Contribution du Julien THOUROT, Ingénieur en chef de l'armement

« *Une excellence académique, scientifique et technologique au service de la souveraineté française et européenne : enjeux et mise en œuvre de la Revue nationale stratégique.* »

« Sciences, technologies et diplomatie dans le désordre mondial »

Résumé :

Dans un contexte géostratégique international extrêmement tendu, les domaines scientifiques et techniques sont au cœur de la défense de nos intérêts. C'est dans ce contexte qu'a été publiée la Revue Nationale Stratégique (RNS) actualisée à l'été 2025, intégrant un scénario central au double enjeu : un conflit de haute intensité aux portes de l'Europe, concomitamment à des attaques hybrides survenant sur le territoire national.

Pour répondre à ce scénario, onze objectifs stratégiques ont été définis, parmi lesquels le onzième, construit autour de l'excellence scientifique et technologique. Cet objectif permet d'obtenir des clés de lecture et des éléments de réponse face aux menaces qui nous entourent, permettant de concilier développements scientifiques et protection de notre recherche, notamment à travers le dispositif de protection du potentiel scientifique et technique de la nation.

I. Un contexte stratégique mondial marqué par une massification des crises

La RNS est un document cadre à vocation interministérielle qui a été actualisé en 2025 sur demande du Président de la République. Il aborde de façon très pragmatique et concise le contexte stratégique auquel fait face la France et propose les actions nécessaires à la France pour s'adapter à cet environnement qui se dégrade.

Le scénario central dressé par la RNS est le suivant :
« L'hypothèse d'une participation des armées françaises à une guerre majeure de haute intensité dans le voisinage de l'Europe et le risque d'actions concomitantes déstabilisatrices de nature hybride pour la sécurité intérieure de la France atteignent un niveau inégalé depuis la fin de la guerre froide. La menace d'une guerre conventionnelle majeure sur le territoire national hexagonal n'est en revanche pas considérée comme crédible. » (§112).

La France doit ainsi se préparer à une situation dans laquelle elle serait engagée dans une guerre aux frontières de l'Europe, ou sa périphérie, hors du territoire national. En parallèle, il est nécessaire de se préparer à des agressions de nature hybride à des fins de rupture de la continuité de la vie de la Nation. Il faut comprendre ici ce type d'agressions : cyber, manipulation de l'information, ingérences numériques étrangères, sabotage, espionnage, instrumentalisation des troubles à l'ordre public, rupture d'approvisionnements stratégiques ou atteintes aux biens vitaux.

L'hypothèse d'une nouvelle agression russe contre l'Europe dans les trois à cinq ans est désormais centrale. Par ailleurs, la Russie continue, malgré son investissement très important dans l'effort de guerre, à mener des recherches fondamentales et appliquées dans les technologies de rupture, qui constituent un enjeu stratégique majeur pour l'avenir. Au-delà de la Russie, trois autres dynamiques structurent notre contexte géostratégique : la situation au Proche-Orient, la rivalité sino-américaine et la relation avec les États-Unis qui entre dans une incertitude structurelle.

Par ailleurs, outre l'approche géographique de la conflictualité, la RNS 2025 consacre des développements aux facteurs de déstabilisation qui se sont tous, peu ou prou concrétisés, en particulier en matière de stratégies hybrides à l'œuvre contre la France. Premièrement, la conflictualité ne se limite plus aux champs de bataille puisque l'on observe des tests de la résilience de la nation à des seuils de conflictualité extrêmement faibles. Ensuite, les attaques dans les champs de l'hybridité sont bien réelles et concernent de nombreux domaines, notamment : cyberattaques, manipulation de l'information, arsenalisation du droit (*lawfare*), économie, sabotage, ingérences. Enfin, la Russie a ainsi orchestré des opérations en France — faux cercueils sous la Tour Eiffel, tags antisémites — pour diviser et déstabiliser. Ces actions touchent aussi nos outre-mer, notamment la Nouvelle-Calédonie et les Antilles.

En dernier lieu, d'autres facteurs de déstabilisation portant en eux autant de vulnérabilités exploitables par nos adversaires, sont pris en compte : le changement climatique et l'effondrement de la biodiversité soulèvent des enjeux sécuritaires et économiques ; un renforcement des migrations massives de la population est susceptible de s'amplifier du fait du changement climatique ; une baisse structurelle des financements humanitaires est observée à l'échelle globale ; et surtout, comme déjà mentionné dans la RNS de 2022, l'innovation s'accélère de manière exponentielle , mettant les Européens au défi de rester dans la course technologique et industrielle, au cœur de la rivalité sino-américaine.

En somme, la frontière entre civil et militaire, entre-temps de paix et temps de guerre, s'est estompée. La contestation et l'hybridité deviennent la norme. La souveraineté française ne se défendra pas uniquement sur les champs de bataille traditionnels et implique tous les champs de la société.

II. L'objectif stratégique n°11 visant l'atteinte d'une « *excellence académique, scientifique et technologique au service de la souveraineté française et européenne* »

L'objectif Stratégique (OS) N°11 est un nouvel objectif et constitue une innovation de la RNS 2025. Dans sa version précédente de 2022, les objectifs en matière de recherche et de technologie étaient dilués dans les objectifs stratégiques. L'édition de 2025 fait donc de la recherche et de la technologie un objectif en soi. L'intention est d'élever les questions de recherche scientifique et de technologies au même niveau que les dix autres objectifs.

Cela reflète une évolution correspondant à une accélération du monde et des enjeux d'innovation. Le monde actuel peut se résumer à ceci : celui qui maîtrise les technologies de rupture a déjà gagné la guerre ou, *a minima*, dispose d'une position dominante. Dans le contexte actuel, l'enjeu principal de cet objectif stratégique est de stimuler et développer l'excellence scientifique, l'innovation technologique, et de ne pas se laisser distancer par des compétiteurs stratégiques. Il s'agit là d'un effort inscrit dans la durée, dans une logique de souveraineté.

Ainsi, le onzième objectif stratégique ne cherche pas à être exhaustif dans son approche, mais signale notamment quatre technologies clefs : l'intelligence artificielle (IA), le quantique, le

spatial et NRBC (pour nucléaire, radiologique, biologique et chimique). Ces technologies et disciplines doivent être maîtrisées en national, sans exclure, dans certains domaines, des possibilités de co-développement ou de co-production avec des partenaires de confiance, notamment européens. On parle ici de technologies présentant des enjeux de souveraineté, ces derniers ne se limitant pas uniquement à la dimension militaire.

Les partenariats sont importants car la recherche progresse structurellement grâce aux coopérations internationales, grâce à la confrontation des idées et des travaux de recherche entre pairs.
Il faut donc encourager ces coopérations, notamment à l'échelle européenne, qui est un espace naturel pour les chercheurs : ils y font face à des problématiques communes, partagent des valeurs communes et bénéficient de dispositifs de financement commun.

Mais il est aussi essentiel de protéger la recherche française face aux tentatives de captation dans un contexte de compétition stratégique féroce. Les États proliférant continuent de cibler la France pour acquérir des savoir-faire utiles à leurs programmes d'armes de destruction massive. Au-delà des États proliférants, la menace peut également venir de compétiteurs stratégiques pour des besoins tant économiques que militaires. À cet égard, les retours, notamment issus des services de renseignement, illustrent la réalité concrète des tentatives de captation et donc avec, l'intérêt du dispositif de protection du potentiel scientifique et technique de la nation (PPST) et de la politique de sécurité économique.

Autrement dit : il faut ouvrir la recherche autant que possible tout en la protégeant autant que nécessaire. La France est une grande nation scientifique qui suscite l'intérêt de ses compétiteurs et il est ainsi nécessaire d'encourager les coopérations internationales tout en protégeant les savoir et savoir-faire français contre les tentatives de captation étrangère.

III. <u>Quelle réponse pour allier compétitivité mondiale et nécessaire besoin de protection</u> ?

Au regard des menaces exposées, comment assurer la liberté de la recherche, inscrite dans le partage des résultats et l'ouverture internationale, tout en défendant nos intérêts, savoirs et savoir-faire ? Comment allier compétitivité mondiale et besoin de protection tout en limitant le risque de nuire à la liberté de la recherche ?

Qu'il s'agisse de propriété intellectuelle et industrielle, de sécurité, y compris face au terrorisme, ou de lutte contre la prolifération d'armes de destruction massive, le pays doit être en mesure de protéger certaines activités de recherche sensibles et combattre l'espionnage technologique pour préserver sa compétitivité.

Pour y répondre, le dispositif de protection du potentiel scientifique et technique de la nation (PPST), piloté au niveau interministériel par le secrétariat général de la défense et de la sécurité nationale, vise à protéger les savoirs, savoir-faire, et technologies stratégiques, sensibles ou innovants reconnus comme intérêts fondamentaux de la nation.

À travers un dialogue resserré entre l'État, ses services spécialisés et les acteurs de la recherche publique ou privée, cette réglementation concilie liberté de la recherche, dynamique des relations économiques et besoin de protection. Cette politique publique a été mise en place en 2011, avec pour objectif la préservation des échanges et des coopérations scientifiques, nécessaires à la recherche scientifique et au progrès technologique, tout en protégeant les intérêts fondamentaux de la Nation, définis par l'article 410-1 du Code pénal.

Ce dispositif s'adresse à tout établissement, public ou privé, qui développe ou met en œuvre au sein d'unités de recherche ou de production des savoirs, savoir-faire ou technologies dont la captation ou le détournement pourraient :

- porter atteinte aux intérêts fondamentaux de la nation, y compris économique ;
- renforcer des arsenaux militaires étrangers ou affaiblir les capacités de défense de la nation ;
- contribuer à la prolifération d'armes de destruction massive et de leurs vecteurs ;
- être utilisés à des fins terroristes sur le territoire national et à l'étranger.

Les savoirs et savoir-faire d'une unité relevant de ce dispositif peuvent alors bénéficier d'une protection juridique fondée sur le Code pénal (article R. 413-5-1). Tout établissement peut obtenir auprès des services de l'État les éléments permettant d'évaluer la pertinence de recourir au dispositif afin de protéger ses activités de recherche ou de production.

Ce dispositif, qui permet à un établissement de se prémunir plus efficacement contre les tentatives de captation d'informations, permet donc aussi à la France de respecter ses engagements internationaux, notamment en termes de lutte contre la prolifération et le terrorisme, et à l'établissement concerné d'agir en tant qu'acteur responsable. Il tient compte du fait que c'est souvent par un ensemble de savoirs et savoir-faire ciblés, une fois acquis sous forme de diverses briques, qui est utile au développement de technologies abouties, notamment dans le cadre de programmes d'armements conventionnels ou d'armes de destruction massive.

Ce dispositif repose principalement sur la délimitation, au sein des établissements publics ou privés, de zones dites « à régime restrictif » (ZRR) qui détiendraient des savoirs, savoir-faire ou technologies sensibles. L'accès à ces zones est soumis à une autorisation préalable du ministère de tutelle de l'établissement, parmi les six ministères concourant à la PPST[1].

Grâce au statut de zone protégée, des sanctions pénales s'appliquent en cas d'intrusion (article 413-7 du code pénal), qu'il s'agisse d'accès physiques ou virtuels. En cas d'intrusion ou de captation indue, le chef d'établissement a ainsi la possibilité de déposer plainte. Le dispositif tire notamment son efficacité du caractère dissuasif des peines encourues.

Ce dispositif, qui se veut toutefois le moins contraignant possible, permet ainsi :

- de disposer d'une protection juridique contre les atteintes pouvant avoir des conséquences sur la compétitivité de l'entité (utilisation frauduleuse d'informations, vol ou captation de données sensibles, pratiques anticoncurrentielles, intrusion dans les systèmes d'information, etc.) ;
- d'offrir une protection ciblée « au juste besoin » afin de protéger uniquement les informations qui doivent l'être ;
- de bénéficier d'un accompagnement étatique personnalisé et privilégié dans la démarche d'élévation du niveau de sécurité de l'établissement ;
- d'appartenir à une communauté de confiance favorable aux partenariats.

En complément, le dispositif a évolué en 2024 et 2025 au regard des risques de prédation accrus et de son ancienneté. Deux nouvelles mesures ont ainsi été ajoutées, l'une consistant en la gradation de la répression en cas de manquement ou d'obstruction aux mesures de protection des ZRR, l'autre instaurant un contrôle accru des coopérations internationales.

[1] Ministères chargés de la Défense, de l'enseignement supérieur et de la recherche, de la transition écologique, de la santé, de l'agriculture et de l'économie.

Enfin, la loi actualisée de programmation militaire, promulguée en août 2026, inclut une mesure dite « anti-débauchage » (article 33), permettant de prévenir le débauchage par une puissance étrangère de chercheurs impliqués dans des travaux particulièrement sensibles, qui sont rattachés à une ZRR.

Face à un monde en rupture où la contestation et l'hybridité sont devenues la norme, la souveraineté française et européenne ne se défendra pas uniquement sur les champs de bataille traditionnels. Elle se joue, d'abord et avant tout, au sein des laboratoires, des centres de recherche et des start-ups. C'est pour cela que l'objectif stratégique n°11 de la RNS s'inscrit dans le panorama des enjeux stratégiques actuels.