les Rendez-vous d'Athéna" en référence à la déesse de la stratégie militaire et de la sagesse chère à la communauté IHEDN, ce cycle est proposé aux membres de l'association à jour de cotisation et aux associations partenaires. Ces conférences sont organisées conjointement avec l'association de l'Armement terrestre (AAT) et avec le soutien de la société ALCIMED.

Ces conférences ont lieu au rythme d'une par mois. Leur organisation présente souvent quelques aléas (orateurs se décommandant car non-disponibles à la date prévue, cas le plus courant). Aller sur notre site Web pour voir les conférences d'octobre, novembre et décembre.

Ces conférences sont généralement enregistrées et consultables en replay sur notre site internet www.aed-ihedn.fr les tableaux qui suivent en donnent la liste des conférences de 2024 et 2025 disponibles.

PROGRAMME DES CONFÉRENCES POUR 2025		
Date	Thème	Commentaires
Mardi 21 janvier	Athéna #1 : L'évolution de la bataille balistique, enjeu des futurs conflits	Orateurs: Younik Thomas et Thomas Merlin (Arianegroup)
19 février	Athéna #2 : L'industrie en temps de guerre : RETEX Ukraine avec vision étatique et vision terrain	Orateurs: Géraud Brun & Xavier Tytelman
13 mars	Athéna # 3 : Éthique de l'IA	Orateur : Alexei Grinbaum (CEA)
15 avril	Athéna # 4 : Basculement climatique et conséquences pour les forces armées	IRIS Responsable du Programme Climat, Energie et Sécurité Orateurs : Julia Tasse et Mathilde Jourde (IRIS)
24 Juin	Athéna # 6 : Economie de guerre et anticipation stratégique.	Table ronde : animée par Grégory Chigolet (Conseiller économique de l'état-major des Armées) + IGA Walter Arnaud (DGA) + Dr Sylvain Moura (France Stratégie)
8 juillet	Athéna # 7 : La réserve opérationnelle industrielle Orateur : ICA Patrick GRELIER	

24 septembre	Athéna # 8 : La stratégie d'influence de la France au Magreb	Oratrice : Imen Chaanbi (consultante géopolitique zone Afrique MO)

CONFÉRENCES ATHÉNA EN 2024		
Date	Thème Intervenants	Commentaires
6 janvier	Athéna # 1 : Éthique et compliance dans les industries de défense	Corinne Lagache (Chief Compliance Officer Nexter)
25 janvier	RDV Odyssée « Résoudre les problèmes complexes »	Violette Faure Bouveret (Mecylium-Strategic Consulting)
28 février	Athéna # 2 : Une industrie nucléaire en pleine relance. Les enjeux en matière de sûreté nucléaire.	Stéphanie Guénot-Bresson (Commissaire de l'ASNR)
4 avril	Athéna # 3 : Quel Retex du conflit ukrainien en matière d'innovation ?	Xavier Tytelman (Consultant Aéronautique et Défense/Président de Aviation NXT France)
23 avril	Athéna #4 : Les armes absurdes	Patrick Michon (3AED-IHEDN- AAT)
21 mai	Athéna # 5 : Investissements, souveraineté et innovation	Table ronde animée par Géraud Brun (Président 3AED-IHEDN)
21 juin	MCO à Eurosatory	Table ronde animée par Valérie Bertheau (ancienne présidente 3AED-IHEDN)
2 juillet	Athéna #6 : Point de situation sur les ovnis- PAN	Table ronde animée par Luc Dini (3 AF)
24 septembre	Athéna #7 : Un musée maritime pour le XXIe siècle	Commissaire général Vincent Campredon
22 octobre	Athéna #8 : La péninsule arabique — des politiques d'armement évolutives	Emma Soubrier (Directrice PRISME, Chercheure associée Université Côte d'Azur)
19 novembre	Athéna # 9 : Économie de guerre et anticipation stratégique	Annulée — reprogrammée en 2025
20 décembre	Athéna #10 : Perspectives des activités spatiales et enjeux de la protection du Centre spatial guyanais	M. Jérome VILA (Maiaspace) — Général Le Bouil (Commandant supérieur des Forces armées de Guyane)

La France face aux ruptures stratégiques

Le présent bulletin d'Athéna est consacré aux synthèses (résumés exécutifs) des rapports des comités de la 4e session nationale majeure de l'IHEDN *Armement et économie de défense* (61e session CHEAR-AED) et *Souveraineté numérique et cybersécurité* (7e session SNC) .

Dans une approche prospective, ils analysent les ruptures stratégiques auxquelles la France sera confrontée, dans les champs :

- AED : transferts de technologies, ressources en économie de guerre, domaine spatial, intelligence économique ;
- SNC : ordinateur quantique, intelligence artificielle, technologies du numérique, cohésion nationale informationnelle.

Ils proposent des recommandations d'actions pour y faire face.

Chaque groupe de quatre résumés exécutifs est suivi d'une liste des membres de chaque comité;

Certains de ces travaux ont fait l'objet d'une courte présentation dans la communication *Lundis de l'HEDN* du 30 juin, intitulée *Les travaux de comité, contributions de l'IHEDN à la stratégie nationale.*

Travaux des quatre comités *Armement et économie de défense*

AED - Comité 1

Face aux ruptures stratégiques, quelle stratégie la France doit-elle adopter pour promouvoir un modèle de partage et de transfert de technologies à différents niveaux de coopération (UE, Otan, reste du monde) ?

La France est confrontée à des enjeux stratégiques complexes dans un environnement international marqué par des changements significatifs, notamment le ralentissement démographique en Occident, une compétition économique exacerbée et une pression croissante sur l'accès aux matériaux critiques ainsi qu'aux technologies avancées. De plus, afin de pallier ses limites financières et industrielles tout en maximisant son autonomie et sa souveraineté, la France a jusqu'à présent promu une stratégie de coopération qui reposait sur les exportations et les partenariats internationaux.

Ce modèle est confronté à plusieurs défis. Parmi ceux-ci figurent l'accroissement des exigences de compensations industrielles (ou offsets) imposées par les clients, la consolidation de concurrents industriels à travers les coopérations passées, ainsi que l'incertitude liée aux évolutions politiques des États partenaires. À ces difficultés s'ajoutent des bouleversements géopolitiques majeurs, tels que le retour des conflits de haute intensité, qui interrogent la pertinence et la résilience du modèle de coopération jusqu'ici adopté par la France.

Sur le plan budgétaire, la question des modalités d'accès aux financements européens et leur impact sur la Base industrielle et technologique de Défense (BITD) française constitue un enjeu central. Une participation active aux négociations portant sur les règlements financiers et programmatiques liés au cadre financier pluriannuel (CFP 2028-2034) de l'Union européenne (UE) s'avère indispensable afin de maximiser l'utilisation des outils communautaires en faveur des priorités françaises.

Par ailleurs, le développement et l'intégration des technologies de rupture, en particulier dans les domaines du numérique (intelligence artificielle, informatique quantique, etc.), nécessitent une analyse approfondie. Ces technologies, souvent situées hors des frontières européennes, en particulier dans la région indopacifique, soulèvent des interrogations sur la dualité technologique, la dépendance envers des fournisseurs externes, et les implications sur la souveraineté nationale. Dans ce contexte, il est impératif :

- de prendre en compte l'existant : les capacités mondiales de production de composants semiconducteurs, essentiels à la défense et à l'économie générale sont situés quasi-exclusivement en Indopacifique où la France dispose déjà d'intérêts territoriaux et économiques. Il convient donc d'avoir une stratégie ciblée sur la zone ;

– de préparer l'avenir dans un but de résilience au travers d'objectifs de réduction de cette dépendance en renforçant les capacités européennes et nationales.

En conclusion, dans un environnement international marqué par l'incertitude et des mutations rapides, la France doit adopter une approche proactive et coordonnée pour sécuriser ses intérêts industriels, technologiques et stratégiques. Cela passe par un engagement actif dans les cadres institutionnels européens, une maîtrise des enjeux technologiques, et une prise en compte des dimensions géopolitiques, notamment dans la région indopacifique.

Face à l'ensemble de ces facteurs internes ou externes, la France doit être capable de bâtir des coopérations de défense à l'horizon 2050 lui assurant la maîtrise dans le développement de technologies de rupture, ainsi qu'une sécurisation de ses approvisionnements et de ses capacités de production industrielle indispensables à sa souveraineté et sa sécurité nationale.

Pour cela, il est proposé comme stratégie que la France promeuve un modèle mixte de coopérations (communautaires et bilatérales), qui passe par la mise en place de structures de gouvernance et de coordination des efforts de développements technologiques entre les différents acteurs (gouvernement, entreprises, universités, centres de recherche). Cette gouvernance devra aider à élaborer une vision stratégique à long terme pour chaque type de technologies, avec des feuilles de route partagées, et permettre ainsi de guider les investissements. Ce modèle devra viser également à un établissement de doubles sources en Europe et dans la zone Indopacifique. Enfin, au vu du caractère essentiel de ces composants, il est nécessaire d'avoir une nouvelle stratégie d'investissement, post European Chips Act, visant à se doter dans un cadre européen des moyens de concevoir et fabriquer des semiconducteurs de nouvelle génération.

La feuille de route déclinant cette stratégie est orientée autour de cinq recommandations détaillées dans le présent rapport avec leurs 24 actions associées :

- **Recommandation** 1 : « planifier la coopération technologique de défense en prévoyant une revue décennale pour l'ajustement des partenariats mis en place ».
- **Recommandation** 2 : « renforcer les coopérations opérationnelles en Europe et en Indopacifique par le biais de déploiement de forces d'appui et d'exercices en coalition ».
- **Recommandation** 3 : « définir et mettre en place une stratégie de coopération ciblée en Indopacifique ».
- **Recommandation** 4 : « appuyer la promotion externe de la BITD française ».
- **Recommandation** 5 : « définir et mettre en place une stratégie de coopération dans le domaine technologique de la production des composants semi-conducteurs ».

Le présent rapport met en exergue une approche intégrée et ambitieuse visant à consolider la souveraineté et l'autonomie technologique et opérationnelle de la France et de l'Europe. À travers des stratégies concertées et prospectives, il souligne l'importance d'un alignement entre les principaux acteurs et d'une intégration des innovations technologiques dans le cadre de coopérations. Les recommandations formulées, allant de la planification technologique à l'instauration de partenariats dans la région indopacifique, reflètent une volonté manifeste de conjuguer progrès technologique et rayonnement stratégique. Sans occulter les risques et les renoncements associés, maîtrisés par des revues périodiques, ce cadre stratégique, articulé autour d'actions concrètes, ouvre des perspectives prometteuses pour relever les défis contemporains, tout en positionnant la France au sein de l'Europe comme un acteur central dans des domaines critiques.

AED - Comité 2

Face aux ruptures stratégiques, quelle stratégie la France doit-elle adopter pour disposer des ressources indispensables dans le cadre de l'économie de guerre ?

Contexte et sujet d'étude

Ces trois dernières années, le retour de conflits de haute intensité, marqué par l'invasion de l'Ukraine par la Russie et l'instabilité au Moyen-Orient, ont acté la transformation de l'environnement géostratégique mondial. Ce bouleversement remet en question les équilibres hérités de l'après-guerre, révèle les vulnérabilités européennes issues des « dividendes de la paix » en matière de défense et fait de nouveau émerger le concept d'économie de guerre, non plus réservé à la période de conflit ouvert, mais désormais étendu à la phase de préparation à celui-ci.

Dans ce cadre, le comité 2 a décidé de porter ses travaux sur la filière missilière française, représentant un domaine d'excellence stratégique, contrainte à s'adapter rapidement à la menace et représentative a priori des enjeux d'une économie de guerre. L'objectif défini est de s'assurer que la France dispose, d'ici 2040, de missiles adaptés à un conflit de haute intensité, dans lequel elle serait impliquée, en qualité et en quantité, tout en gardant la flexibilité pour reconfigurer l'outil industriel si ledit conflit était évité ou arrêté.

Analyse prospective

Dans ce contexte, et afin d'établir les scénarios prospectifs, deux variables ont été retenues :

- le niveau d'alliance (politique, militaire et économique) des concurrents stratégiques avec deux valeurs :
  - valeur minimale : des alliances bilatérales, au cas par cas entre certains concurrents stratégiques et pas systématiques,
  - valeur maximale : la mise en place d'alliances militaires et économiques structurées et semblables à ce qui a pu exister pendant la guerre froide avec le Pacte de Varsovie ;
- la vitesse d'évolution de l'engagement militaire en termes de doctrine et de technologie avec deux valeurs :
  - valeur minimale : il existe des innovations technologiques qui sont apportées aux systèmes d'armes, mais qui ne sont pas de nature à modifier significativement la façon de faire la guerre ;
  - valeur maximale : il existe des développements rapides de nouvelles armes et de modes de combats qui rendent obsolescents les systèmes actuels et obligent à une adaptation de la doctrine militaire.

Le croisement de ces deux variables a conduit à retenir deux scénarios prospectifs :

- scénario dit favorable « France au cœur d'un système d'alliances » : caractérisé par une intégration forte à l'Union européenne et à l'Otan, une BITD européenne consolidée, des chaînes d'approvisionnement sécurisées, avec une interrogation, la possibilité que l'effort de défense soit contesté par une population peu mobilisée. Dans ce scénario, la France est devenue le leader européen de la filière missile, mais doit, ce faisant, s'appuyer sur

des industriels européens pour une partie de ses approvisionnements ;
- Scénario dit dégradé « France isolée » : caractérisé par un désengagement américain, une fragmentation de l'Union européenne, des conflits multiples, des ruptures technologiques chez les concurrents, une nécessité pour la France de compter sur sa propre industrie avec une mobilisation nationale massive. La France se retrouve isolée politiquement et militairement, les autres industriels occidentaux travaillant eux en priorité au profit de leurs alliances.

Objectif stratégique et grands principes

Afin de répondre au mieux à l'un ou l'autre des scénarios, le cas pratique suivant a été retenu : l'objectif stratégique d'être capable de fournir aux armées des missiles adaptés et différenciés pour un conflit de haute intensité à l'horizon 2040. La stratégie proposée repose sur le développement et le renforcement d'une filière industrielle missilière dite « high-low mix » et composée des segments « haut du spectre » et « bas du spectre » avec les caractéristiques suivantes :
- **haut du spectre** : missiles de hautes performances pour contrer les menaces les plus élevées, pour les frappes dans la profondeur, la précision et la dissuasion ;
- **bas du spectre** : missiles rustiques produits en masse à bas coût pour répondre aux besoins d'attrition, permettant de contrer les munitions téléopérées ou les missiles/roquettes bas coût ainsi que les drones légers, et capables d'assurer une capacité de saturation.

Cet objectif stratégique repose sur les grands principes suivants :
- maintien de l'autonomie stratégique sur les capacités critiques (protection des intérêts vitaux, dissuasion) ;
- développement de partenariats européens pour les autres besoins ;
- développement simultané de deux segments (haut et bas du spectre), reposant sur des architectures modulaires, l'usage de technologies civiles, et la capacité à évoluer rapidement.

Synthèse des recommandations opérationnelles

La stratégie proposée conduit aux recommandations suivantes :
1. **Augmenter** les moyens de production en prévoyant des surcapacités industrielles et mobiliser l'industrie civile.
2. **Renforcer** les chaînes de sous-traitance en identifiant et traitant les goulets d'étranglement et en maintenant des stocks critiques sur l'ensemble de la chaîne.
3. **Réduire** les dépendances aux contrôles d'exportation, notamment américains, en soutenant l'autonomie européenne, en réduisant la dépendance aux matières premières et en anticipant les substitutions et les mécanismes de réquisition.
4. **Préparer** la Nation en développant des centres de formation mutualisés, en valorisant les métiers industriels de défense et en développant une réserve industrielle nationale.
5. **Optimiser** la conception des missiles via des spécifications simplifiées, orientées sur la productibilité notamment par l'utilisation de technologies éprouvées, d'architectures modulaires et l'intégration de composants civils.
6. **Renforcer** le soutien des PME/ETI, notamment grâce à des dispositifs financiers et faciliter les investissements dans la BITD pour les investisseurs privés ou institutionnels.
7. **Faciliter** l'accès au foncier industriel et la transition vers l'économie de guerre en capitalisant sur le cadre législatif ou réglementaire existant ou en l'adaptant.

AED - Comité 3

Face aux ruptures stratégiques, quelle stratégie la France doit-elle adopter pour identifier et pérenniser les technologies critiques pour les applications militaires dans le domaine spatial ? »

Le domaine spatial connaît des mutations profondes et rapides qui bouleversent l'équilibre des puissances établies. Alors que l'Espace devient un champ de conflictualité stratégique, marqué par la multiplication des acteurs et la diversité de leur profil, les ruptures technologiques et l'accroissement des dépendances industrielles, la France doit préserver son autonomie stratégique. La perte temporaire de son accès souverain à l'Espace entre 2023 et 2025, couplée à la montée en puissance des géants privés et étatiques internationaux met en lumière l'urgence de repenser son positionnement dans le domaine spatial militaire.

Dans ce contexte, la réflexion développée dans ce rapport et par notre comité tout au long de la session 2024/2025 de l'IHEDN, « Quelle stratégie la France doit-elle adopter pour identifier et pérenniser les technologies critiques pour les applications militaires dans le domaine spatial ? » revêt un intérêt évident. Ces technologies critiques conditionnent les capacités de défense futures de la France. L'objectif politique retenu à l'horizon 2035 est clair : garantir l'autonomie stratégique de la France dans le domaine spatial de défense. Cela implique de permettre aux forces armées françaises une liberté suffisante de compréhension, de décision et d'action dans, depuis et vers l'espace circumterrestre.

Cela se traduit par : une organisation efficace de la filière spatiale, un pilotage centralisé des partenariats, un modèle économique dual civil/militaire, l'identification et la sécurisation, d'ici 2028, des technologies critiques et ressources nécessaires à l'autonomie spatiale.

Ce cap stratégique s'appuie sur la notion de « juste suffisance » : la France renonce à certaines maîtrises technologiques non essentielles, acceptant des dépendances maîtrisées, en contrepartie d'une souveraineté ciblée sur les capacités jugées critiques.

L'analyse prospective de l'évolution du champ spatial dans les applications de défense conduit à retenir deux variables : la solidité de l'Union européenne (UE) dans le domaine spatial et l'accessibilité au domaine spatial.

La première reflète le degré de cohésion stratégique et industrielle au sein de l'UE, déterminant pour la mutualisation des moyens et la capacité à bâtir une souveraineté collective. La seconde variable traduit l'évolution du marché spatial, entre démocratisation technologique portée par le New Space et verrouillage stratégique par quelques acteurs dominants. Leur croisement permet de cartographier des futurs contrastés, allant d'une fragmentation compétitive à une gouvernance intégrée sous tension, et d'éprouver ainsi la robustesse des choix stratégiques face à des contextes incertains, mais plausibles.

De cette analyse prospective, deux scénarios principaux ont été construits :

- *pro se quisque* — une UE fragmentée dans un Espace à l'accès banalisé ;

- ***make EU First!*** — une UE solidaire, mais dans un Espace devenu restreint, monopolisé par quelques puissances dominantes.

Afin de tester au mieux les options disponibles, deux stratégies possibles ont été envisagées et confrontées aux scénarios :

- stratégie A — Big Brother ou l'intra-dépendance : viser une présence sur tous les segments spatiaux, en ne maîtrisant que certaines briques, et en comptant sur des partenariats profonds pour le reste ;
- stratégie B — Analyse et Efficacité Dirigées (AED) ou l'interdépendance : concentrer les moyens sur un nombre restreint de capacités souveraines et s'appuyer sur des partenariats ou des achats de services pour les autres.

Cette démarche méthodique conduit à retenir une version enrichie de la Stratégie B : elle privilégie une indépendance ciblée sur les capacités critiques, combinée à une veille à 360° de l'innovation spatiale, civile comme militaire, afin de détecter les ruptures technologiques futures. Cette stratégie est particulièrement résiliente face aux scénarios prospectifs, bien alignée avec les ressources financières disponibles et parfaitement à même de préserver l'autonomie opérationnelle des armées françaises, notamment en lien avec la mission de dissuasion.

Principes structurants :

- cartographie des besoins opérationnels, différenciant souveraineté et dépendances acceptables ;
- hiérarchisation des technologies critiques via la DGA, en partenariat avec le secteur civil ;
- soutien ciblé à la montée en maturité des briques technologiques critiques du domaine militaire ;
- révision cyclique (tous les trois ans) pour adapter l'effort stratégique aux évolutions technologiques ;
- coordination renforcée des acteurs publics et privés.

Les cinq recommandations opérationnelles du rapport s'inscrivent dans une logique cohérente avec la stratégie retenue d'interdépendance maîtrisée et d'indépendance ciblée, enrichie d'une veille à 360° sur l'innovation spatiale.

La première recommandation vise à

[1] **structurer** une gouvernance nationale cohérente et lisible, condition indispensable pour hiérarchiser les capacités à maîtriser souverainement et piloter les arbitrages entre ce qui relève de la souveraineté technologique et ce qui peut être acquis en coopération ou sur étagère du fait du caractère consubstantiellement dual de l'Espace.

Les deuxième et troisième recommandations renforcent respectivement

[2] **l'identification** précoce des technologies critiques et leur

[3] **financement** pérenne, répondant directement à l'exigence de consolider les segments jugés essentiels dans la stratégie.

La quatrième recommandation complète cette ambition en

[4] **sécurisant** les ressources non financières (compétences humaines, matières premières), qui conditionnent la pérennité à long terme des savoir-faire stratégiques.

Enfin, la cinquième recommandation, centrée sur

[5] **la** gouvernance des partenariats européens, vient activer le levier d'interdépendance choisie : elle permet à la France de renforcer ses capacités par des coopérations ciblées et équilibrées, sans remettre en cause son autonomie sur les segments critiques. Ensemble, ces recommandations créent un système articulé, robuste et agile, afin de préserver la souveraineté technologique française dans un écosystème spatial en pleine recomposition.

Cette stratégie vise à placer la France dans une position de puissance spatiale autonome et influente, capable de sécuriser ses intérêts de défense dans un monde en recomposition géostratégique. Elle appelle à une mobilisation forte, agile et coordonnée des acteurs publics comme privés, à l'échelle française et européenne.

AED - Comité 4

« Comment armer la France dans le domaine de l'intelligence économique offensive et du lobbying afin d'être leader du marché européen de défense d'ici 2040 ? »

Les menaces portant sur le potentiel industriel et technologique de la défense sont critiques et nécessitent, pour y faire face, des actions ambitieuses, structurées et robustes pour défendre les intérêts stratégiques de l'État, notamment dans un contexte de désinhibition de la violence.

Il s'agit notamment d'armer la France dans le domaine de l'intelligence économique (IE) offensive et du lobbying afin d'être leader du marché européen de défense d'ici 2040 (objectif stratégique). L'enjeu n'est rien de moins que de garantir la sécurité, la prospérité et la souveraineté du pays face aux menaces actuelles et futures.

En appliquant la méthode prospective de l'IHEDN, le comité a retenu deux scénarios extrêmes. Le premier ***Les marchands au service des princes*** est caractérisé par un retour des États-puissances, le développement de modèles dirigistes, dans lesquels quelques grands États mobilisent leur puissance économique, industrielle et financière, le repli protectionniste, la remise en cause des traités et organisations internationales dans un contexte de guerre commerciale exacerbée. Le second ***Les princes au service des marchands*** assume l'avènement d'un modèle ultra-libéral où des entreprises transnationales dominent les États. Ce scénario entérine l'effacement des États au profit d'un nouvel ordre mondial : fin des *États-providence*, fragmentation sociale, délégation de fonctions régaliennes au secteur privé.

Ces scénarios illustrent des futurs possibles où les dynamiques de pouvoir entre États et entreprises pourraient évoluer de manière radicale, influençant profondément les structures économiques, sociales et politiques mondiales. Aussi, pour atteindre l'objectif stratégique défini supra, considérant le nécessaire renforcement par la France de son ambition, le comité met en avant la stratégie visant à asseoir la position de leader de la France sur le marché européen de défense assurée par une utilisation assumée, décomplexée et adaptée de l'IE offensive tout en s'appuyant sur des capacités d'influence amplifiées et renforcées au sein des institutions européennes. (stratégie).

La mise en œuvre d'une telle stratégie nationale nécessite le déploiement d'actions coordonnées. Elle se décline en cinq lignes directrices (recommandations) qui sont détaillées dans le rapport :

- **Optimiser** l'action de « l'équipe France » au niveau européen en s'appuyant sur des communautés de destin, des coalitions de circonstance et la présence dans les instances européennes.
- **Renforcer** l'arsenal juridique, financier et économique pour défendre les intérêts européens et plus particulièrement français face à nos compétiteurs étrangers.
- **Coordonner** l'action au niveau interministériel tout en développant la culture IE et les outils au sein de chaque ministère.
- **Développer** une culture offensive de l'IE et en déployer les outils au profit des marchés d'armement et au sein de la BITD française et du MINARM.
- **Structurer** la filière IE au profit, notamment, de la sécurité économique des PME/ETI/

start-ups de la BITD en déconcentrant vers des structures publiques et privées locales ou sectorielles et en labellisant.

Les recommandations énoncées et les actions correspondantes permettent de répondre à la problématique. Elles présupposent une volonté politique forte afin de permettre à la France de préserver son outil de défense, devenu un facteur de puissance existentiel.

Membres des comités AED

Comité 1

Amargier Stéphane, DGA
Amate Maud, DGA
Decouvoux du Buysson Franc;ois, SGA
Dorbon Jean-Marie NavalGroup, rapporteur
Duclercq Julie, TERNWAVES
Gaime Fabrice, ARQUUS, secrétaire du comité
Gonzales Frédéric, armée de l'Air et de l'Espace
Knox Mark, US Navy
Le Goff Xavier, DGA
Richez Vincent, Conseil régional des Hauts-de-France
Volto Olivier, Airbus, président du comité
Tessaud Nicolas, DGA

Comité 2

Andrieu Grégory ;ICA, DGA ;
Bourdarias Clément ; ArianeGroup ; Responsable programmes systèmes d'information défense
Cabre Olivier ; Service de santé des Armées ; vétérinaire chef des services
Casasoprana Stéphanie ; Thales International SAS - Directrice marketing
Daux Matthieu ; ICA, DGA
Devos Ludovic ; Framatome - Directeur offres et gouvernance
Doithier Martin ; col. ministère des Armées ;
Lipski Michel ; col. armée de l'air et de l'espace
Mathelin Jean-Marie ; KNDS CBRN - Directeur général délégué
Morand Catherine ; Crédit Agricole SA - Responsable sanctions internationales
Parra Estelle ; Safran Electronics and Defense - Directrice du développement et de la R&T
Toth Kevin ; col. US Army ;

Comité 3

Beytout-Lamarque Coline, Croix-rouge française, Responsable adjointe DIH
Bonfils Olivier, KNDS, Directeur Industrie et Supply Chain
Chapeaux Thierry, armée de l'Air et de l'Espace, Chef du bureau « Contrôle export matériel de guerre »
Jousset Frédéric, Agence spatiale européenne, Chef de programme
Le Bras Florent, DGA, Directeur de programme et de segment de management
Martin Nicolas, Sopra Steria, Directeur commercial Défense
Remond Benjamin, DGA adjoint à la sous-directrice *Europe occidentale et Amérique du Nord*
Salmon Lionel, Thales, Directeur *Cybersécurité des systèmes d'information*
Schellenberger Raphaël, , Député du Haut-Rhin
Tevier de Beaune Caroline, DGA, Adjoint finances
de Vaulchier Guilhem, ministère des Armées, Chef de pôle

Comité 4

Bertrand Régis (rapporteur de comité), CNES
Carpentier Christophe, ICA DGA
Desgrees du Lou Geoffroy, col. armée de Terre
Galerneau Mathieu, Dassault Aviation
Guenin Céline, CV EMM
Khing Florent, État-major de l'armée de Terre
Lecat Pierre-Marie, ICA, DGA
Malvoisin Bénédicte, ministère des Armées et des anciens combattants
Meunier Sandrine, ICETA1 DGA
Plisson Thomas, Commissariat à l'énergie atomique et aux énergies alternatives
Reisch François (secrétaire de comité), MBDA
Suel Frédéric (président de comité), Marine nationale

Travaux des quatre comités
Souveraineté numérique et cybersécurité
La France au défi des ruptures stratégiques

SNC - Comité 1

Face aux ruptures stratégiques, quelle stratégie d'alliances et de partenariats la France doit-elle envisager afin de gagner en autonomie stratégique en matière cyber et numérique ? »

Penser les stratégies d'alliances et de partenariats à l'aune de l'amplification et de l'accélération de la transformation numérique

« *L'univers technologique se divise dans une nouvelle guerre froide entre l'Occident et la Chine, avec le monde émergent en arbitre* »[1]. Dans un podcast récent, le journaliste Pierre Haski revient sur les conséquences de l'affrontement commercial engagé par le président américain Donald Trump vis-à-vis de la Chine, qui aurait pour effet d'accélérer le découplage technologique de cette dernière et donc de réduire ses dépendances vis-à-vis du reste du monde. Le numérique est devenu, à l'instar d'autres dimensions stratégiques, un terrain de contestation des puissances. Si des logiques de découplage des chaînes de valeur technologiques sont à l'œuvre par les grandes puissances et les puissances moyennes (comme l'Union européenne), elles demeurent limitées et contraintes par les spécificités de ces chaînes de valeur qui induisent un degré minimum d'interdépendance. C'est pourquoi maîtriser la dimension stratégique numérique impose de penser en termes d'alliances et de partenariats, c'est-à-dire sous une forme de coopération qui offre divers niveaux d'intégration, et dans un rapport de confiance plus ou moins fort. Cela revient également à avoir une capacité d'accès et d'usage des technologies et d'en assurer la protection et donc leur cybersécurité.

Si la France possède de nombreuses forces dans le domaine du numérique (excellence de la recherche, industriels d'envergure mondiale, expertise en termes de cybersécurité notamment), elle n'en demeure pas moins une puissance moyenne dans cette compétition internationale en raison notamment de ses dépendances. Pour gagner en autonomie stratégique en matière cyber et technologique, la France doit réduire ces dernières sur un horizon à moyen et long terme et via une stratégie et feuille de route définies et exécutables. Au vu des interdépendances précitées, cet objectif passe nécessairement par une stratégie d'alliances et de partenariats ciblés sur des briques technologiques critiques.

1 HASKI, Pierre, « Poussée par la guerre commerciale de Trump, la Chine accélère son découplage technologique », France Inter, 1er mai 2025. Podcast disponible à l'adresse : https://www.radiofrance.fr/franceinter/podcasts/geopolitique/geopolitique-du-jeudi-01-mai-2025-9173970

Face à l'émergence potentielle à moyen terme d'un ordinateur quantique capable de remettre en cause la sécurité de nombreuses infrastructures numériques, il est choisi de s'intéresser plus spécifiquement à ce domaine technologique. D'autant que la recherche et le développement sur la chaîne de valeur de l'ordinateur quantique tendent à irriguer d'autres secteurs stratégiques du numérique. En cela, l'ordinateur quantique constitue un défi majeur pour maîtriser la dimension stratégique numérique.

À partir du cas structurant que constituent l'émergence et la généralisation de l'ordinateur quantique, est proposé un modèle de stratégie d'alliances et de partenariats, destiné à renforcer l'autonomie stratégique de la France dans ce domaine. Il est conçu pour être transposable à d'autres domaines technologiques critiques. L'objectif stratégique est de mettre en œuvre des alliances et des partenariats publics et privés ciblés aux niveaux national, européen et extraeuropéen, reposant sur la maîtrise de composants critiques de la chaîne de valeur de l'ordinateur quantique, pour disposer à l'horizon 2040 d'une capacité autonome. Cette ambition s'inscrit dans un contexte d'incertitude, alors même que la deuxième stratégie nationale sur les technologies quantiques tarde à voir le jour[2]. Ce rapport entend ainsi impulser une nouvelle dynamique pour éviter que la France ne soit reléguée au second plan dans la course mondiale à l'ordinateur quantique.

Aux croisements des enjeux géopolitiques, technologiques et sociétaux

Au regard de leurs effets structurants, cette stratégie est pensée à l'aune des ruptures stratégiques potentielles et de tendances de fond qui pourraient rebattre les cartes des chaînes de valeur technologiques et influer sur la capacité de la France à gagner en autonomie stratégique cyber et technologique. Si elles sont multiples, ce rapport s'est en particulier intéressé aux ruptures stratégiques dans les domaines géopolitique (notamment en termes de polarisation entre les États-Unis et la Chine, et d'émergence de puissances régionales) et technologique (notamment en termes de technologies de rupture : intelligence artificielle, quantique, robotique, etc.), ainsi qu'aux transformations profondes induites par le réchauffement climatique et la transition démographique. L'accès aux ressources, aux talents, aux capacités à investir et à se défendre dans un monde polarisé, est un enjeu que ces ruptures et tendances soulèvent avec une plus vive acuité dans le champ numérique. Dans ce domaine, elles conduisent à réévaluer les alliances traditionnelles, telles que l'Organisation du traité de l'Atlantique Nord (Otan) ou des organes internationaux, comme l'Organisation des Nations unies (ONU), et à inclure dans l'analyse aussi bien les puissances moyennes extraeuropéennes que les acteurs non étatiques, comme les grands acteurs technologiques (GAFAM, BATX[3]…), qui dominent et façonnent les évolutions numériques. Elles invitent également à penser la société dans son ensemble comme un acteur à part entière, avec des effets sur la population et une question profonde d'acceptabilité des arbitrages (et potentiellement des renoncements) que la stratégie pourrait induire.

Cinq variables clés ont été choisies pour approfondir cette analyse :

- l'acceptation des nouvelles technologies par la population ;
- la capacité d'alignement des États membres européens ;
- la conflictualité entre la Chine et les États-Unis ;
- la dépendance du marché européen aux technologies américaines ;
- la maîtrise de l'ordinateur quantique capable d'effondrer la sécurité des infrastructures numériques.

2 Institut Montaigne, « Quantique : vers une logique de marché », octobre 2024. Disponible à l'adresse : https://www.institutmontaigne.org/ressources/pdfs/publications/quantique-vers-une-logique-de-marche_0.pdf

3 Baidu, Alibaba, Tencent, and Xiaomi

Elles ont été retenues au regard de leur complémentarité et, pour certaines, leur caractère « cygne noir », c'est-à-dire du fait à la fois de leur rareté et de leur portée potentiellement considérable si elles se réalisaient.

Parmi elles, deux variables pivots ont été identifiées pour bâtir des scénarios permettant d'éprouver la stratégie : la conflictualité entre la Chine et les États-Unis et la maîtrise de l'ordinateur quantique capable d'effondrer la sécurité des infrastructures numériques. Ces variables permettent de couvrir à la fois les domaines technologique et géopolitique, mais aussi de générer les scénarios les plus extrêmes pour tester la robustesse de la stratégie. Il convient à ce titre de préciser que l'orientation sur l'ordinateur quantique visée a été précisée à l'issue de cette analyse prospective, qui en a fait ressortir le caractère structurant pour la dimension stratégique numérique. Les scénarios retenus ont permis d'éprouver la variabilité d'une stratégie d'alliances et de partenariats dans le champ numérique, entre un bloc occidental soudé, mais avec une autonomie stratégique forte de la France (scénario « La France, un partenaire particulier du bloc occidental »), et une France isolée et affaiblie dans la compétition internationale (scénario « La France, résiste, prouve que tu existes »).

Une alliance nationale, des partenariats entre États fondés sur trois cercles concentriques

Cette analyse prospective a également permis de faire ressortir un critère critique à prendre en compte dans l'établissement d'une stratégie d'alliances et de partenariats en matière technologique : le caractère dual ou non de la technologie. Si la technologie est duale et revêt donc une importance spécifique pour la sécurité nationale, il sera plus difficile de bâtir des alliances et les partenariats seront favorisés. C'est le parti pris que présente cette stratégie. Pour gagner en autonomie stratégique en matière cyber et technologique, elle repose en effet sur une double dimension :

- une stratégie d'alliances public-privé au niveau national avec les parties prenantes nationales impliquées dans la recherche et le développement de l'ordinateur quantique et la cybersécurité ;
- une stratégie de partenariats avec d'autres États et d'autres acteurs privés, qui repose sur trois cercles concentriques, du plus intégré au moins intégré :
  - un premier cercle paneuropéen de confiance structuré autour des Pays-Bas, du Royaume-Uni, de l'Allemagne et de la Finlande : ils sont choisis pour leurs compétences avancées et complémentaires dans les domaines de la recherche, des infrastructures quantiques, et de la cybersécurité ,
  - un second cercle articulé autour des pays du « Club Rafale » (partenaires de la France au Moyen-Orient, Inde, etc.), auquel est intégré le Canada du fait des intérêts partagés en matière d'ordinateur quantique : ce cercle exploite le réseau de partenariats déjà développé par la France, avec une extension naturelle des partenariats de défense existants et une consolidation de canaux diplomatiques et industriels ;
  - un troisième cercle constitué de partenariats choisis permettant de répondre à des enjeux ciblés (à titre d'exemple, sur des opportunités de marchés, de ressources humaines, de financement, etc.) : ce cercle doit permettre à la France de saisir des opportunités spécifiques sans engagement structurel lourd.

La structure adaptable de cette stratégie permet de répondre aux évolutions technologiques et surtout aux recompositions géopolitiques, assurant à la France une agilité précieuse face aux enjeux scientifiques, économiques et sécuritaires de l'ordinateur quantique.

Concernant le rôle de l'Union européenne, cette stratégie ne remet pas en cause l'engagement de la France à cette échelle, qui permet de donner un cadre et une impulsion aux États membres. Elle n'en fait toutefois pas le levier pivot pour atteindre l'objectif stratégique visé.

La stratégie retenue propose ainsi une trajectoire structurée en cinq phases :

Phase 1 - 2025-2026 : structuration et mobilisation nationale.

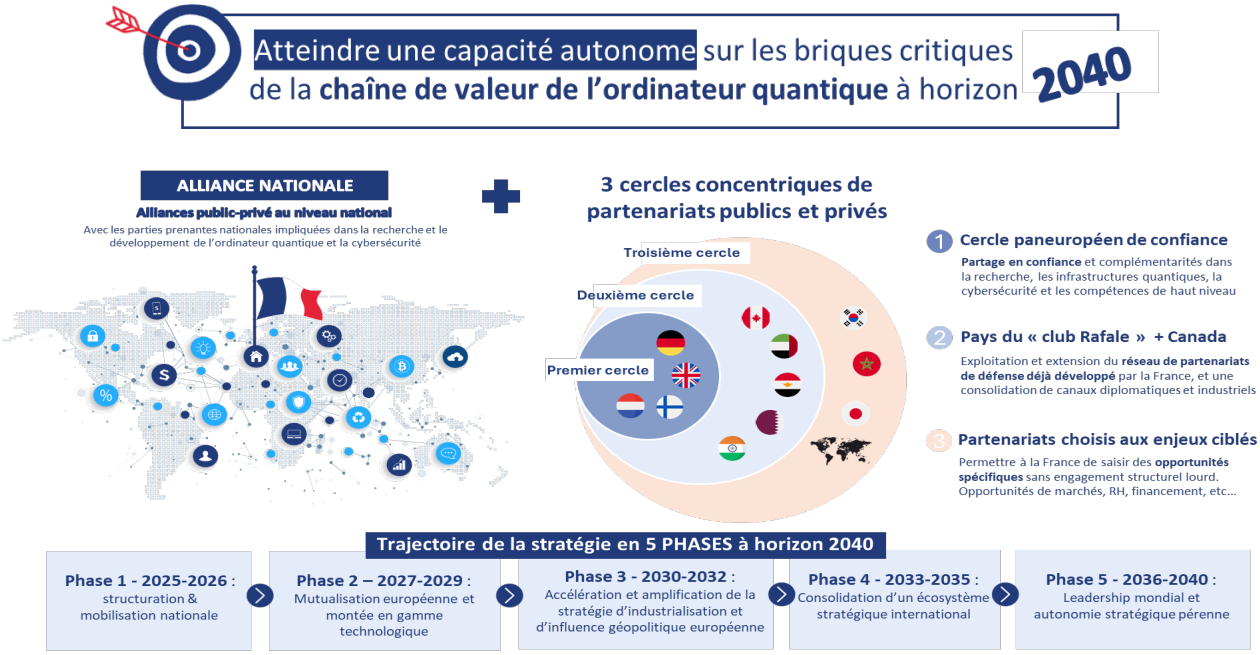
Phase 2 - 2027-2029 : mutualisation européenne et montée en gamme technologique.

Phase 3 - 2030-2032 : accélération et amplification de la stratégie d'industrialisation et d'influence géopolitique européenne.

Phase 4 - 2033-2035 : consolidation d'un écosystème stratégique international.

Phase 5 - 2036-2040 : leadership mondial et autonomie stratégique pérenne.

Ci-dessous une représentation synthétique de la stratégie retenue et de sa trajectoire à horizon 2040 :



Cinq recommandations qui incarnent différentes approches d'alliances et de partenariats

Au cœur de ces phases, cinq recommandations opérationnelles ont été retenues dans ce rapport, car elles illustrent de manière complémentaire l'articulation envisagée en termes d'alliances et de partenariats :

- **Recommandation** 1 — *Quantum for Good*, l'ordinateur quantique au service de la société : démocratiser la connaissance de l'ordinateur quantique et sa contribution aux défis sociétaux.
- **Recommandation** 2 — *Le Hub du quantique* : mettre en place une organisation « totem » de la France qui permettra d'assurer les actions de la stratégie nationale quantique en animant et coordonnant les acteurs et sites d'excellence existants sur le territoire national.
- **Recommandation** 3 — *Quantum startup for defence* : lancer, avec les partenaires du premier cercle, un programme de défense qui s'adresse aux startups françaises et eu-

ropéennes possédant une technologie critique dans la chaîne de valeur de l'ordinateur quantique.

- **Recommandation** 4 — « L'Airbus du quantique » : structurer un consortium européen autour de l'ordinateur quantique réunissant les États membres européens les plus avancés sur la chaîne de valeur de l'ordinateur quantique et les principaux acteurs industriels et académiques européens.
- **Recommandation** 5 — « Partenariats d'opportunités » : établir des partenariats « gagnant-gagnant » ciblés sur des dimensions critiques de la chaîne de valeur de l'ordinateur quantique, hors Europe.

SNC - Comité 2

Quelle stratégie la France doit-elle adopter pour maximiser les opportunités offertes par le numérique et l'IA dans les principaux domaines d'intervention de la puissance publique, notamment compte tenu des velléités d'activités régaliennes de la part des grandes plateformes et des progrès technologiques ?

Face aux ruptures stratégiques du numérique, la France doit adopter une stratégie ambitieuse pour préserver son modèle démocratique, en consolidant, avec ses alliés européens, une industrie numérique de confiance performante à l'horizon 2040.

Cette situation d'urgence impose un choix stratégique clair, qui doit conjuguer réalisme et ambition pour faire de l'Europe une puissance respectée, tout particulièrement dans le numérique, et construire une alternative crédible aux modèles américain et chinois.

Contexte : le défi des ruptures stratégiques

Les grandes plateformes numériques développent des velléités d'activités régaliennes et concentrent un pouvoir technologique et économique sans précédent. Ces évolutions menacent la souveraineté numérique française et européenne.

Notre analyse prospective révèle quatre scénarios possibles à l'horizon 2040. Le plus probable, la « colonie numérique », verrait la France perdre sa souveraineté en restant vassalisée aux acteurs dominants. Le plus défavorable, le « Great Firewall of Everywhere », conduirait à une balkanisation de l'espace numérique et marquerait la fin de la mondialisation numérique.

Stratégie retenue : une approche équilibrée

Notre objectif stratégique s'énonce ainsi : « À l'horizon 2040, préserver notre modèle démocratique en consolidant, avec nos alliés européens, une industrie numérique de confiance performante. »

Notre analyse montre qu'une stratégie de continuité des actions déjà engagées ne suffira pas. La France doit combiner deux approches complémentaires. D'une part, une stratégie de réalignement qui capitalise sur les initiatives existantes, comme France 2030, en les réorientant vers une massification et des objectifs européens. D'autre part, une stratégie de rupture qui propose des transformations radicales pour

répondre à une urgence géopolitique et potentiellement militaire.

Cette stratégie combinée offre la souplesse nécessaire pour s'adapter aux évolutions

géopolitiques et technologiques sans renoncer à nos valeurs. Elle permet de proposer des mesures à différents degrés d'acceptabilité, dont le séquencement peut être ajusté aux modifications de contexte.

Cinq recommandations et leurs plans d'action au service de notre stratégie

R1 Politique : la force de l'Union européenne pour créer une industrie performante sur le segment du numérique de confiance.

Créer une définition commune européenne du « numérique de confiance » intégrant les valeurs démocratiques. Mobiliser les pays pionniers dès 2026 pour poser les bases intellectuelles.

Déployer un cadre normatif et des financements dédiés à partir de 2030. Favoriser le

rayonnement international à partir de 2035.

R2 Financement : des ressources pour le numérique de confiance européen

Créer un fonds de pension collectant 1 % des cotisations retraite européennes, générant 25 milliards d'euros d'investissement par an. Harmoniser la taxation des publicités en ligne à 10 % dans toute l'Union européenne pour financer l'information de qualité.

R3 Formation et gestion des talents : l'éducation numérique pour tous

Atteindre 90 % d'alphabétisation numérique en France à l'horizon 2040 et favoriser la cohésion sociale via un contrat d'engagement citoyen et une réserve nationale du numérique. Déployer 120 000 robots d'assistance pédagogique utilisant l'IA pour personnaliser l'apprentissage au cours de la vie.

R4 Champ informationnel : vers une information de confiance

Créer des plateformes de médias sociaux aux algorithmes publics et audités. Authentifier les utilisateurs et contenus pour lutter contre la désinformation. Responsabiliser les plateformes en les soumettant au même régime que les médias traditionnels.

R5 Ruptures technologiques et environnementales : les conditions du changement

Investir dans des « Projets scientifiques d'intérêt stratégique » qui se concentrent sur quelques grands enjeux, comme le développement des biotechnologies végétales pour la dépollution.

Créer un leadership européen en robotique au service de l'humain et pour la construction d'ouvrages de grandes dimensions.

Bénéfices attendus

Ces recommandations représentent un investissement massif mais indispensable. Le fonds de pension européen mobiliserait l'épargne continentale au service de l'innovation. La taxation harmonisée des publicités rapprocherait les conditions de concurrence entre acteurs européens et américains. L'effort de recherche à 4 % du PIB et les investissements dans le domaine de l'énergie replaceraient l'Europe au niveau des puissances technologiques mondiales. La France et l'Europe (re)deviendraient compétitives sur les technologies de pointe. Elles développeraient des champions européens capables de rivaliser, grâce à des atouts spécifiques, avec les GAFAM (US) et les BATX (Chine). L'industrie du numérique de confiance créerait des emplois qualifiés et exporterait ses solutions partout dans le monde.

L'éducation numérique généralisée transformerait la France en société résiliente face aux menaces cyber. La maîtrise de l'information de confiance protégerait les démocraties contre les manipulations d'opinions. En 2040, l'Europe disposerait d'un écosystème numérique renforcé et performant lui permettant de se protéger de ses adversaires, de se maintenir face à ses compétiteurs, tout en permettant aux citoyens européens d'exprimer leurs cultures et leurs valeurs démocratiques. Ils bénéficieraient de services numériques transparents, sécurisés et respectueux de leurs droits fondamentaux.

Sur le plan géopolitique, l'Europe renforcerait sa position de troisième voie entre les modèles américain et chinois. Elle proposerait une alternative fondée sur la transparence, l'éthique et le respect des droits humains. Cette position lui permettrait d'attirer les talents mondiaux et de nouer des alliances technologiques avec les démocraties partenaires.

Conditions de réussite et arbitrages nécessaires

Le succès de cette stratégie repose sur trois piliers fondamentaux :

- la construction d'un consensus européen autour de la définition du numérique de confiance. Celui-ci nécessite un travail diplomatique intense avec l'Allemagne, l'Italie, Les Pays-Bas et l'Estonie comme pays pionniers.
- la mobilisation de financements à la hauteur des enjeux. Le fonds de pension européen et l'harmonisation fiscale doivent créer les conditions d'un financement endogène de l'innovation européenne. Cette autonomie financière est indispensable pour réduire la dépendance aux capitaux américains et chinois.

l'acceptabilité sociale des transformations proposées. Le fonds de pension européen et les investissements massifs en R&D pourraient se heurter à la réticence des partenaires sociaux. Ils nécessiteront une pédagogie et une transparence constante auprès des citoyens. La confiance numérique ne peut se construire sans l'adhésion de la population.
Cette stratégie nécessite par ailleurs des choix difficiles et des renoncements.

- Sur le plan technologique, la France devra allouer ses moyens en priorité aux secteurs identifiés dans le rapport. L'expertise scientifique sera cruciale pour identifier les champions technologiques de demain.
- Sur le plan social, au-delà des enjeux d'acceptabilité mentionnés supra, l'encadrement des plateformes et le contrat d'engagement citoyen sont porteurs de restrictions des libertés individuelles. Il faudra convaincre les citoyens que ces mesures visent à protéger la démocratie contre les manipulations externes.
- Sur le plan industriel, le « pari européen » implique de créer des relations de confiance entre partenaires. Il faut éviter les concurrences déloyales entre acteurs européens et créer des organismes de financement proportionnés à l'espace continental. Cette coopération renforcée sera déterminante pour le succès de la stratégie.

En résumé, notre stratégie offre un chemin vers une autonomie stratégique européenne vis-à-vis de ses compétiteurs et vers une souveraineté française renforcée. Elle conjugue pragmatisme politique et ambition technologique, en proposant une alternative crédible aux modèles américain et chinois.

La France doit agir maintenant avec ses alliés pour faire de l'Europe un acteur incontournable de l'économie numérique mondiale, garant d'un cadre de vie numérique respectueux des valeurs démocratiques, de la dignité des citoyens et de leurs droits fondamentaux.

SNC - Comité 3

Face aux ruptures stratégiques, Quelle stratégie la France doit-elle mettre en œuvre pour un développement numérique et technologique souverain et soutenable, y compris en matière de défense ?

« Les *Américains étaient nos frères, ils ne sont plus que des lointains cousins* ». Ces propos volontairement provocants de l'économiste et essayiste Alain Minc, lors d'une interview donnée à Ecorama en mai 2025[4] à l'occasion des cent premiers jours de présidence de D. Trump II, sont le reflet d'une préoccupation d'importance, dont la France — voire l'Europe entière — a pris conscience au cours des derniers mois : certaines ruptures stratégiques sont effectivement de nature à remettre en cause des certitudes ancrées très profondément dans notre pensée collective, et à impacter significativement nos organisations, nos vies de tous les jours, notre liberté de pensée, d'expression et d'agir.

Alors que Français et Européens ont largement tiré profit des dividendes de la paix depuis la fin de la Seconde Guerre mondiale, et ont pu ainsi financer des modèles sociaux avantageux tout en bénéficiant d'avancées numériques et technologiques directement issues de la Silicon Valley, plusieurs évènements récents sont venus rebattre les cartes d'un ordre mondial que l'on pensait inamovible. Le réchauffement climatique, le retour de la guerre sur le sol européen, le durcissement de la posture économique et (anti) environnementale américaine ou l'émergence affichée d'un axe sino-russe renforcé sont autant de ruptures stratégiques qui se sont avérées clivantes pour de nombreux États et citoyens, à commencer par ceux de l'Union européenne et de la France en particulier. Si l'actualité politique et économique renforce le besoin d'une analyse de notre positionnement vis-à-vis des États-Unis, l'échiquier du développement numérique et technologique est cependant à multiples dimensions : la Chine, la Russie, Taiwan — pour ne citer qu'eux — jouent un rôle tout aussi important dans la dynamique d'ensemble.

Peut-on en effet se permettre en tant que nation de s'en remettre, sur des questions aussi critiques que le numérique et la technologie, de façon quasi aveugle à des puissances étrangères — fussent-elles des alliées de confiance dans un passé récent — dont on ne maîtrise ni les ambitions, ni les exigences, ni même les positionnements idéologiques ? Le Général de Gaulle avait répondu à cette question en dotant la France de l'arme nucléaire : « S'il faut que la France ait une épée, il faut que ce soit la sienne ».

À l'heure où la technologie a envahi l'espace privé, qu'elle se pose d'une certaine façon en garante de notre confort de vie et de notre efficacité économique, mais qu'elle est également une composante indispensable de notre système de défense, elle devient d'une certaine façon l'arme nucléaire du XXIe siècle. Dès lors, la question de notre souveraineté en la matière devient essentielle, voire vitale. Il s'agit pour nous de trouver une stratégie de développement numérique et technologique souverain et soutenable, y compris en matière de défense, qui nous permette de positionner la France dans une situation de force sur la scène internationale, quelles que soient les évolutions ou ruptures qui se profilent. Clara Chappaz, ministre déléguée au Numérique, l'a d'ailleurs rappelé lors de la conférence de presse

4 https://www.youtube.com/watch?v=o0YW3-Ggvhw

du 14 avril 2025 : « la souveraineté numérique est une cause commune. Elle engage l'État, les entreprises et les citoyens pour construire une Europe numérique plus forte, plus libre et plus souveraine. Il n'y a pas de prospérité économique durable sans souveraineté numérique. »

En effet, les changements auxquels nous avons assisté au cours de ces derniers mois ne sont peut-être que les prémices de ruptures encore plus marquées qu'il nous faut anticiper pour identifier une stratégie française capable d'assurer à notre pays une certaine résilience. Ces ruptures, quelles sont-elles ? De nombreux paramètres peuvent évoluer et amener les États à reconsidérer leur position. Parmi les catalyseurs majeurs de transformations possibles, la capacité de l'Union européenne à perdurer ou se renforcer en tant que réalité institutionnelle, politique, économique et éventuellement militaire, compte certainement parmi les plus importants.

S'agissant de numérique et de technologie, l'application — ou non — d'une législation extraterritoriale sur les données et leur protection est également de nature à modifier significativement des choix et des postures étatiques vis-à-vis d'éditeurs de logiciels, dont l'importance financière et stratégique les place quasiment au rang des États. Deux principaux scénarios peuvent se dégager du croisement de ces variables. Un premier, très favorable mais malheureusement peu plausible, serait celui d'une Union européenne forte qui réussirait à gagner son autonomie stratégique en provoquant l'émergence de champions technologiques tout en bloquant l'application sur son sol de lois extraterritoriales.

À l'opposé, un second scénario verrait l'éclatement d'une Union incapable de se positionner en acteur crédible, induisant de facto un recours massif aux technologies étrangères. Un tel échec pourrait alors se payer au prix fort : celui de l'envoi systématique de toutes les données et informations des utilisateurs aux États étrangers et technologiquement avancés ayant su imposer leurs obligations extraterritoriales.

Pour la France, la réponse à de tels scénarios se doit d'être d'ampleur. Cette assertion résulte d'ailleurs d'une nécessité et non d'un choix. En effet, la complexité du monde numérique et des technologies est telle qu'elle peut se représenter par un système multicouche dans lequel évolue un écosystème d'acteurs de taille considérable et en constante évolution 2

Réussir à construire et maintenir une forme de souveraineté dans un tel environnement nécessite une capacité d'investissements extrêmement importante et une réflexion sur le temps long compte tenu de l'ampleur des travaux à mener. Finalement, l'objectif peut être formulé ainsi : d'ici 2040, il faut positionner la France dans un rapport de force équilibré avec ses partenaires et compétiteurs numériques et technologiques potentiels, et permettre ainsi la prise en compte de ses exigences, notamment en matière de soutenabilité.

Y parvenir peut se faire de différentes manières. Par exemple, durcir immédiatement le rapport de force pour exercer une forme de pression auprès d'acteurs étrangers à l'accès au marché européen aurait le mérite d'afficher clairement nos ambitions, alors que renforcer le lobbying auprès de nos grands fournisseurs étrangers pour s'assurer de la prise en compte de nos exigences de soutenabilité laisserait voir une posture plus conciliante, mais aussi plus incertaine.

Une stratégie hybride peut permettre de répondre à notre objectif tout en minimisant le risque de rupture brutale avec nos partenaires historiques ou potentiels. Cette stratégie, dont la mise en œuvre doit démarrer dès 2025, repose à court terme sur l'identification de leviers permettant de protéger la propriété et la confidentialité de nos données critiques, sans remettre en cause l'exploitation des technologies étrangères et notamment américaines.

La prise en compte de l'ensemble de nos exigences de soutenabilité et l'obtention d'une forme de souveraineté plus aboutie pourra émerger dans un second temps, mais nécessite pour

être crédible un niveau de maturité dont nous ne disposons pas encore sur le volet technologique dans l'Union européenne.

Concrètement, nous formulons cinq recommandations, dont nous pensons que la mise en œuvre est nécessaire pour atteindre notre objectif, et dont toutes — même si elles vont se déployer dans le temps — peuvent être initiées dès la rentrée 2025.

(1) **Engager** l'État, via notamment la mobilisation de l'épargne privée, pour mettre en place un accompagnement fort sur les technologies renforçant l'autonomie stratégique. Il s'agit clairement de permettre l'émergence des champions de demain, notamment sur les technologies de rupture que sont l'IA et les technologies quantiques. Compte tenu des investissements nécessaires, les actions devront être menées à un niveau européen, impliquant pour la France des renoncements pour certains de ses acteurs nationaux, et dont il faut avoir conscience.

(2) **Construire** et relayer un narratif sur l'autonomie stratégique auprès des citoyens pour les rendre acteurs du changement et conscients des renoncements ou efforts auxquels ils auront nécessairement à faire face.

(3) **Systématiser,** a minima pour les structures étatiques ainsi que pour les OIV/OSE[5], la mise en place, sous gouvernance de l'ANSSI, de mécanismes « *zero trust* » sur les données hébergées ou en lien avec des solutions technologiques étrangères (et notamment américaines). En effet, dans le contexte actuel, les législations de protection européennes ne peuvent plus être considérées comme une garantie pérenne quant à la non-exploitation de nos informations par des tiers.

(4) **Lancer** le développement d'un kit d'autonomie stratégique composé de plusieurs briques logicielles souveraines et/ou open source, permettant à l'ensemble des entreprises et organisations de minimiser leur dépendance aux solutions américaines. La réduction de l'empreinte « non souveraine » dans les systèmes d'information de nos organisations est en effet une condition *sine qua non* pour crédibiliser une posture plus offensive et, in fine, garantir une réponse satisfaisante à nos exigences.

(5) **Durcir** les conditions d'accès au marché européen en négociant avec les différents États membres. Cette dernière recommandation peut être perçue comme la plus agressive et appelle donc une mise en œuvre mesurée, tant dans les modalités de son application que dans sa fenêtre temporelle de déploiement. Un affichage précoce de cette intention pourrait donner lieu à un changement de posture brutal de nos partenaires technologiques à titre défensif, sans que nous soyons en situation d'en absorber les conséquences. La taille du marché européen est néanmoins un atout considérable sur lequel il serait dommage de faire l'impasse dans un contexte technologique de plus en plus compétitif.

5 Opérateurs d'importance vitale/opérateurs de services essentiels

SNC - Comité 4

Résilience des sociétés

Face aux ruptures stratégiques, quelle stratégie de cohésion nationale la France doit-elle adopter dans le champ informationnel ?

La multiplication des ruptures stratégiques à laquelle notre pays est confronté met en péril la cohésion nationale — ce socle du vivre-ensemble qui constitue le ciment de notre Nation — en fragilisant ses fondements et en bouleversant l'ordre établi.

Les vulnérabilités induites par ces ruptures sont désormais systématiquement exploitées par nos compétiteurs, au travers d'ingérences étrangères qui s'inscrivent dans le cadre de conflits hybrides, caractérisés par l'absence de confrontation physique directe, mais amplifiés par l'essor rapide des technologies.

Ces ingérences ciblent particulièrement le champ informationnel, devenu un véritable théâtre d'opérations. Par des campagnes de désinformation, les acteurs hostiles cherchent à manipuler les perceptions, attiser les divisions internes et instrumentaliser les failles sociétales. Leur objectif est clair : miner la confiance des citoyens envers leurs institutions et affaiblir la résilience de l'État de l'intérieur.

La question centrale est donc de savoir comment l'État, dans le champ informationnel, est en mesure de renforcer la résilience des citoyens face à ces agressions informationnelles, de quelque nature qu'elles soient.

Analyse prospective

Deux scénarios prospectifs peuvent être envisagés à l'horizon 2040 pour anticiper les évolutions possibles de l'impact des ruptures stratégiques combiné au paysage informationnel mondial.

Le premier envisage l'émergence d'une oligarchie informationnelle, dans laquelle des acteurs économiques privés, dotés d'un pouvoir technologique et financier considérable, prendraient le contrôle des flux d'information à l'échelle mondiale. Ces entités remettraient en cause la souveraineté des États, en devenant elles-mêmes des acteurs géopolitiques de premier plan.

Le second scénario est celui d'un totalitarisme informationnel, porté par des régimes autoritaires imposant leur vision du monde par une censure systémique et globale. Ce modèle entraînerait une paralysie progressive des institutions, affectant particulièrement les démocraties libérales, incapables de faire face à une telle asymétrie informationnelle.

Dans les deux hypothèses, l'enjeu est majeur : sans stratégie de résilience, les démocraties risquent un affaiblissement durable, voire un effondrement structurel.

Stratégies étudiées

Pour y faire face, une stratégie volontariste et anticipatrice s'impose. Elle repose sur plusieurs piliers fondamentaux, comme la régulation, la coopération européenne, l'éducation, la mobilisation collective et la construction d'un socle narratif républicain partagé.

Cette stratégie a pour ambition de restaurer la confiance, de renforcer la cohésion nationale et de faire de chaque citoyen un acteur engagé de la résilience collective. Elle combine des mesures

de court terme avec une approche résolument structurelle et de long terme, afin d'inscrire la résilience dans la durée, non comme une simple réaction aux crises, mais comme un levier durable de stabilité et de souveraineté.

Recommandations opérationnelles

1. Disposer d'une stratégie nationale de lutte contre la désinformation ayant, entre autres finalités, celle de la cohésion nationale.

L'objectif est de mettre en place une stratégie centralisée, proactive et coordonnée, pilotée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN). Ce chantier doit être constitué d'une phase de diagnostic, d'une équipe interministérielle, et d'une rédaction finalisée à fin 2025. L'objectif est d'unifier les efforts étatiques, privés et citoyens en vue d'une action cohérente dans l'espace informationnel.

2. Développer une culture commune de l'information afin de lutter contre les ingérences étrangères et la désinformation.

Cette mesure vise à construire une société capable de critique, correctement informée et formée grâce à l'éducation (modules scolaires, cours en ligne de type Massive Open Online Course [MOOC], brevet de lutte contre la désinformation), la sensibilisation familiale et citoyenne, et des engagements concrets des médias. L'enjeu est de donner à chacun les moyens d'identifier et contrer la désinformation, dès le plus jeune âge.

3. Créer des obligations légales en matière de lutte contre la désinformation ou le renforcement de la cohésion nationale.

L'objectif est de responsabiliser tous les acteurs de l'information par le biais d'obligations contraignantes (fact-checking, certification des influenceurs, identité numérique de confiance, etc.) mais aussi par des incitations économiques (crédit d'impôt, subventions). Le but est de garantir une information fiable, tout en respectant les libertés fondamentales.

4 Créer un organisme européen de coordination de la lutte contre la menace informationnelle.

Pour faire face à une menace exogène, la création d'une agence européenne spécialisée est recommandée. Elle s'inspirera de l'ENISA et soutiendra la montée en compétence des États membres via un partage d'expertise et des projets communs. Cette mesure renforcera la résilience collective au niveau de l'UE et nécessitera un fort consensus politique.

5. Raconter la France positivement autour de valeurs communes

Renforcer la cohésion nationale passe par la valorisation d'un récit historique commun, l'usage renforcé des symboles républicains dans l'espace public, et une communication internationale cohérente promouvant une image positive de la France. Cela suppose aussi une harmonisation des programmes de sciences humaines, l'organisation de rituels civils et un engagement de long terme pour consolider l'unité nationale.

Membres des comités SNC

Comité 1

Bannier Stéphane, col. armée de l'Air et de l'Espace, ministère des armées
Bellefqih Redouane, directeur général de Deloitte Conseil, Deloitte France
Chretien Jennyfer, directrice de cabinet, Agence nationale de la sécurité des systèmes d'information
Claude Sophie, vice-présidente Home Services, Orange
Daoulas Didier, directeur du pôle marine énergie logistique, Bessé
Dulgherian Alexandre, chef d'entreprise, Secure Systems & Services (VINCI Energies)
Feyt Nathalie, vice-présidente Product Security, Schneider Electric
Lanusse Anne, directrice des systèmes d'information Raffinage Chimie, TotalEnergies
le Gall Arnaud, député (Val d'Oise),
Manivet Philippe, chef de service, Assistance publique - Hôpitaux de Paris
Pochon Sébastien, responsable cybersécurité, Enedis
Strebel-Vailler Fabien, colonel de la gendarmerie nationale

Comité 2

Barrande Philippe, directeur des systèmes d'information, Commissariat des armées
Bas Patrick, directeur de recherche, CNRS,
Belloy Augustin, Groupe Galeries Lafayette, Président de Citynove Asset Management
Beurdouche Benjamin, Mozilla, chercheur en cryptographie et méthodes formelles
Buhl Daisy, ministère des Armées,
Clier Jérôme, Tomco, directeur général
Gambier Franck, DGA directeur du segment de management « Cybersécurité du socle numérique des armées »
Lauriau Adeline, Boston Consulting Group, directrice principale et conseillère juridique exécutive
Masson Jean-Baptiste, Institut Pasteur - Inria, directeur de recherche
Meyrieux Emmanuel, OVHcloud, responsable sécurité clients
Tordjman Julien, France Télévisions, directeur délégué Cybersécurité / RSSI
Weyer Florian, HAROPA PORT, Directeur général délégué - Transition numérique

Comité 3

de Castelet Benoît, BNP Paribas PF, Directeur de cabinet de la directrice générale
Fiorentino Alessandro, Infhotep, ADEQUACY
Forterre-Chapard Franceline, ministère de l'Intérieur, sous-directrice des applications numériques
Gauquelin Gustave, secrétaire général Agence des participations de l'État,
Gerbeau Jean-Frédéric, Inria, directeur général délégué à la science
Germain Anne, Bpifrance, Directrice d'investissement sénior
Mercier Jean-Christophe, Alptis Assurances, directeur des systèmes d'information
Petry Hervé, gen. Gendarmerie nationale, Chef de l'unité nationale cyber
Riotton Véronique, Députée de Haute-Savoie
Sommervogel Éric, Crédit Agricole Payment Services, Chief Data Officer
Trubert Matthieu, CGT, secrétaire national de l'UFICT)

comité 4

Alazet Laure, directrice, Sibilardo
Breda Catherine, directrice sécurité des systèmes d'information, Véolia Propreté
Buchet Marion, DGAC directrice du Computer Emergency Response Team Aviation,
de La Taille David, Secrétaire général, Transactis (Groupe Société Générale)
Farges Olivia, Administrateur de l'État
Gibbe Pierre, SNCF Réseau, directeur, Université de l'Ingénierie
Hemery Henri, GRDF, responsable sécurité des systèmes d'information,
Latombe Philippe, Député de Vendée,
Lemonnier Vincent, col. ANFSI, adjoint à la direction des communications tactiques,
Mereuze Cédric, col. EMAT,Chef du bureau Cyberdéfense