

Les nouveaux paradigmes de la Défense : Entre souveraineté technologique et coopérations stratégiques

Posted on July 10, 2026 by Shizneider BAPTISTE

Face à l'émergence de menaces hybrides et au retour des conflits de haute intensité, la notion de défense ne peut plus se limiter à la puissance militaire conventionnelle. Cet article explore la nécessité pour les États de renforcer leur souveraineté technologique, notamment dans les domaines de l'intelligence artificielle et du spatial, tout en consolidant des alliances stratégiques agiles.

Nous analysons comment la modernisation des équipements et l'adaptation des doctrines militaires deviennent les piliers indispensables d'une stabilité durable dans un monde multipolaire en constante mutation.

La transformation contemporaine des équilibres stratégiques mondiaux impose une relecture profonde des fondements de la puissance militaire et de la sécurité nationale, en particulier dans la mesure où la technologie est devenue le vecteur central de la dissuasion, de la projection de force et de la résilience des États. Cette mutation ne saurait être appréhendée par les seuls prismes traditionnels de la géopolitique classique, car elle engage une redéfinition des frontières de la souveraineté, non plus seulement territoriales mais technologiques, industrielles et informationnelles. La défense, autrefois conçue comme un domaine réservé des États dotés de capacités militaires conventionnelles, s'inscrit désormais dans une dynamique où la maîtrise des chaînes de valeur technologiques, la capacité d'innovation duale et la robustesse des écosystèmes industriels constituent des déterminants de premier ordre de l'autonomie stratégique. Dans ce contexte, la souveraineté technologique émerge comme un nouveau paradigme de la puissance, défini par la capacité d'un État ou d'un ensemble d'États à concevoir, produire, déployer et maintenir des systèmes critiques sans dépendance excessive vis-à-vis d'acteurs externes, tout en préservant la liberté de décision politique et opérationnelle. Cependant, cette aspiration à la souveraineté ne peut être poursuivie de manière autarcique, car la complexité des technologies de défense

modernes – de l'intelligence artificielle aux systèmes hypersoniques, en passant par les architectures quantiques et les microélectroniques avancées – excède les capacités de développement isolé de la plupart des nations, y compris des plus puissantes. Il s'ensuit une tension structurelle, à la fois théorique et pratique, entre la nécessité de préserver une souveraineté technologique nationale ou régionale et l'impératif de coopérer au sein de coalitions, d'alliances et de partenariats stratégiques pour partager les coûts, les risques et les expertises. Cet article vise à analyser cette tension fondamentale, en examinant comment les nouveaux paradigmes de la défense se construisent autour de l'articulation entre souveraineté technologique et coopérations stratégiques, et quelles implications cette articulation comporte pour la conception des doctrines militaires, des politiques industrielles de défense et des architectures de sécurité internationale.

La souveraineté technologique comme nouveau fondement de la puissance stratégique

La notion de souveraineté technologique, bien qu'encore en cours de conceptualisation dans la littérature académique et stratégique, s'impose progressivement comme un cadre analytique pertinent pour comprendre les reconfigurations contemporaines de la puissance. Elle ne se réduit pas à une simple question de capacité industrielle ou de balance commerciale dans les secteurs de haute technologie, mais engage une réflexion plus profonde sur les conditions de l'autonomie décisionnelle des États dans un environnement marqué par l'interdépendance technologique, la fragmentation des chaînes de valeur et la militarisation croissante des innovations duales. [1] La souveraineté technologique peut ainsi être définie comme la capacité d'un État ou d'un ensemble d'États à maîtriser les technologies critiques nécessaires à la sauvegarde de ses intérêts vitaux, à la conduite de ses opérations militaires et à la protection de ses infrastructures essentielles, sans subir de contraintes externes susceptibles de compromettre sa liberté d'action politique ou stratégique. [3] Cette définition implique plusieurs dimensions interdépendantes : une dimension industrielle, liée à la capacité de production et à la résilience des chaînes d'approvisionnement ; une dimension cognitive, relative à la maîtrise des savoirs, des brevets et des compétences humaines ; une dimension décisionnelle, concernant la liberté de concevoir, d'acquérir et d'employer des systèmes technologiques sans veto externe ; et une dimension normative, touchant à la capacité de définir les standards, les protocoles et les cadres réglementaires qui régissent l'usage des technologies de

défense.

L'émergence de la souveraineté technologique comme enjeu stratégique majeur s'explique par plusieurs facteurs structurels. Premièrement, la globalisation des chaînes de valeur technologiques, bien qu'ayant permis des gains d'efficacité et d'innovation, a également accru la vulnérabilité des États aux ruptures d'approvisionnement, aux embargos et aux pressions géoéconomiques. [4] La crise des semi-conducteurs de 2020-2023, les tensions autour des matériaux rares et les restrictions à l'exportation de technologies sensibles ont démontré que la dépendance technologique pouvait se transformer en levier de coercition stratégique entre grandes puissances. [12] Deuxièmement, la militarisation accélérée des technologies duales, notamment l'intelligence artificielle, la robotique autonome, les biotechnologies et les systèmes quantiques, a brouillé les frontières entre secteurs civils et militaires, rendant la distinction traditionnelle entre défense et économie de moins en moins opérante. Cette convergence implique que la souveraineté technologique ne peut plus être circonscrite aux seuls domaines de la défense classique, mais doit englober l'ensemble de l'écosystème d'innovation, y compris les start-ups, les laboratoires de recherche et les plateformes numériques. Troisièmement, la numérisation des conflits et la montée en puissance des menaces hybrides, incluant les cyberattaques, la désinformation et les opérations d'influence, ont fait de la maîtrise des infrastructures informationnelles et des données un enjeu de souveraineté aussi crucial que la possession d'armements conventionnels. Dans ce contexte, la souveraineté technologique devient un préalable à toute forme crédible de dissuasion et de défense, car elle conditionne la capacité des États à agir de manière autonome dans des environnements contestés et à résister aux tentatives de déstabilisation par des acteurs étatiques ou non étatiques.

La mise en œuvre de la souveraineté technologique requiert des politiques industrielles et d'innovation ambitieuses, articulées autour de plusieurs axes stratégiques. Elle implique d'abord un effort de réindustrialisation et de relocalisation des capacités de production critiques, notamment dans les secteurs des microélectroniques, des matériaux avancés, des systèmes de propulsion et des composants de défense. Les États-Unis, par exemple, ont lancé plusieurs initiatives dans le cadre de leur National Defense Industrial Strategy, dont le Microelectronics Commons Program et le Secure Enclave, visant à renforcer la résilience de la chaîne d'approvisionnement en microélectronique stratégique et à réduire la dépendance

vis-à-vis des fabricants étrangers. [11] De même, l'Union européenne a inscrit la souveraineté technologique comme un objectif central de sa politique de défense, à travers des instruments tels que le European Defence Fund, le European Defence Industrial Programme et des initiatives sectorielles comme le European Space Shield, destiné à renforcer les capacités spatiales de défense et à promouvoir l'interopérabilité des systèmes nationaux. Ces politiques s'accompagnent de mécanismes de financement public, de partenariats public-privé et de mesures incitatives visant à stimuler l'investissement dans les technologies critiques et à favoriser l'émergence d'écosystèmes industriels intégrés.

Au-delà de la dimension industrielle, la souveraineté technologique exige également un effort de construction et de préservation du capital cognitif, c'est-à-dire des savoirs, des compétences et des capacités d'innovation qui sous-tendent la maîtrise des technologies de défense. Cela passe par le soutien à la recherche fondamentale et appliquée, la formation de talents spécialisés dans les domaines de l'ingénierie, de l'informatique et des sciences appliquées, ainsi que par la protection des bases de connaissances et des brevets contre les transferts non désirés et les appropriations externes. La compétition pour les talents, en particulier dans les secteurs de l'intelligence artificielle, du quantique et de la cybersécurité, est devenue un enjeu géostratégique majeur, les États cherchant à attirer et à retenir les chercheurs, les ingénieurs et les entrepreneurs capables de conduire l'innovation de pointe. Par ailleurs, la souveraineté technologique implique une capacité à définir les standards et les normes qui régissent l'usage des technologies de défense, afin de garantir la compatibilité des systèmes, la sécurité des échanges et la protection des données sensibles. La participation active aux instances de normalisation internationale, la promotion de standards ouverts et interopérables, et la coordination avec les partenaires alliés constituent des leviers importants pour renforcer cette dimension normative de la souveraineté.

Enfin, la souveraineté technologique ne peut être conçue comme une fin en soi, mais doit être mise en relation avec les objectifs stratégiques et les impératifs opérationnels de la défense. La maîtrise des technologies critiques ne prend son sens que si elle contribue à améliorer les capacités militaires, à renforcer la dissuasion et à garantir la liberté d'action des forces armées dans des environnements complexes et contestés. Cela suppose une intégration étroite entre les communautés technologiques, industrielles et militaires, afin d'assurer que les innovations développées répondent aux besoins réels des opérations et puissent

Les nouveaux paradigmes de la Défense : Entre souveraineté technologique et coopérations stratégiques

être déployées de manière efficace et sécurisée. La notion de « souveraineté décisionnelle », développée dans le contexte de l'intelligence artificielle militaire, illustre cette exigence : elle désigne la capacité des commandants militaires à comprendre, contrôler et expliquer les décisions prises par les systèmes autonomes, afin de préserver la responsabilité humaine et la conformité aux normes éthiques et juridiques. [3] La souveraineté technologique, ainsi comprise, ne se réduit pas à une simple accumulation de capacités techniques, mais constitue un élément indissociable de la stratégie globale de défense, articulé avec les doctrines militaires, les architectures de commandement et les priorités d'investissement.



Les limites de l'autarcie technologique et la nécessité des coopérations stratégiques

Malgré l'impératif de souveraineté technologique, aucune nation, pas même les plus puissantes, ne peut prétendre maîtriser de manière isolée l'ensemble des technologies critiques nécessaires à sa défense. La complexité croissante des systèmes d'armement modernes, la rapidité des cycles d'innovation et l'ampleur des investissements requis rendent l'autarcie technologique non seulement coûteuse, mais aussi stratégiquement risquée, car elle expose les États à des retards de développement, à des obsolescences accélérées et à des vulnérabilités non anticipées. [6] Cette réalité impose une réévaluation des approches traditionnelles de la souveraineté, en reconnaissant que celle-ci ne peut être poursuivie que dans le cadre de coopérations stratégiques bien conçues, permettant de partager les coûts, les risques et les expertises, tout en préservant les marges d'autonomie décisionnelle nationales. Les coopérations stratégiques,

Les nouveaux paradigmes de la Défense : Entre souveraineté technologique et coopérations stratégiques

qu'elles prennent la forme d'alliances formelles, de partenariats technologiques ou de coalitions ad hoc, deviennent ainsi un complément indispensable, et non une alternative, à la souveraineté technologique.

L'exemple des programmes hypersoniques illustre de manière particulièrement éloquente cette dynamique. Les technologies hypersoniques, qui permettent le développement de vecteurs capables de se déplacer à des vitesses supérieures à Mach 5 et de manœuvrer de manière imprévisible, constituent un enjeu stratégique majeur pour la dissuasion et la projection de force. [7] Cependant, leur développement requiert des investissements massifs, des infrastructures de test spécialisées et des expertises pointues dans des domaines tels que les matériaux à haute température, les systèmes de propulsion avancés et les algorithmes de guidage et de contrôle. Face à ces défis, les États-Unis, le Royaume-Uni et l'Australie ont signé en novembre 2024, dans le cadre du pilier II de l'accord AUKUS, un accord de coopération sur les essais hypersoniques, baptisé HyFliTE (Hypersonic Flight Test and Experimentation), visant à mettre en commun leurs installations d'essai, à partager les informations techniques et à coordonner les campagnes de vols d'essai, avec un financement total de 252 millions de dollars américains et jusqu'à six campagnes trilatérales prévues d'ici 2028. [7] Cette coopération permet non seulement d'accélérer le développement des technologies hypersoniques, mais aussi de réduire les coûts individuels pour chaque pays, tout en renforçant l'interopérabilité des systèmes et la cohérence des doctrines d'emploi. Elle illustre également comment la souveraineté technologique peut être préservée au sein d'un cadre coopératif, puisque chaque partenaire conserve la maîtrise de ses propres programmes nationaux, tout en bénéficiant des avantages de la mutualisation des ressources et des expertises.

De manière similaire, les initiatives de coopération dans le domaine des technologies quantiques témoignent de la reconnaissance croissante, par les États, de la nécessité de coordonner leurs efforts pour maîtriser des technologies aux implications stratégiques profondes, notamment en matière de cryptographie, de détection et de calcul haute performance. Le Royaume-Uni a pris en mai 2025 la présidence de la Communauté quantique transatlantique de l'OTAN, un forum rassemblant des experts en quantique issus de 22 pays alliés, afin de faciliter la collaboration entre les secteurs quantiques et de la défense, d'identifier les applications prioritaires et de promouvoir l'interopérabilité des systèmes. [8] Parallèlement, le G7 a adopté en juin 2025, lors de son sommet à Kananaskis au

Les nouveaux paradigmes de la Défense : Entre souveraineté technologique et coopérations stratégiques

Canada, une déclaration conjointe engageant ses membres à coordonner leurs efforts en matière de technologies quantiques, à travers la création d'un groupe de travail conjoint sur les technologies quantiques, chargé de guider la coopération en matière de recherche, de commercialisation, de normalisation et de gestion des risques. Cette initiative vise à renforcer les investissements publics et privés, à développer une main-d'œuvre qualifiée, à promouvoir l'inclusion et à protéger les technologies sensibles contre les transferts non désirés, tout en encourageant la collaboration scientifique ouverte entre les pays partageant les mêmes valeurs. [15] Ces démarches montrent que la souveraineté technologique dans le domaine quantique ne peut être atteinte que par une combinaison de renforcement des capacités nationales et de coopération internationale structurée, permettant de bénéficier des synergies entre les écosystèmes d'innovation tout en préservant les intérêts stratégiques de chaque acteur.

Les coopérations stratégiques ne se limitent pas aux domaines technologiques de pointe, mais s'étendent également à la sécurisation des chaînes d'approvisionnement et à la résilience des bases industrielles de défense. L'OTAN, par exemple, a renforcé sa coopération avec ses partenaires de l'Indo-Pacifique, reconnaissant l'interconnexion entre la sécurité euro-atlantique et la stabilité Indo-Pacifique, et s'engageant à approfondir le dialogue et la coopération en matière de sécurité des chaînes d'approvisionnement, de développement, de production et de processus d'approvisionnement. [8] Cette coopération inclut l'exploration de projets communs dans les domaines spatial et maritime, ainsi que dans le secteur des munitions, et la poursuite de la collaboration sur les technologies émergentes et disruptives, en s'appuyant sur les acteurs de l'innovation, y compris les start-ups duales. [8] De même, les États-Unis et l'Inde ont renforcé leur partenariat technologique stratégique, à travers des initiatives telles que l'Initiative sur les technologies critiques et émergentes (iCET), visant à mobiliser les investissements du secteur privé et les partenariats dans les secteurs technologiques stratégiques, y compris la défense. Ces coopérations témoignent d'une prise de conscience croissante que la sécurité des chaînes d'approvisionnement et la résilience industrielle sont des enjeux collectifs, nécessitant une coordination entre alliés et partenaires pour faire face aux risques de rupture, de dépendance excessive et de coercition économique.

Cependant, les coopérations stratégiques ne sont pas sans risques et ne sauraient être envisagées comme une solution universelle aux défis de la souveraineté

technologique. Elles comportent des défis majeurs, notamment en matière de protection des secrets industriels et technologiques, de répartition équitable des coûts et des bénéfices, et de préservation de l'autonomie décisionnelle des partenaires. [10] La dépendance vis-à-vis des partenaires, même alliés, peut créer de nouvelles vulnérabilités, en particulier si les priorités stratégiques divergent ou si les engagements politiques fluctuent. De plus, la complexité des cadres juridiques et réglementaires, les différences en matière de standards et de protocoles, et les contraintes liées aux contrôles à l'exportation peuvent entraver la fluidité des coopérations technologiques. Il est donc essentiel que les coopérations stratégiques soient conçues de manière à équilibrer mutualisation et autonomie, en établissant des mécanismes clairs de gouvernance, de protection des informations sensibles et de répartition des responsabilités. La souveraineté technologique, dans ce contexte, ne doit pas être entendue comme une exclusion systématique des coopérations, mais comme la capacité de négocier et de structurer ces coopérations de manière à préserver les marges de manœuvre nationales et à garantir que les bénéfices stratégiques soient partagés de manière équitable.



Les domaines technologiques critiques et leurs implications pour la souveraineté et la coopération

La tension entre souveraineté technologique et coopération stratégique se manifeste avec une acuité particulière dans les domaines technologiques critiques qui façonnent l'avenir des capacités de défense. Parmi ces domaines, l'intelligence artificielle, les systèmes autonomes, les technologies quantiques, les armements hypersoniques, les microélectroniques avancées et les infrastructures cybernétiques occupent une place centrale, car ils déterminent non seulement les performances des systèmes militaires, mais aussi la résilience des États face aux menaces hybrides et aux disruptions technologiques. L'analyse de ces domaines permet d'identifier les arbitrages spécifiques entre souveraineté et coopération, ainsi que les dynamiques émergentes qui structurent les nouvelles configurations de la puissance stratégique.

L'intelligence artificielle (IA) militaire constitue l'un des domaines les plus transformateurs et les plus controversés des technologies de défense contemporaines. Les applications de l'IA dans le domaine militaire sont multiples, allant de l'analyse de données et de la reconnaissance de patterns à la prise de décision assistée, en passant par le contrôle des systèmes autonomes et la cyberdéfense. [14] L'IA offre des avantages significatifs en termes de rapidité de traitement, de précision et d'adaptabilité, permettant aux forces armées de mieux anticiper les menaces, d'optimiser les opérations et de réduire les pertes humaines. Cependant, son déploiement soulève également des défis majeurs en matière de souveraineté, car la maîtrise des algorithmes, des données et des infrastructures de calcul est concentrée entre les mains d'un nombre restreint d'acteurs, principalement des entreprises technologiques et des centres de recherche situés dans un petit nombre de pays. La dépendance vis-à-vis des plateformes d'IA développées par des acteurs externes, en particulier dans les domaines de l'apprentissage automatique et des modèles de langage, peut compromettre la souveraineté décisionnelle des États, en limitant leur capacité à comprendre, contrôler et expliquer les décisions prises par les systèmes autonomes. Par ailleurs, les risques liés à la sécurité des données, à la manipulation des algorithmes et à l'exploitation des vulnérabilités des systèmes d'IA renforcent la nécessité de développer des capacités nationales ou régionales en matière d'IA de défense, tout en préservant la possibilité de coopérer avec des partenaires partageant les mêmes normes éthiques et de sécurité.

Les systèmes autonomes, qu'ils soient terrestres, aériens, maritimes ou sous-marins, représentent un autre domaine critique où les enjeux de souveraineté et de coopération s'entremêlent de manière complexe. Les drones, les robots de combat et les véhicules autonomes offrent des capacités opérationnelles inédites, notamment en termes de persistance, de précision et de réduction des risques pour les personnels militaires. Cependant, leur développement et leur emploi requièrent des expertises avancées en matière de capteurs, de navigation, de communication et de prise de décision autonome, qui ne sont pas également réparties entre les États. La dépendance vis-à-vis des fournisseurs étrangers de composants critiques, tels que les capteurs, les moteurs et les logiciels de contrôle, peut limiter la souveraineté opérationnelle des États, en particulier en cas de tensions géopolitiques ou de restrictions à l'exportation. En même temps, la complexité des systèmes autonomes et la rapidité des cycles d'innovation rendent difficile pour la plupart des pays de développer de manière isolée des capacités complètes et compétitives. [6] Les coopérations technologiques, telles que les programmes

conjointes de développement de drones, les initiatives de standardisation des protocoles de communication et les exercices interopérables, deviennent ainsi des leviers essentiels pour renforcer les capacités tout en préservant les marges d'autonomie nationale.

Les technologies quantiques, bien qu'encore largement au stade de la recherche et du développement, promettent de transformer profondément les capacités de défense, notamment en matière de cryptographie, de détection et de calcul. [15] Les ordinateurs quantiques, une fois matures, pourraient rendre obsolètes les systèmes de chiffrement actuels, compromettant la sécurité des communications militaires et des infrastructures critiques. Les capteurs quantiques, quant à eux, offrent des capacités de détection et de navigation d'une précision inégalée, susceptibles de révolutionner la surveillance, la reconnaissance et la guidance des armes. [15] Cependant, la maîtrise des technologies quantiques requiert des investissements massifs, des infrastructures spécialisées et des compétences rares, concentrées dans un nombre limité de pays et d'entreprises. La souveraineté technologique dans ce domaine implique non seulement de développer des capacités nationales de recherche et de développement, mais aussi de protéger les savoirs et les brevets contre les transferts non désirés, tout en participant activement aux initiatives de coopération internationale, telles que la Communauté quantique transatlantique de l'OTAN et le groupe de travail conjoint du G7 sur les technologies quantiques. Ces coopérations permettent de partager les coûts et les risques, de promouvoir l'interopérabilité des systèmes et de définir des standards communs, tout en préservant les intérêts stratégiques de chaque acteur.

Les armements hypersoniques, déjà mentionnés, constituent un autre domaine où les enjeux de souveraineté et de coopération s'articulent de manière complexe. La capacité de développer et de déployer des systèmes hypersoniques est perçue comme un multiplicateur de force stratégique, en raison de leur vitesse, de leur manœuvrabilité et de leur capacité à contourner les défenses antimissiles existantes. [7] Cependant, le développement de ces systèmes requiert des technologies avancées dans plusieurs domaines, notamment les matériaux résistants à la chaleur, les systèmes de propulsion et les algorithmes de guidage, qui ne sont pas accessibles à tous les pays. Les coopérations, telles que l'accord HyFLiTE dans le cadre d'AUKUS, permettent de mutualiser les ressources et les expertises, d'accélérer les cycles de développement et de renforcer l'interopérabilité des systèmes, tout en préservant la souveraineté nationale sur les

programmes d'armement. Cependant, ces coopérations doivent être conçues de manière à éviter les dépendances excessives et à garantir que les bénéfices stratégiques soient partagés de manière équitable entre les partenaires.

Les microélectroniques avancées, en particulier les semi-conducteurs et les composants de défense, constituent un domaine critique où la souveraineté technologique est directement liée à la sécurité nationale. [11] La dépendance vis-à-vis des fabricants étrangers, en particulier dans les régions géopolitiquement instables, expose les États à des risques de rupture d'approvisionnement, de sabotage et de coercition économique. [13] Les initiatives telles que le Microelectronics Commons Program et le Secure Enclave aux États-Unis, ainsi que les efforts de l'Union européenne pour renforcer la production européenne de semi-conducteurs, visent à réduire ces dépendances et à assurer la résilience des chaînes d'approvisionnement. [12] Cependant, la complexité des processus de fabrication, les coûts élevés et la concentration des compétences dans un petit nombre d'entreprises rendent difficile pour la plupart des pays de développer des capacités complètes de production de microélectroniques. Les coopérations technologiques, telles que les partenariats entre les États-Unis, l'Union européenne, le Japon et la Corée du Sud, deviennent ainsi essentielles pour partager les coûts, les risques et les expertises, tout en préservant les marges d'autonomie nationale. [8]

Enfin, les infrastructures cybernétiques et les capacités de cyberdéfense constituent un domaine où la souveraineté technologique et la coopération stratégique sont indissociables. La numérisation des conflits et la montée en puissance des menaces hybrides ont fait de la cybersécurité un enjeu de défense majeur, nécessitant des capacités avancées pour protéger les infrastructures critiques, détecter les intrusions et contrer les attaques. [10][16] La souveraineté technologique dans ce domaine implique de maîtriser les infrastructures réseaux, les logiciels de sécurité et les protocoles de communication, ainsi que de développer des capacités nationales de cyberdéfense et de cyberrenseignement. Cependant, la nature transfrontalière des menaces cybernétiques et la complexité des architectures réseaux rendent nécessaire la coopération entre les États, les alliances et les secteurs privés pour partager les informations sur les menaces, coordonner les réponses et développer des standards communs. Les initiatives telles que la coopération OTAN-Indo-Pacifique, les partenariats technologiques entre les États-Unis et l'Inde, et les efforts du G7 en matière de technologies quantiques sécurisées

Les nouveaux paradigmes de la Défense : Entre souveraineté technologique et coopérations stratégiques

illustrent cette dynamique de coopération, qui doit être équilibrée avec les impératifs de souveraineté nationale en matière de sécurité des données et des infrastructures. [8]



Les implications doctrinales et organisationnelles de la tension souveraineté-coopération

La tension entre souveraineté technologique et coopération stratégique ne se limite pas aux domaines technologiques et industriels, mais engage une transformation profonde des doctrines militaires, des architectures de commandement et des organisations de défense. Les États sont contraints de repenser leurs approches traditionnelles de la défense, en intégrant les nouvelles réalités de la dépendance technologique, de la complexité des coopérations internationales et de la nécessité de préserver l'autonomie décisionnelle. [9] Cette transformation implique des changements doctrinaux, organisationnels et culturels, qui ne peuvent être accomplis sans une réflexion stratégique approfondie et une coordination entre les différentes composantes de l'appareil de défense.

Sur le plan doctrinal, la tension entre souveraineté et coopération impose une réévaluation des principes de dissuasion, de projection de force et de résilience. La dissuasion, traditionnellement fondée sur la possession d'armements nucléaires et conventionnels crédibles, doit désormais intégrer la dimension technologique comme un élément central de la crédibilité stratégique. La capacité de développer, de déployer et de maintenir des systèmes technologiques avancés, sans dépendance excessive vis-à-vis des acteurs externes, devient un facteur de dissuasion aussi important que la possession d'armements traditionnels. [3] Cependant, la complexité des technologies modernes et la nécessité de coopérer avec des alliés et des partenaires imposent une réflexion sur les conditions dans lesquelles la coopération renforce ou affaiblit la crédibilité de la dissuasion. Une coopération bien conçue, qui mutualise les coûts et les risques tout en préservant l'autonomie décisionnelle, peut renforcer la dissuasion en augmentant les capacités collectives et en signalant la cohérence stratégique entre les partenaires. En revanche, une coopération mal conçue, qui crée des dépendances excessives ou compromet la souveraineté décisionnelle, peut affaiblir la dissuasion en limitant la liberté d'action des États et en introduisant des vulnérabilités non anticipées. La doctrine militaire doit ainsi intégrer une réflexion sur les conditions optimales de la coopération technologique, en définissant des critères clairs pour évaluer les bénéfices et les risques des partenariats, ainsi que des mécanismes pour préserver l'autonomie décisionnelle.

La projection de force, autre pilier des doctrines militaires traditionnelles, doit également être repensée à la lumière des nouvelles réalités technologiques. La capacité de projeter des forces à distance, de manière rapide et décisive, dépend désormais de la maîtrise des technologies de communication, de navigation, de renseignement et de logistique, qui sont fortement intégrées dans des réseaux globaux et interdépendants. La souveraineté technologique implique de maîtriser ces réseaux et de garantir leur résilience face aux perturbations, aux cyberattaques et aux tentatives de déstabilisation. [10] Cependant, la complexité des architectures réseaux et la nécessité de coopérer avec des alliés pour des opérations combinées imposent une réflexion sur les conditions dans lesquelles la coopération renforce ou affaiblit la capacité de projection de force. Une coopération bien conçue, qui assure l'interopérabilité des systèmes, la sécurité des échanges et la cohérence des procédures, peut renforcer la projection de force en permettant des opérations combinées efficaces et en augmentant les capacités collectives. En revanche, une coopération mal conçue, qui introduit des incompatibilités techniques, des vulnérabilités de sécurité ou des dépendances excessives, peut

affaiblir la projection de force en limitant la flexibilité opérationnelle et en créant des points de défaillance critiques. La doctrine militaire doit ainsi intégrer une réflexion sur les conditions optimales de la coopération technologique, en définissant des critères clairs pour évaluer l'interopérabilité, la sécurité et la résilience des systèmes, ainsi que des mécanismes pour préserver la flexibilité opérationnelle.

La résilience, enfin, devient un principe doctrinal central, en raison de la complexité des environnements opérationnels contemporains et de la multiplication des menaces hybrides. La résilience implique la capacité de résister aux perturbations, de s'adapter aux changements et de récupérer rapidement après des chocs, qu'ils soient technologiques, opérationnels ou informationnels. La souveraineté technologique contribue à la résilience en assurant la maîtrise des technologies critiques et la protection des infrastructures essentielles. Cependant, la complexité des chaînes de valeur technologiques et la nécessité de coopérer avec des alliés et des partenaires imposent une réflexion sur les conditions dans lesquelles la coopération renforce ou affaiblit la résilience. Une coopération bien conçue, qui diversifie les sources d'approvisionnement, partage les informations sur les menaces et coordonne les réponses, peut renforcer la résilience en augmentant les capacités collectives et en réduisant les vulnérabilités. En revanche, une coopération mal conçue, qui crée des dépendances excessives, des points de défaillance uniques ou des incompatibilités techniques, peut affaiblir la résilience en limitant la capacité de récupération et en introduisant des risques systémiques. La doctrine militaire doit ainsi intégrer une réflexion sur les conditions optimales de la coopération technologique, en définissant des critères clairs pour évaluer la diversification, la redondance et la sécurité des systèmes, ainsi que des mécanismes pour préserver la capacité de récupération.

Sur le plan organisationnel, la tension entre souveraineté et coopération impose une transformation des structures de commandement, des processus de décision et des cultures de défense. Les organisations de défense traditionnelles, souvent hiérarchisées et centralisées, doivent évoluer vers des structures plus flexibles, plus décentralisées et plus interconnectées, capables de s'adapter rapidement aux changements technologiques et opérationnels. [6] La souveraineté technologique implique de développer des capacités internes de recherche, de développement et d'innovation, ainsi que des compétences en matière de gestion des technologies et des données. Cependant, la complexité des coopérations internationales et la

nécessité de coordonner avec des alliés et des partenaires imposent une réflexion sur les conditions dans lesquelles les structures organisationnelles doivent être adaptées pour faciliter la coopération sans compromettre la souveraineté. Des structures organisationnelles bien conçues, qui intègrent des mécanismes de coordination, de partage d'informations et de gouvernance, peuvent faciliter la coopération en assurant la cohérence des décisions, la sécurité des échanges et la responsabilité des acteurs. En revanche, des structures mal conçues, qui introduisent des lourdeurs bureaucratiques, des incompatibilités culturelles ou des vulnérabilités de sécurité, peuvent entraver la coopération en limitant la flexibilité et en créant des tensions entre les partenaires. Les organisations de défense doivent ainsi intégrer une réflexion sur les conditions optimales de la coopération technologique, en définissant des critères clairs pour évaluer la flexibilité, la sécurité et la cohérence des structures, ainsi que des mécanismes pour préserver l'autonomie décisionnelle.

La culture de défense, enfin, doit évoluer pour intégrer les nouvelles réalités de la coopération technologique et de la souveraineté décisionnelle. Les cultures de défense traditionnelles, souvent marquées par le secret, la méfiance et la centralisation, doivent évoluer vers des cultures plus ouvertes, plus collaboratives et plus décentralisées, capables de faciliter la coopération sans compromettre la sécurité. La souveraineté technologique implique de développer une culture de l'innovation, de la prise de risque et de l'apprentissage, afin de stimuler la créativité et l'adaptabilité. Cependant, la complexité des coopérations internationales et la nécessité de protéger les secrets technologiques imposent une réflexion sur les conditions dans lesquelles la culture de défense doit être adaptée pour faciliter la coopération sans compromettre la sécurité. Des cultures de défense bien conçues, qui intègrent des mécanismes de confiance, de transparence et de responsabilité, peuvent faciliter la coopération en assurant la cohérence des décisions, la sécurité des échanges et la responsabilité des acteurs. En revanche, des cultures mal conçues, qui introduisent des méfiances excessives, des rigidités bureaucratiques ou des vulnérabilités de sécurité, peuvent entraver la coopération en limitant la flexibilité et en créant des tensions entre les partenaires. Les organisations de défense doivent ainsi intégrer une réflexion sur les conditions optimales de la coopération technologique, en définissant des critères clairs pour évaluer la confiance, la transparence et la responsabilité des cultures, ainsi que des mécanismes pour préserver la sécurité.

Vers un équilibre stratégique : scénarios et trajectoires pour la défense du futur

La tension entre souveraineté technologique et coopération stratégique ne peut être résolue par une formule unique, mais doit être appréhendée comme un équilibre dynamique, évoluant en fonction des contextes géopolitiques, des avancées technologiques et des priorités stratégiques des États. Plusieurs scénarios et trajectoires peuvent être envisagés pour l'avenir de la défense, chacun comportant des implications différentes pour la souveraineté, la coopération et la stabilité stratégique. L'analyse de ces scénarios permet d'identifier les options stratégiques, les risques et les opportunités, ainsi que les conditions nécessaires pour parvenir à un équilibre viable entre souveraineté technologique et coopération stratégique.

Un premier scénario, que l'on pourrait qualifier de « souveraineté renforcée », implique un effort accru des États pour développer des capacités technologiques nationales ou régionales, en réduisant les dépendances vis-à-vis des acteurs externes et en renforçant les bases industrielles de défense. Ce scénario pourrait être favorisé par une détérioration des relations géopolitiques, une fragmentation accrue des chaînes de valeur technologiques et une montée des tensions entre grandes puissances, conduisant les États à privilégier l'autonomie stratégique au détriment de la coopération internationale. Dans ce scénario, les États investiraient massivement dans la recherche et le développement, la production nationale et la protection des savoirs, afin de maîtriser les technologies critiques et de garantir leur liberté d'action. Cependant, ce scénario comporte des risques importants, notamment en termes de coûts, de retard technologique et de fragmentation des écosystèmes d'innovation, qui pourraient affaiblir la compétitivité globale des États et réduire leur capacité à faire face aux défis technologiques complexes. [5] De plus, la réduction des coopérations pourrait affaiblir la stabilité stratégique, en augmentant les risques de malentendus, de courses aux armements et de confrontations.

Un deuxième scénario, que l'on pourrait qualifier de « coopération approfondie », implique un renforcement des coalitions, des alliances et des partenariats technologiques, en mutualisant les coûts, les risques et les expertises, tout en préservant les marges d'autonomie nationales. Ce scénario pourrait être favorisé par une stabilisation relative des relations géopolitiques, une reconnaissance accrue des interdépendances technologiques et une volonté des États de faire face

collectivement aux défis technologiques complexes. Dans ce scénario, les États renforceraient les coopérations existantes, telles que l'OTAN, AUKUS et les initiatives du G7, et en développerait de nouvelles, notamment dans les domaines de l'intelligence artificielle, du quantique et des technologies spatiales. [7] Les coopérations permettraient de partager les coûts et les risques, d'accélérer les cycles d'innovation, de renforcer l'interopérabilité des systèmes et de définir des standards communs, tout en préservant les intérêts stratégiques de chaque acteur. Cependant, ce scénario comporte également des risques, notamment en termes de dépendance excessive, de vulnérabilités partagées et de pertes de souveraineté décisionnelle, qui pourraient compromettre la liberté d'action des États et introduire des risques systémiques. De plus, la complexité des coopérations et les divergences de priorités stratégiques pourraient entraver la cohérence des décisions et la sécurité des échanges.

Un troisième scénario, que l'on pourrait qualifier de « souveraineté coopérative », implique une articulation plus fine entre souveraineté technologique et coopération stratégique, en reconnaissant que les deux ne sont pas mutuellement exclusives, mais complémentaires. Ce scénario pourrait être favorisé par une reconnaissance accrue des limites de l'autarcie technologique et des risques de la dépendance excessive, ainsi que par une volonté des États de développer des approches hybrides, combinant renforcement des capacités nationales et coopérations ciblées. Dans ce scénario, les États investiraient dans les technologies critiques où la souveraineté est essentielle, tout en coopérant dans les domaines où la mutualisation des ressources et des expertises est bénéfique. Les coopérations seraient conçues de manière à préserver les marges d'autonomie nationale, en établissant des mécanismes clairs de gouvernance, de protection des informations sensibles et de répartition des responsabilités. Ce scénario permettrait de bénéficier des avantages de la souveraineté et de la coopération, tout en limitant les risques de dépendance excessive et de fragmentation. Cependant, ce scénario requiert une coordination stratégique fine, une confiance accrue entre les partenaires et des mécanismes robustes pour gérer les tensions et les risques. [8]

La trajectoire la plus probable, compte tenu des tendances actuelles, semble être une combinaison des scénarios de « souveraineté renforcée » et de « coopération approfondie », avec une articulation progressive vers une « souveraineté coopérative ». Les États, confrontés à des environnements géopolitiques incertains et à des défis technologiques complexes, sont susceptibles de renforcer leurs

capacités nationales et régionales, tout en approfondissant les coopérations avec les alliés et les partenaires partageant les mêmes intérêts et valeurs. Cette trajectoire implique des investissements massifs dans la recherche et le développement, la production nationale et la protection des savoirs, ainsi qu'un renforcement des coalitions, des alliances et des partenariats technologiques. [12] Elle requiert également une coordination stratégique fine, une confiance accrue entre les partenaires et des mécanismes robustes pour gérer les tensions et les risques. La réussite de cette trajectoire dépendra de la capacité des États à articuler souveraineté et coopération de manière équilibrée, en préservant les marges d'autonomie nationale tout en bénéficiant des avantages de la mutualisation des ressources et des expertises.

Conclusion stratégique : repenser la défense à l'ère de la technologie contestée

La défense, à l'aube de la troisième décennie du XXI^e siècle, ne peut plus être pensée en termes de territoires, de troupes et d'armements seuls, mais doit intégrer comme dimension centrale la maîtrise des technologies critiques et la capacité de coopérer de manière stratégique. La souveraineté technologique, entendue comme la capacité de maîtriser les chaînes de valeur, les savoirs et les infrastructures nécessaires à la sécurité et à la liberté d'action, est devenue un préalable à toute forme crédible de dissuasion et de projection de force. Cependant, cette souveraineté ne peut être poursuivie de manière autarcique, car la complexité des technologies modernes et l'ampleur des investissements requis imposent une coopération structurée avec des alliés et des partenaires. La tension entre souveraineté et coopération n'est pas une contradiction à résoudre, mais un équilibre dynamique à gérer, en articulant renforcement des capacités nationales et mutualisation des ressources et des expertises. Les États qui réussiront à trouver cet équilibre, en développant des approches hybrides combinant souveraineté renforcée et coopération approfondie, seront les mieux positionnés pour faire face aux défis technologiques et stratégiques du futur. À l'inverse, ceux qui privilégieront l'un au détriment de l'autre s'exposeront à des risques de dépendance excessive, de retard technologique et de fragmentation stratégique. La défense du futur, ainsi, ne sera pas seulement une question de capacités militaires, mais de stratégies technologiques, de coopérations intelligentes et de souverainetés bien comprises.

Bibliographie

Les nouveaux paradigmes de la Défense : Entre souveraineté technologique et coopérations stratégiques

1. European Commission. (2024). Technological sovereignty of the EU. European Commission.
https://ec.europa.eu/assets/rtd/srip/2024/ec_rtd_srip-report-2024-chap-08.pdf
- European Parliament. (2025). Defence and artificial intelligence. European Parliament.
[https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI\(2025\)769580_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf)
- European Parliament. (2025). European Space Shield – action plan. European Parliament.
<https://www.europarl.europa.eu/legislative-train/carriage/european-space-shield-%E2%80%93-action-plan/report?sid=9701>
- G7. (2025). G7 Commits to Global Coordination on Quantum Technology As Strategic Stakes Rise. Quantum Policy Briefing.
<https://thequantuminsider.com/2025/06/18/g7-commits-to-global-coordination-on-quantum-technology-as-strategic-stakes-rise/>
- NATO. (2025). NATO Science & Technology Strategy. NATO.
<https://www.nato.int/content/dam/nato/webready/documents/sto/STO-strategy-2025.pdf>
- NATO. (2025). Statement between NATO Secretary General and the four Indo-Pacific partners. NATO.
<https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/statement-between-nato-secretary-general>
- NATO. (2025). The United Kingdom takes the lead of NATO's Transatlantic Quantum Community. NATO.
<https://www.nato.int/en/news-and-events/articles/news/2025/05/13/the-united-kingdom-takes-the-lead-of-natos-transatlantic-quantu>
- U.S. Department of Defense. (2024). AUKUS Partners Sign Landmark Hypersonics Agreement. U.S. Department of Defense.
<https://www.war.gov/News/Releases/Release/Article/3966986/aukus-partners-sign-landmark-hypersonics-agreement/>
- U.S. Department of Defense. (2024). Department of Defense Awards \$25.8 Million to Sustain the U.S. Domestic Strategic Radiation-Hardened Microelectronics Supply Chain. U.S. Department of Defense.

Les nouveaux paradigmes de la Défense : Entre souveraineté technologique et coopérations stratégiques

<https://www.war.gov/News/Releases/Release/Article/3897343/departement-of-defense-awards-258-million-to-sustain-the-us-domestic-st>

1. U.S. Government Accountability Office. (2025). DEFENSE INDUSTRIAL BASE: Actions Needed to Strengthen Supply Chain Resilience. GAO.
<https://www.gao.gov/assets/gao-25-107283.pdf>
1. Big Innovation Centre. (2025). AI in Military and Defence (20 October 2025). Big Innovation Centre.
https://biginnovationcentre.com/wp-content/uploads/2026/01/AI-in-Military-and-Defence-8-Sep-2025_compressed.pdf
1. IE Center for the Governance of Change. (2025). DEFENSE IN THE AGE OF DEEP TECH. IE Center for the Governance of Change.
https://static.ie.edu/CGC/CGC_DefenseInAgeDeepTech.pdf
1. Korean Economy Institute. (2024). KOREA POLICY. Korean Economy Institute.
https://keia.org/wp-content/uploads/2024/12/KEI_KoreaPolicy_2024_V2-I2_Digital_FINAL_edited_2.pdf
1. Springer. (2026). Technology, Crisis, and Sovereignty: New Frontiers for a Strategic Defense. Springer.
https://link.springer.com/chapter/10.1007/978-3-032-20729-6_3
1. ResearchGate. (2023). Technology sovereignty as an emerging frame for innovation policy. ResearchGate.
<https://www.sciencedirect.com/science/article/pii/S0048733323000495>
1. PMC. (2026). Managing technological sovereignty: a systematic review of supply chain resilience strategies in the semiconductor industry. PMC.
<https://pmc.ncbi.nlm.nih.gov/articles/PMC13002567/>

About The Author

Les nouveaux paradigmes de la Défense : Entre souveraineté technologique et coopérations stratégiques



[Shizneider BAPTISTE](#)

Expert et Consultant en Diplomatie et Relations internationales |
Analyste en Stratégie internationale (Sécurité et Défense) |
Analyste en Renseignement, Stratégies et Guerre d'influence

[See author's posts](#)