ÉTUDES
DE L'IFRI

CENTRE DES ÉTUDES DE SÉCURITÉ FOCUS STRATÉGIQUE n° 126

JUILLET
2025

Repenser la fonction « Protection – Résilience »

Un nécessaire changement de paradigme face à un environnement qui se durcit

Guillaume FURGOLLE

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une fondation reconnue d'utilité publique par décret du 16 novembre 2022. Elle n'est soumise à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

ISBN : 979-10-373-1078-1

Couverture : Opérateurs de l'armée de l'Air et de l'Espace mettant en œuvre des systèmes de défense sol-air © Jean-Luc Brunet/Armée de l'Air et l'Espace

Comment citer cette publication :

Guillaume Furgolle, « Repenser la fonction "Protection – Résilience". Un nécessaire changement de paradigme face à un environnement qui se durcit », *Focus stratégique*, n° 126, Ifri, juillet 2025.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Focus stratégique

Les questions de sécurité exigent une approche intégrée, qui prenne en compte à la fois les aspects régionaux et globaux, les dynamiques technologiques et militaires mais aussi médiatiques et humaines, ou encore la dimension nouvelle acquise par le terrorisme ou la stabilisation post-conflit. Dans cette perspective, le Centre des études de sécurité se propose, par la collection ***Focus stratégique***, d'éclairer par des perspectives renouvelées toutes les problématiques actuelles de la sécurité.

Associant les chercheurs du centre des études de sécurité de l'Ifri et des experts extérieurs, ***Focus stratégique*** fait alterner travaux généralistes et analyses plus spécialisées, réalisées en particulier par l'équipe du Laboratoire de Recherche sur la Défense (LRD).

Comité de rédaction

Auteur

Guillaume Furgolle est chercheur au sein du Laboratoire de recherche sur la défense (LRD) du Centre des études de sécurité (CES) de l'Ifri, où il contribue aux études relatives aux enjeux maritimes, notamment polaires et indopacifiques, mais également sécuritaires, capacitaires et stratégiques pour la France.

Remerciements

L'auteur remercie chaleureusement les personnalités suivantes pour leur appui dans la réalisation de cette étude :

- les divisions Protection et sécurité de l'État (PSE) et Affaires internationales, stratégiques et techniques (AIST) du Secrétariat général de la défense et de la sécurité nationale (SGDSN) ;
- la Direction de la protection des installations, moyens et activités de la défense (DPID), et tout particulièrement son directeur et son chef de cabinet ;
- la division Emploi des forces – Protection de l'État-major des Armées (EMA) ;
- l'État-major interarmées du territoire national métropolitain (EMIA TN) ;
- la Sous-direction du droit public et du droit privé de la Direction des Affaires juridiques (DAJ/D2P) du Secrétariat général pour l'administration (SGA).

Résumé

La France comme les autres pays européens est confrontée de manière directe, tout particulièrement depuis le début de la guerre en Ukraine, à une stratégie hybride de déstabilisation mise en œuvre par la Russie. Cette stratégie se matérialise dans l'ensemble des champs et des milieux possibles d'affrontement et a pour objectif, outre de saper le soutien occidental à l'Ukraine, d'affaiblir les pays européens avec lesquels la Russie se perçoit dans une confrontation systémique de long terme.

Cet emploi décomplexé d'actions déstabilisatrices, par la Russie mais pas exclusivement, qui se matérialise concrètement dans l'espace national appelle une réflexion sur la manière de s'en protéger. Cette réflexion vient naturellement questionner la fonction stratégique « Protection – Résilience », dont l'enjeu est par essence la défense des intérêts nationaux sous le seuil de la dissuasion nucléaire.

Cette fonction stratégique, dans sa forme actuelle et moderne, est le fruit d'un long processus de maturation sur les quatre-vingts dernières années, les dernières décennies ayant été significativement marquées par le terrorisme. *A contrario*, la menace étatique contre le territoire national a semblé une perspective moins actuelle et pressante que le reste des priorités stratégiques pour la France.

Le nouveau contexte géostratégique et le retour de la guerre en Europe viennent remettre en question le paradigme du territoire national préservé de la confrontation entre États. Pour autant, les fondements établis pour la protection des activités critiques sur le territoire national, nourris par plus de vingt ans de menace terroriste, apparaissent comme solides mais méritent néanmoins d'être reconsidérés pour mieux faire face à une menace étatique, composite, dirigée et organisée, qui s'inscrit dans le long terme. Par ailleurs, les développements technologiques, tels que les armes *low cost* ou l'intelligence artificielle, démultiplient la capacité de nuisance potentielle des acteurs malveillants et demandent à être pris en compte.

Au-delà, le nouveau contexte incite à repenser notre approche de la protection et de la résilience du territoire national. Alors que ce dernier revient au centre du jeu dans un espace stratégique contesté entre États et marqué par un néo-impérialisme débridé, il nous revient de déterminer les moyens et les fins auxquels que nous sommes prêts à consentir pour en assurer la protection, et ce tant en termes de ressources que sur le plan éthique ou sociétal.

Executive summary

France, like other European countries, is directly confronted with a hybrid destabilization strategy implemented by Russia, particularly since the start of the war in Ukraine. This strategy materializes in all possible fields and environments of confrontation and aims, in addition to undermining Western support for Ukraine, to weaken the European countries with which Russia sees itself in a long-term systemic face-off.

This disinhibited use of destabilizing actions, by Russia, but not exclusively, which is concretely materializing in the national space, calls for reflection on how to protect against it. This reflection naturally calls into question the "Protection – Resilience" strategic function, the essence of which is the defense of national interests below the threshold of nuclear deterrence.

This strategic function, in its current, modern form, is the fruit of a long process of maturation over the last eighty years, the last few decades having been significantly marked by terrorism. On the other hand, the state threat to France's national territory has seemed a less current and pressing prospect than the rest of France's strategic priorities.

The new geostrategic context and the return of war to Europe call into question the paradigm of national territory preserved from confrontation between states. Nevertheless, the foundations laid for the protection of critical activities on national territory, nurtured by more than twenty years of terrorist threat, appear to be solid, but nonetheless deserve to be reconsidered in order to better cope with a composite, directed and organized state threat, which is part of the long term. Technological developments, such as low-cost weapons and artificial intelligence, are multiplying the potential damaging capacity of malicious actors and need to be taken into account.

Beyond that, the new context prompts us to rethink our approach to the protection and resilience of our national territory. At a time when the latter is once again at the center of the game in a strategic space contested between States and marked by unbridled neo-imperialism, it is up to us to determine the means and ends to which we are prepared to consent in order to ensure its protection, in terms of both resources and ethical or societal considerations.

Sommaire

Introduction

Les Jeux olympiques de Paris de l'été 2024, événement international majeur pour la France se déroulant dans un contexte géopolitique sous tension, ont mis à l'honneur les enjeux de sécurité et de protection à grande échelle sur le territoire national. En effet, la réussite de cet événement, consacrée par le président de la République dans son discours de bilan, n'aurait pu être sans le très important dispositif civilo-militaire de protection associé, tant dans le champ physique que numérique.

Nonobstant cette actualité, et si les grandes fonctions stratégiques françaises ainsi que la notion de résilience ne sont formellement introduites que par le *Livre blanc sur la défense et la sécurité nationale* publié en 2008, les fondements conceptuels de la fonction « Protection – Résilience » sont, eux, gravés dans l'histoire des sociétés humaines : défendre le territoire, protéger les populations, être capable de faire face aux crises. Aussi, ce qui caractérise la protection sur le plan stratégique, c'est avant tout le contexte dans lequel elle s'inscrit.

La chute de l'Union des républiques socialistes soviétiques (URSS) en 1991 vient mettre fin à la menace existentielle qui pesait sur la France depuis des décennies dans un contexte de guerre froide entre deux blocs de nations. Dès sa formalisation, la fonction « Protection – Résilience » s'inscrit donc dans un contexte d'engagements extérieurs pour la France et de guerre au loin contre le terrorisme international, laissant le territoire national en retrait, bien que la menace terroriste y soit un sujet d'attention épisodique depuis 1978[1]. Toutefois, la série des attentats djihadistes sur le territoire national qui débute en 2012 vient progressivement bousculer le relatif sentiment de sécurité du territoire national, sans néanmoins menacer les fondamentaux de la bonne marche de la nation.

Par la suite, une série d'événements majeurs en France et dans le monde vient éprouver la confiance de la nation en matière de protection du territoire national et de résilience : les attentats de 2015, la pandémie de Covid-19 en 2020, la guerre russo-ukrainienne en 2022, puis l'attaque du Hamas contre le sud d'Israël en 2023. En toile de fond, les matérialisations de plus en plus agressives et désinhibées des logiques de puissance mises en œuvre par des compétiteurs stratégiques, au premier rang desquels la Russie, viennent mettre à mal le sentiment d'un territoire national préservé des agressions étatiques par le statut de puissance nucléaire de la France.

1. Attentat de mai 1978 à Orly, attentats du Groupe islamique armé (GIA) en 1995 et 1996, attentats de Madrid et de Londres en 2004-2005.

Ce bouleversement s'accompagne de l'émergence de nouvelles menaces, rendue possible par la prolifération technologique : attaques saturantes et frappes à longue distance, prolifération et sophistication des manœuvres dans le champ numérique, le tout potentiellement perpétré par des acteurs non étatiques. En parallèle, le changement climatique qui s'accélère s'accompagne de la survenance de plus en plus fréquente de phénomènes extrêmes (sécheresses, incendies, inondations, cyclones et tempêtes, montée des eaux) qui font peser un risque naturel accru et indiscriminé sur les sociétés humaines fragilisées par le contexte géopolitique marqué par la conflictualité et les tendances nationales au repli sur soi.

La fonction stratégique « Protection – Résilience » est par essence duale, en ce sens qu'elle s'adresse tant aux menaces qu'aux risques, naturels, sanitaires ou autres. Il peut en outre y avoir une porosité entre menaces et risques, à l'instar des risques sociaux qui peuvent constituer une menace lorsqu'ils sont instrumentalisés. La distinction entre menaces et risques, c'est le caractère intentionnel et dirigé de ces premières, ainsi que la volonté de nuire qui les sous-tend, *a contrario* de la nature chaotique et indiscriminée des risques. Cette étude prend donc le parti de se focaliser sur les menaces, pour lesquelles la réponse concerne ou implique plus directement le volet défense et sécurité de l'État. L'étude se concentre sur les menaces exogènes et leurs manifestations internes directes, telles que les instrumentalisations, considérant que les menaces internes (groupes extrémistes, terrorisme militant ou politique) ne sont pas l'objet de la bascule stratégique à l'œuvre, bien que ces deux types de menaces puissent se répondre l'une l'autre. Enfin, parmi l'ensemble des acteurs qui concourent à la fonction « Protection – Résilience », l'étude se focalisera principalement sur la contribution des armées.

Les stratégies hybrides mises en œuvre par certains de nos compétiteurs ou adversaires se matérialisent par un emploi opportuniste de l'ensemble de la palette des modes d'action possibles, dans tous les champs d'affrontement, en vue de déstabiliser nos sociétés pour prendre l'avantage dans la compétition stratégique. Outre l'existence de cultures stratégiques favorisant le recours à l'hybridité, comme en Russie, ces stratégies sont notamment permises par la centralisation du pouvoir dans les régimes autoritaires ainsi que par une certaine pratique mettant en avant les services secrets ou spéciaux et l'action clandestine. Cela doit inciter à sortir d'une logique de protection par milieu ou domaine, qui peut sembler plus efficace ou simple à mettre en œuvre mais ne répond pas à la transversalité de la menace hybride.

Ce panel de menaces et de risques étendu, pour une grande partie déjà existant mais qui se manifeste de manière plus aiguë, incite à questionner l'approche française de la fonction stratégique « Protection – Résilience », tant dans ses fondements conceptuels que sur la pertinence de sa

déclinaison actuelle. En particulier, dans la France d'aujourd'hui, quelles doivent être la place et les modalités pour la contribution des armées à la réponse de l'État face à des agressions contre le territoire, la population ou les intérêts nationaux, *a fortiori* de nature militaire ?

Pour cela, cette étude se propose tout d'abord de revenir sur le processus de genèse et de maturation de la fonction stratégique « Protection – Résilience ». Ensuite, elle s'attachera à caractériser les menaces actuelles et potentielles qui pèsent sur les intérêts français et méritent d'être prises en compte. Elle mettra ensuite en lumière les atouts, les faiblesses et les dynamiques du dispositif français de protection face à ces menaces. Enfin, elle explorera quelques pistes d'amélioration du dispositif national de « Protection – Résilience », en prenant en compte les spécificités françaises dans la possible réponse nationale à cette problématique qui touche plus largement l'ensemble des pays européens.

Avant tout développement, une question sémantique émerge. En effet, plusieurs termes coexistent dans le domaine de la protection et de la résilience. De manière non exhaustive, on peut citer : vital, stratégique, critique, essentiel.

- *Vital*, au sens des intérêts vitaux couverts par la dissuasion nucléaire, se réfère à ce qui touche à la survie de l'État et de la nation. Cependant, les activités d'importance vitale pour l'État, au sens du dispositif correspondant (SAIV), sont celles dont le dysfonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, ou encore l'exercice de l'autorité de l'État[2]. Cela représente donc une acception plus large et moins exclusive.
- *Stratégique* est un terme relatif à l'art de la guerre. Il désigne normalement ce qui présente un intérêt du point de vue militaire, ou donne un avantage décisif dans la confrontation avec un adversaire. Aussi, est stratégique ce qui est indispensable à la manœuvre militaire ou à l'action politique de l'État dans le cadre d'une confrontation au niveau étatique, voire para-étatique.
- *Critique* est étymologiquement associé à la notion de changement, de seuil. Est critique ce qui conditionne la bascule entre deux états. En termes de protection, et de résilience, on peut ainsi imaginer que critique devrait se référer à ce qui conditionne la bascule d'un état normal de la vie de la nation sous contrôle à un état hors de contrôle.
- *Essentiel* est ce qui a trait à l'essence, la nature fondamentale des choses et des êtres. Plus communément, il désigne ce qui est indispensable ou d'une grande importance. C'est cette acception qui vaut pour le

2. Instruction générale interministérielle n°6600/SGDSN/PSE/PSN du 7 janvier 2014 relative à la sécurité des activités d'importance vitale.

dispositif des Opérateurs de services essentiels (OSE). Néanmoins, le positionnement du dispositif OSE par rapport au dispositif SAIV semble placer *de facto* en retrait par rapport au terme vital dans la sémantique de l'État.

Ainsi, la multiplication incrémentale des initiatives pour mieux protéger ce qui doit ou mérite de l'être, avec des appellations variables, peut conduire une certaine confusion parmi les acteurs non initiés qui apparaît préjudiciable à la bonne appréhension des enjeux en la matière. Une clarification institutionnelle formelle pourrait s'avérer pertinente pour lever ces ambiguïtés.

La fonction stratégique « Protection – Résilience » : genèse et maturation

Le cœur conceptuel de la fonction Protection est la défense du territoire et la protection des Français sur leur sol. Si les fonctions stratégiques dans leur acception actuelle n'apparaissent formellement qu'en 2008, le concept de protection du territoire national n'est bien évidemment pas nouveau et sa maturation s'inscrit dans le contexte historique, avec des épisodes récents de ruptures qui influencent profondément son évolution.

Alors que les guerres qui ont marqué l'histoire européenne ont naturellement fait de la défense du territoire un enjeu majeur pendant des siècles, l'avènement de l'Organisation du traité de l'Atlantique nord (OTAN), la logique de la guerre froide et la dissuasion nucléaire éloignent durablement la menace étatique du territoire national. La fonction stratégique Protection naît ainsi comme une construction hybride, avec une approche duale civilo-militaire entre risques et menaces, et dans une logique de défense dans la profondeur. Il s'agit d'agir à la source sur les phénomènes projetés qui impactent le territoire national. Le terrorisme international, le durcissement de la compétition stratégique puis le retour de la guerre en Europe viennent pourtant mettre à mal ce paradigme et replacer la défense du territoire au cœur des préoccupations.

Des fondements historiques : la Garde nationale et la défense du territoire

Fruit de divers forums populaires et milices communales nées de la Révolution française de 1789, la Garde nationale perdure pendant l'essentiel du XIXe siècle. Son rôle est d'assurer le maintien de l'ordre dans chaque commune en temps de paix mais également la défense militaire du pays en temps de guerre, en complément de l'armée régulière, en s'appuyant en masse sur la jeunesse. La Garde nationale est maintenue jusqu'à sa dissolution en juillet 1871, aux lendemains des insurrections de la Commune de Paris qu'elle a soutenues[3]. Le vide créé par sa dissolution est compensé en 1872 par la création de la réserve militaire et de l'armée territoriale[4].

3. R. Dupuy, *La Garde nationale, 1789-1872*, Paris, Gallimard, 2010.
4. X. Boniface, « La réforme de l'armée française après 1871 », *Inflexions*, vol. 2012/3, n° 21, p. 41-50.

Quatre-vingts ans plus tard, les enseignements de la Seconde Guerre mondiale conduisent à une réflexion de fond sur la notion de défense du territoire. Ainsi, fort du traumatisme qu'a représenté la campagne de France, le général de Gaulle signe en janvier 1945 un décret portant création du Commandement de la défense aérienne du territoire (DAT), comme manifestation de la volonté de restaurer la souveraineté nationale sur le territoire métropolitain[5]. La Posture permanente de sûreté aérienne (PPS-A) est ensuite initiée en 1964 en parallèle de l'avènement des capacités françaises de dissuasion nucléaire, à savoir la création des Forces aériennes stratégiques et l'arrivée dans les forces des premiers bombardiers *Mirage* IV et des premiers ravitailleurs C-135F[6].

En matière de défense terrestre, les leçons du second conflit mondial, au travers de l'emploi des troupes aéroportées pour des assauts sur les lignes arrière, mais aussi les actions clandestines de la résistance et des maquis, illustrent la nécessité de protéger les arrières du front. La situation insurrectionnelle de 1947, tentative de coup d'État pilotée par le Parti communiste français, marque profondément les esprits et finit de convaincre du besoin de mettre en place un dispositif de défense du territoire. Placé sur l'arrière du corps de bataille, il a vocation à déjouer les actions subversives pouvant être menées par l'URSS et ses relais communistes. Une nouvelle organisation, la Défense intérieure du territoire (DIT), est instaurée quelques années plus tard en 1956 pour faire face à cette menace de type subversif alors mieux appréhendée. Prenant acte de l'incapacité d'un dispositif purement militaire à y faire face, la participation civile est accrue, au travers notamment d'états-majors mixtes civilo-militaires, et le maintien de l'ordre y est traité de manière comparable à la défense contre les éléments ennemis implantés, parachutés, débarqués ou infiltrés[7]. La DIT comprend aussi un volet d'action psychologique visant à se protéger de la propagande de guerre de l'adversaire.

À la suite du putsch des généraux de 1961 en Algérie, un processus de construction législative aboutit en 1962 à la définition des fondements d'une riposte militaire aux actions subversives au moyen d'une Défense opérationnelle du territoire (DOT)[8], qui voit coexister les pouvoirs civils et militaires. Outre la menace subversive, cette DOT se conçoit aussi et surtout face à la menace d'invasion militaire par les forces du pacte de Varsovie : couverture des arrières durant la phase d'affrontement, mais aussi ensuite résistance militaire décentralisée en cas d'invasion.

5. L. Rataud, « La défense aérienne est consubstantielle de l'ambition de souveraineté », Institut des hautes études de défense nationale (IHEDN), non daté.
6. « La posture permanente de sûreté aérienne française », Direction de la mémoire, de la culture et des archives, Secrétariat général pour l'administration du ministère des Armées, non daté.
7. A. Bizard, « La Défense opérationnelle du territoire (DOT) », *Pouvoirs,* n° 38, 1986, p. 87-97.
8. Décret n° 62-209 du 24 février 1962 fixant les attributions de l'inspecteur général de la défense opérationnelle du territoire, *Journal officiel de la République française*, 25 février 1962.

Dans le prolongement du *Livre blanc sur la défense* de 1972, les fondements de la défense du territoire sont ensuite clarifiés par un décret en 1973. Il stipule que, contrairement aux défenses aérienne et maritime du territoire, la DOT n'est pas permanente mais mise en œuvre sur décision du gouvernement en cas de menace avérée, et s'inscrit en complément de la défense civile. Sa finalité est triple : assurer la protection des installations militaires (prioritairement celles liées à la force nucléaire stratégique), s'opposer aux actions ennemies à l'intérieur du territoire, et mener des opérations de résistance militaire en cas d'invasion. Les plans de défense associés au concept de DOT couvrent l'ensemble du territoire, au travers de la défense des points sensibles mais également de la défense d'ensemble qui consiste à compliquer la tâche de l'ennemi *via* le contrôle du territoire[9].

Les armées participent à cette époque de façon inégale à la DOT. La gendarmerie en est la composante majeure, portant notamment la responsabilité de la protection des points sensibles civils nationaux et de l'action de premier niveau contre les menaces isolées. En deuxième niveau, l'armée de Terre fournit des forces de niveau régimentaire. L'ensemble des forces impliquées dans la DOT repose toutefois très largement sur la mobilisation des réserves[10].

Si le concept de DOT est le fruit d'une longue antériorité historique, sa formalisation moderne est assez tardive et s'adapte progressivement en se complexifiant. Pour autant, la DOT reste toujours une priorité moindre de la défense militaire et bénéficie d'organisations robustes et bien décrites, mais de moyens bien en retrait de l'ambition. En outre, la DOT s'inscrit dans le contexte spécifique de la guerre froide. Avec la fin de la menace soviétique en 1991, le volet permanent de la DOT continue d'être assuré, notamment par la gendarmerie, mais les moyens de réserve et de mobilisation affectés aux missions non permanentes de la DOT diminuent progressivement, voire disparaissent[11].

Sur le plan maritime, au-delà du *Livre blanc* de 1972 – et bien que la protection des approches maritimes nationales ait toujours été une des missions premières de la Marine nationale, *a fortiori* nucléaire –, le concept de sauvegarde maritime n'est formalisé qu'au début des années 2000. Il se traduit par la Posture permanente de sauvegarde maritime (PPSM) qui regroupe l'ensemble de ses missions relevant de la Défense maritime du territoire (DMT) et de l'Action de l'État en mer (AEM). Cette approche moderne acte le caractère global de la notion de protection face à un panel

9. Décret n° 73-235 du 1er mars 1973 relatif à la défense opérationnelle du territoire, amendé par décret le 24 avril 2007.
10. A. Bizard, « La Défense opérationnelle du territoire (DOT) », *op. cit.*
11. « La défense opérationnelle du territoire (DOT) : quels enjeux et quels moyens », Direction de la mémoire, de la culture et des archives, Secrétariat général pour l'administration du ministère des Armées.

large et composite de menaces et de risques, et préfigure la forme actuelle de la fonction stratégique « Protection[12] ».

Au bilan, on peut voir que la formalisation de la protection comme fonction stratégique trouve ses racines au lendemain de la Seconde Guerre mondiale et de l'occupation, et ce sans surprise, la défense du territoire étant consubstantielle de la notion de souveraineté.

Une formalisation moderne incrémentale mise au défi par la menace terroriste

Le *Livre blanc sur la défense* publié en 1972, dans le contexte de l'accession par la France à une capacité nucléaire complète, regroupe les capacités attendues des forces armées en quatre piliers : la capacité nucléaire de dissuasion, la défense du territoire, la manœuvre en Europe et la capacité d'action hors-Europe[13]. Si en termes de protection, la priorité d'alors est clairement donnée aux éléments de la Force nucléaire stratégique, les germes de la future fonction stratégique y sont tous déjà présents : la défense militaire du territoire, mais également celle de ses approches maritimes et de son espace aérien, ainsi que la résilience de la société *via* notamment la protection de ses infrastructures critiques. Ces trois piliers de la stratégie de défense française – dissuasion nucléaire, protection et intervention – constituent un socle conceptuel qui va perdurer pendant plusieurs décennies.

En effet, si les événements survenus après la chute du mur de Berlin, notamment la disparition du pacte de Varsovie, les mutations accélérées de l'environnement européen et international, les progrès technologiques ou économiques, motivent la rédaction d'un nouveau *Livre blanc* en 1994, ce dernier ne marque pas une rupture par rapport à la politique de défense définie par Georges Pompidou et Michel Debré en 1972[14].

Pour autant, les attentats perpétrés par le Groupe islamiste armé (GIA) algérien en France en 1995 conduisent le gouvernement français à réactiver au stade renforcé le plan Vigipirate[15], version améliorée du plan Pirate créé en 1981 à la suite de la vague d'attentats perpétrée par des organisations palestiniennes et d'extrême gauche en 1978. Ce plan, qui définit la répartition des responsabilités et les principes de l'action de l'État dans le cadre de la lutte contre le terrorisme, s'inscrit bien dans le champ de la vigilance, de la prévention et de la protection. Certaines mesures du plan font appel aux armées. Les dispositifs de l'armée de l'Air et la Marine nationale qui assurent en permanence la protection de l'espace

12. C. Girard, « La sauvegarde maritime », *La Jaune et la Rouge*, n° 596, 2004.
13. *Livre blanc sur la défense*, 1972.
14. *Livre blanc sur la défense*, 1994.
15. Vigilance et protection des installations contre les risques d'attentats terroriste à l'explosif.

aérien et des approches maritimes sont intégrés dans le plan Vigipirate. En complément, de 700 à 1 100 militaires sont déployés pour le volet terrestre, dont près de la moitié en Île-de-France. Le plan Vigipirate, jamais désactivé depuis 1995, constitue ainsi le premier jalon de l'engagement moderne des forces terrestres pour la protection du territoire national.

Quelques années plus tard, les événements du 11 septembre 2001 marquent une rupture à l'échelle mondiale de la perception de la menace aérienne. L'éventualité d'un détournement d'avions civils par des terroristes pour les utiliser comme des armes de destruction de grande ampleur est prise en compte et conduit à un renforcement significatif de la posture permanente de sûreté aérienne française[16].

Le *Livre blanc sur la défense et la sécurité nationale* publié en 2008, plus de vingt ans après le précédent, est le premier à s'inscrire dans le cadre d'une armée professionnelle. Il introduit cinq grandes fonctions stratégiques, identifiées progressivement depuis la fin de la conscription et qui reflètent les réalités stratégiques du moment : dissuasion ; protection ; prévention ; intervention ; connaissance et anticipation.

Le couple dissuasion et protection traduit la permanence défensive, et le couple prévention et intervention traduit la disponibilité offensive. La cinquième fonction a vocation à éclairer les incertitudes qui caractérisent l'environnement stratégique et à orienter l'action dans les quatre autres fonctions. Le *Livre blanc* de 2013 vient actualiser celui de 2008 au prisme des changements majeurs intervenus dans l'environnement international depuis, notamment les révolutions arabes, la crise économique de 2008 et le pivot américain vers le Pacifique[17]. Les trois piliers de la stratégie de défense française, protection, dissuasion et intervention, y sont réaffirmés, ainsi que les cinq grandes fonctions stratégiques.

L'enjeu de la protection est clairement affiché dans la description de la fonction stratégique correspondante. Il s'agit de garantir l'intégrité du territoire, assurer aux Français une protection efficace contre l'ensemble des risques et des menaces dont l'impact pourrait être majeur, préserver la continuité des grandes fonctions vitales de la Nation et conforter sa résilience. Elle s'exerce en priorité sur le territoire national et les zones de forte implantation ou de forte exposition des communautés françaises à l'étranger.

Pour autant, bien que plus pressante qu'auparavant depuis la fin de la guerre froide, la menace est perçue comme encore distante, comme l'illustre l'accent mis sur l'analyse des risques et la fonction renseignement. La prise en compte de cette menace est donc pour la France du ressort de l'action

16. B. Foussard et T. Garreta, « Quelle action de l'Armée de l'air face aux menaces au-dessus de nos villes ? », *Revue de la Défense Nationale*, 2017/1, n° 796, p. 63-67.
17. *Livre blanc sur la défense et la sécurité nationale*, 2013, p. 7-8.

internationale, que ce soit dans le cadre de l'Union européenne (UE), de l'OTAN ou en coalition de circonstance. Le *Livre blanc* de 2013 est ainsi axé sur l'engagement de la France sur la scène internationale, en concertation étroite avec ses partenaires européens comme avec ses alliés, tout en maintenant une capacité d'initiative propre. Pour autant, dans un contexte de contrainte budgétaire, le *Livre blanc* de 2013 vient acter la suppression de 34 000 postes sein du ministère de la Défense sur la période 2014-2019, avec une volonté affichée de prioriser des capacités autonomes et réactives de projection, en mesure d'agir au loin sur les menaces les plus significatives sur les intérêts de la France et ceux de ses partenaires et alliés.

Par conséquent, en l'absence de menace perçue de nature militaire contre le territoire national, la mission des armées y est essentiellement envisagée au travers des dispositifs permanents de sûreté. En complément, les armées peuvent se voir confier en cas de crise majeure, sur réquisition de l'autorité civile, des missions de défense et de sécurité civile en renfort des forces de sécurité intérieure[18] notamment avec des moyens spécialisés. Le principe établi est de ne recourir aux armées dans ce contexte que lorsque les moyens de l'autorité civile sont estimés indisponibles, inadaptés, inexistants ou insuffisants (règle des 4 « I »[19]).

Les attentats de janvier 2015[20] en région parisienne, revendiqués par l'organisation terroriste islamiste Al-Qaïda dans la péninsule arabique (AQPA), viennent tragiquement remettre en question ce paradigme stratégique de la menace distante. Cette menace terroriste dirigée contre la France fait instantanément de la protection du territoire national et de la population l'une des priorités stratégiques du moment. Elle conduit en particulier au lancement en urgence de l'opération militaire Sentinelle, en complément du plan Vigipirate de lutte contre la menace terroriste en vigueur depuis 1995. Dans les jours qui suivent les attaques, les effectifs militaires déployés sur le territoire sont portés à 10 000 personnes, notamment dans la capitale, pour assurer la sécurité des lieux jugés sensibles : transports, gares, aéroports ou lieux de culte notamment[21]. Malgré Sentinelle, d'autres attentats ou tentatives d'attentats mobilisent les forces de sécurité tout au long de l'année 2015.

En ce sens, l'année 2015 représente une rupture dans la perception par la France de l'immunité de son territoire national. En effet, ces actes de terrorisme sont qualifiés « d'actes de guerre commis sur le sol français, qui sont le fait d'organisations terroristes militarisées, capables de planifier des

18. Code de la défense, article L.1321-1, disponible sur : www.legifrance.gouv.fr.
19. *Ibid.*
20. Attentats sur *Charlie Hebdo* et l'Hyper Cacher.
21. E. Tenenbaum, « La Sentinelle égarée ? L'armée de Terre face au terrorisme », *Focus stratégique*, n° 68, Ifri, juin 2016.

actions coordonnées et de manœuvrer comme des commandos[22] ». Le Parlement justifie la militarisation de la réponse et l'ampleur du dispositif Sentinelle par la dangerosité de cette menace. Il s'agit non de renforcer des forces de sécurité défaillantes mais de montrer que la réponse apportée à des attaques aussi agressives sur le sol français est une réponse militaire et massive. Le recours aux armées est donc un choix politique délibéré[23].

Le changement majeur apporté par l'opération Sentinelle est l'accroissement de la visibilité de l'action des armées dans le cadre de la sécurité intérieure sur le territoire national. En effet, de simple force d'appoint ponctuelle aux forces de sécurité intérieure dans le cadre du plan Vigipirate, leur rôle devient plus permanent et significatif dans le cadre de Sentinelle. Des réformes sont même engagées à partir de 2016 afin de répondre aux questions juridiques posées par cette forme de contribution des armées à la sécurité intérieure. Une Posture de protection terrestre (PPT), déclinée en contrat opérationnel de protection, est définie en 2016[24]. En cas de crise majeure sur le sol national, elle permet de déployer jusqu'à 10 000 militaires en trois échelons pendant un mois, sur réquisition de l'autorité civile, en appui aux forces de sécurité intérieure. Pour autant, le principe de primauté de ces dernières pour le maintien de l'ordre ou contre la menace terroriste demeure.

L'effort considérable des armées pour assurer la défense du territoire national dans ce contexte de menace terroriste, à savoir le déploiement sur le territoire de 7 000 à 10 000 militaires entre janvier 2015 et fin 2016 alors qu'il avait été envisagé initialement pour une courte durée, va être par la suite ajusté pour répondre au besoin dans la durée sans obérer la capacité de l'armée de Terre à assurer ses autres missions ainsi que sa préparation opérationnelle. Le dispositif Sentinelle est réagencé fin 2017, *via* le placement d'une partie des forces en alerte, dans l'optique de réduire le volume de forces déployé en permanence sur le territoire[25].

En parallèle, si la *Revue nationale stratégique* publiée en octobre 2017 reconnaît la persistance de la menace du terrorisme djihadiste, elle ne le considère que comme l'un élément du catalogue des nombreuses priorités françaises, dans un environnement stratégique incertain et un cadre budgétaire très contraint[26], en dépit d'une Loi de programmation militaire (LPM) 2014-2019 réactualisée à la hausse en 2015 suite au lancement de

22. O. Audibert Troin et C. Léonard (rapporteurs), *Rapport d'information sur la présence et l'emploi des forces armées sur le territoire national*, Rapport n° 3864, Paris, Commission de la Défense nationale et des forces armées, Assemblée nationale, juin 2016.
23. L'opération Sentinelle, Cour des comptes, septembre 2022.
24. E. Boz-Acquin, « Le nouveau cadre juridique d'intervention des forces armées en milieu terrestre face au terrorisme », *Notes de la FRS*, Fondation pour la recherche stratégique, août 2020.
25. « *Sentinelle* : bilan et perspectives pour les années à venir », Fondation IFRAP, 21 septembre 2017.
26. B. Alomar, « *Revue stratégique de défense et de sécurité nationale* : une occasion manquée ? », *Revue de la défense nationale*, vol. 10, n° 805, 2017, p. 34 -38.

l'opération Sentinelle et pour assumer le coût des engagements extérieurs[27]. Face aux affirmations de puissance et au déclin du multilatéralisme, le rôle des armées à l'extérieur du territoire national est réaffirmé, dans la prévention et l'intervention, en réponse aux crises comme pour permettre à la France d'être fidèle à ses engagements internationaux et de donner corps à ses partenariats stratégiques, en Afrique, au Moyen-Orient, en Asie-Pacifique.[28]

L'enjeu renouvelé de la protection et l'avènement de la résilience comme facteurs stratégiques

En dépit du poids de Sentinelle, notamment pour l'armée de Terre, le recentrage stratégique de 2015-2016 est de courte durée pour une France résolument tournée vers l'extérieur et qui se conçoit comme un acteur du monde. Il permet néanmoins de reposer les bases d'une capacité des armées à opérer sur le territoire national, et à mieux faire face aux menaces auxquelles elles y sont confrontées.

Ainsi, outre Sentinelle, la menace terroriste contre le territoire national amène, tout particulièrement à partir de 2015, à une prise de conscience du besoin de renforcer le dispositif de protection des emprises et des infrastructures militaires et la sûreté des agents du ministère de la Défense. En parallèle du lancement de l'opération Sentinelle, et en réaction à des projets d'attentats déjoués contre des emprises de la Marine nationale, un plan Cuirasse est activé par les armées pour renforcer la protection des emprises militaires. Le lancement de ce plan permet de mettre en évidence de réels besoins en matière d'infrastructures de protection. Ce plan Cuirasse n'empêche toutefois pas le vol largement médiatisé d'au moins 150 détonateurs et de pains de plastic sur le dépôt de munitions de Miramas dans les Bouches-du-Rhône à l'été 2015, qui vient directement et publiquement questionner l'efficacité du dispositif de protection des sites militaires[29], après notamment des années de sous-financement matériel et humain du volet infrastructures pour cause de restrictions budgétaires.

Cela conduit le ministère de la Défense à lancer un « plan d'urgence » pour renforcer la protection des emprises militaires et confirme le bien-fondé de la décision, prise dès septembre 2014, de la création d'une structure responsable devant le ministre de la Défense de la protection des entités relevant de son ministère. La mission de celle-ci, tout d'abord restreinte aux installations liées à la dissuasion, est très vite élargie à

27. Opération Sangaris en République centrafricaine, opération Barkhane au Sahel, opération Chammal en Irak et en Syrie.
28. « Préface du Président de la République », *Revue nationale stratégique*, octobre 2017.
29. « Vol d'explosifs à Miramas : la Défense lance un plan d'urgence », Challenges, 30 juillet 2015.

l'ensemble du ministère, des entreprises de défense et des établissements publics rattachés. La création de la Direction de la protection des installations, moyens et activités de la Défense (DPID) est officialisée par décret en août 2015[30].

Conséquence des vols de Miramas, la DPID est chargée d'une évaluation de la protection de l'ensemble des dépôts de munitions, avant de mettre en œuvre dès 2016 un schéma directeur fonctionnel « Sécurité – Protection » visant à rehausser le niveau de protection des emprises sensibles au travers d'un plan d'équipement de plusieurs centaines de milliers d'euros échelonné sur la période 2017-2022.

Parallèlement, la France est confrontée au retour des stratégies de puissance. Ainsi, le retour de la Russie sur la scène internationale comme puissance militaire de premier plan, notamment après la crise russo-géorgienne de 2008, l'annexion de la Crimée en février 2014 et l'implication dans la crise syrienne à partir de 2015, est bien souligné par la *Revue nationale stratégique* de 2017. Cette dernière évoque également la Chine, sans s'attarder toutefois sur le retour à grande échelle d'une course aux armements dans une optique classique de puissance, telle que la Chine la conduit déjà à cette époque. La *Revue nationale stratégique* évoque les questions de désinformation et les manœuvres dites « ambiguës », en désignant principalement la Russie. Ces dernières sont les manifestations de stratégies indirectes employées par ces puissances, dans une logique d'économie des forces ou de maîtrise de l'escalade, afin par exemple de rester sous le seuil de l'agression caractérisée[31].

La pandémie mondiale de Covid-19 qui débute en janvier 2020 vient étouffer l'écho de ces stratégies de puissance, en contraignant l'ensemble des pays du monde à se focaliser sur leur situation sanitaire intérieure, et en suscitant une forte coopération internationale dictée par la nécessité. L'« opération militaire spéciale » russe contre l'Ukraine en février 2022 agit comme un électrochoc et vient marquer sans plus aucune ambiguïté le retour de la guerre sur le continent européen et, à travers lui, la possibilité d'une attaque militaire contre un État européen, ou d'actes agressifs à l'encontre de ses infrastructures militaires ou civiles.

En parallèle du retour des manifestations de la puissance, la notion de résilience prend progressivement une dimension stratégique. Le concept de résilience émerge initialement dans le champ des sciences sociales et de la stratégie avec les attentats du 11 septembre 2001[32]. Il qualifie la capacité de l'ensemble d'une entité politico-stratégique à résister aux conséquences

30. S. Taleb, « Après le vol d'explosifs à Miramas, l'armée engage un plan d'urgence pour la protection des sites de munitions », *Huffington Post*, 30 juillet 2015.
31. E. Tenenbaum, « Le piège de la guerre hybride », *Focus stratégique*, n° 63, Ifri, octobre 2015.
32. A. Leprince, « Le concept de résilience face au terrorisme », *Revue de la Défense nationale*, vol. 8, n° 803, 2017, p. 61-66.

d'une agression ou d'une catastrophe majeure, puis à rétablir rapidement sa capacité à fonctionner dans un mode acceptable. Il apparaît dans les textes officiels au travers du *Livre blanc sur la défense et la sécurité nationale* de 2008, avec un caractère essentiellement institutionnel. Il s'élargit par la suite dans le *Livre blanc* de 2013, où la résilience est appréhendée comme le fruit de la vigueur du lien armées-nation et de l'appropriation collective de la stratégie de défense et de sécurité nationale[33].

C'est toutefois la *Revue nationale stratégique* de 2017 qui pose pour la première fois la résilience comme l'un des composants de l'autonomie stratégique de la France[34]. Par la suite, la crise du Covid-19 entre 2020 et 2022 met bien en évidence l'enjeu de résilience au travers de la continuité des fonctions essentielles de la nation (santé, services publics, transports, etc.) ainsi que sur le plan matériel avec la question des stocks stratégiques (stocks pétroliers, matériel médical, voire stocks alimentaires). L'opération militaire sur le territoire national lancée en 2020 dans le contexte de la crise sanitaire est d'ailleurs opportunément nommée Opération Résilience.

La prise en compte de cet enjeu est formalisée au travers de la *Stratégie nationale de résilience* (SNR) publiée en avril 2022, qui a pour objectif de bâtir la résilience de la société. Le cadre conceptuel de cette stratégie est bien évidemment la gestion des catastrophes, naturelles ou industrielles, mais également la réponse aux menaces de nature humaine : manipulations de l'information, ingérences, cyberattaques, voire guerre hybride ou agression armée. L'attaque du Hamas contre Israël le 7 octobre 2023, puis les salves de missiles échangées entre l'Iran, les Houthis et Israël viennent ensuite achever de convaincre, s'il en était besoin, de l'impérieuse nécessité de bâtir la résilience de la nation dans un contexte géopolitique brutal et décomplexé.

C'est dans ce contexte général menaçant que s'inscrit la réflexion sur la fonction stratégique « Protection – Résilience » portée par cette étude. Toutefois, l'efficacité de tout dispositif de protection, tout comme la résilience, ne se conçoivent qu'en rapport avec une menace bien identifiée. Il convient donc de dresser un état des lieux de la menace et de la façon dont le dispositif actuel de protection est armé pour y répondre.

33. *Ibid.*
34. *Revue nationale stratégique*, octobre 2017, p. 56.

Un spectre de menace élargi

À l'instar des autres pays européens, la France est actuellement confrontée à un large panel de menaces contre son territoire, ses infrastructures matérielles ou immatérielles, ou sa population. Certaines sont actuelles et avérées, d'autres potentielles ou en gestation.

Le tableau ci-dessous dresse un classement synthétique de ces menaces, très variables tant en termes d'origine, de finalité ou de criticité. Pour autant, toutes intéressent et posent un défi au dispositif national de protection, et méritent pour cela d'être prises en compte.

Panel des menaces identifiées, existantes ou potentielles

Types de menaces	Types d'acteurs	Milieu d'action	Finalité
Attentats terroristes	Non étatique / Interne (endoctrinés)	Physique	Effet psychologique
Sabotage	Étatique / Interne (*proxies*)	Physique	Perturber une capacité critique
Attaques indirectes, non attribuées (missiles, drones…)	Étatique / Non étatique (*proxies*)	Physique	Perturber une capacité critique
Attaque directe limitée (missiles de croisière ou balistiques)	Étatique / Non étatique (*proxies*)	Physique	Perturber une capacité critique
Assasinats	Étatique / Non étatique (djihadistes) / Interne (*proxies*)	Physique	Perturber une capacité critique / Effet psychologique
Espionnage	Étatique / Interne (*proxies* ou sympathisants)	Informationnel	Renseignement
Survols, violation de l'espace aérien	Étatique / Interne (*proxies* ou sympathisants)	Informationnel	Intimidation / Renseignement / Tester le dispositif
Cyberattaques	Étatique / Non étatique (sympathisants ou criminels)	Numérique	Perturber une capacité critique / Perturber le fonctionnement de la société
Actions informationnelles (propagande, désinformation, ingérence électorale)	Étatique / Non étatique (sympathisants)	Informationnel	Effet psychologique / Perturber le fonctionnement de la société
Corruption, subversion	Étatique / Non étatique (sympathisants)	Humain	Renseignement / Perturber une capacité critique

Source : tableau réalisé par l'auteur © Ifri, 2025.

Du groupuscule à l'État puissance : un large éventail d'acteurs

Dans le contexte international et l'environnement sécuritaire actuels, on peut distinguer quatre principaux types d'acteurs pouvant être à l'origine de menaces contre le territoire national. Leur diversité complexifie d'autant la tâche des acteurs de la protection.

Le premier de ces acteurs est la mouvance djihadiste internationale. La situation s'est améliorée avec notamment la fin du califat de l'État islamique (EI) en Syrie, en 2019, qui a vraisemblablement réduit sa capacité projetée de nuisance[35]. Ensuite, le dispositif français de lutte antiterroriste a été amélioré suite aux attentats de 2015[36], avec notamment le renforcement technique, financier et humain des services de renseignement (Direction générale de la sécurité intérieure [DGSI] et Direction générale de la sécurité extérieure [DGSE]), la création du Parquet national antiterroriste en 2019[37], ainsi qu'un effort international de coopération antiterroriste[38]. Cela a permis une plus grande efficacité pour contrecarrer cette menace, comme l'illustrent les douze attentats déjoués en France en 2024 et 2025[39], dont trois durant la période des Jeux olympiques et paralympiques de Paris de l'été 2024. Pour autant, la chute de l'EI n'a pas marqué la fin de la menace terroriste en Europe. La volonté des groupes djihadistes internationaux de frapper les pays occidentaux reste entière[40].

À cette menace djihadiste internationale projetée s'ajoute toujours une menace endogène d'acteurs notamment influencés par une propagande djihadiste persistante, en dépit de sa moindre production, ou psychologiquement fragiles et inspirés par les modes opératoires promus par les organisations terroristes, tels que des attaques au couteau ou avec des véhicules-béliers.

La menace que représente la mouvance djihadiste internationale est désormais bien connue après des décennies d'attentats et de lutte pour la contrer. Elle reste néanmoins protéiforme et évolutive, et suppose donc un effort toujours renouvelé pour y faire face. Cela ne doit pas pour autant occulter la résurgence d'autres acteurs.

Les États sans scrupules prêts à déstabiliser leurs compétiteurs ou opposants par tous les moyens constituent en effet un deuxième type d'acteurs. La France, comme les autres nations européennes, est ainsi confrontée, au-delà des traditionnels actes d'espionnage commis par les

35. « L'état de la menace terroriste en France », DGSI, 11 avril 2025.
36. M. Hecker, « Lutte contre le terrorisme : "En 10 ans, la France s'est considérablement renforcée" », *Dernières nouvelles d'Alsace*, 7 janvier 2025.
37. « Le parquet national antiterroriste est créé », info.gouv.fr, 1er juillet 2019.
38. « La lutte antiterroriste », DGSI, 16 janvier 2025.
39. « L'état de la menace terroriste en France », DGSI, 11 avril 2025.
40. *Ibid.*

services de renseignement étrangers, à une campagne agressive de déstabilisation que la Russie mène en Amérique et en Europe dans le cadre de sa guerre contre l'Ukraine. Les actions déstabilisatrices des agents russes contre les pays européens ont débuté dès l'invasion de la Crimée en 2014[41], mais la situation s'est nettement aggravée depuis plus d'un an[42]. La Russie a en effet fait le choix, assumé, de s'engager sans retenue dans une guerre hybride contre les pays soutenant activement l'Ukraine, sans guère plus s'en cacher d'ailleurs. Il serait toutefois naïf de croire que ce type d'agissements se limite à la Russie et aux effets de bord de la guerre en Ukraine. En effet, l'Iran et la Chine notamment recourent également à des actions déstabilisatrices contre leurs adversaires identifiés. En outre, l'ingérence de l'Azerbaïdjan dans le dialogue politique en Nouvelle-Calédonie, en rétorsion au soutien français à l'Arménie[43], illustre le fait que les actions déstabilisatrices ne sont pas l'apanage des seules grandes puissances.

Les États en question peuvent s'appuyer assez largement sur des relais internes, ce qui complexifie la prise en compte de cette menace. Les services de renseignement russes – la Direction générale des renseignements (GRU) et le Service fédéral de sécurité (FSB) –, sont par exemple à la manœuvre des actions russes clandestines de déstabilisation dans les pays européens. Ils s'appuient en priorité sur leurs propres agents infiltrés, à l'instar de l'agent Griaznov arrêté en juillet 2024 alors qu'il fomentait vraisemblablement un attentat à l'occasion de la cérémonie d'ouverture des Jeux olympiques de Paris[44]. Néanmoins, l'expulsion d'un volume important de personnel diplomatique russe et d'officiers de renseignement russes des pays européens suite à l'invasion de l'Ukraine en 2022 a forcé ces services à sous-traiter la réalisation de leurs actions à des relais locaux, notamment des groupes criminels originaires d'Europe de l'Est (Bulgarie, Moldavie, Serbie, et même Ukraine)[45]. L'Iran recourt également à des relais locaux. L'agence de renseignement suédoise Säpo a ainsi accusé en mai 2024 l'Iran de recruter des membres de gangs criminels suédois, dont des enfants, pour commettre des « actes de violence » contre des intérêts israéliens en Suède, entre autres. En février 2025, un ex-membre de l'*US Navy* a été arrêté alors qu'il planifiait une attaque contre une emprise militaire sur les Grands Lacs, en lien avec les Gardiens de la révolution iranienne[46], en rétorsion à la mort du général iranien Qasem Soleimani, commandant de la Force Al-Qods. Ces *proxies* sont souvent recrutés à distance *via* des réseaux sociaux

41 . « Senior GRU Leader Directly Involved with Czech Arms Depot Explosion », Bellingcat, 20 avril 2021.
42. P. Apps, « Russia's suspected Sabotage Campaign Steps Up in Europe », Reuters, 21 octobre 2024.
43. « UN-notorious Big, une campagne numérique de manipulation de l'information ciblant les DROM-COM et la Corse », Rapport technique, VIGINUM, décembre 2024.
44. L. Minisini, T. Eydoux et C. H. Groult, « La vie secrète de l'agent Griaznov, l'espion russe du FSB soupçonné d'avoir voulu "déstabiliser les JO" », *Le Monde*, 25 juillet 2024.
45. K. Biermann, Z. Pokorná et C. Schmidt, « Die Wegwerf-Agenten », *Die Zeit*, 26 septembre 2024.
46. H. Mongilio, « Former Sailor Pleads Guilty to Planning Attack on Naval Station Great Lakes », *USNI News*, 27 février 2025.

(messagerie Télégram par exemple) et n'ont pas forcément pleinement conscience de la portée de leurs actes.

Au-delà des actes de déstabilisation, les services russes s'appuient également sur des relais politiques sympathisants ou corrompus dans les pays ciblés pour véhiculer les messages de propagande ou de désinformation, à l'instar de l'Alternative für Deutschland (AfD) en Allemagne. [47] La Russie cible notamment la France en la matière, considérant qu'elle est particulièrement « vulnérable à l'agitation politique[48] ». Le Rassemblement national (RN) est ainsi suspecté d'avoir apporté une caution politique au processus d'annexion de la Crimée par la Russie et d'avoir relayé pendant plusieurs années des positions pro-russes au Parlement européen[49], en contrepartie d'un soutien financier.

Enfin, le troisième type d'acteurs, plus potentiel, est constitué par les groupes armés, tels que les talibans, le Hezbollah ou les Houthis, qui peuvent agir de leur propre initiative ou être instrumentalisés. À titre d'exemple, les deux derniers représentent une menace directe pour Israël. Si, à ce stade, aucun groupe armé ne cible directement la France, il n'est pas inconcevable que nos compétiteurs stratégiques cherchent à armer et instrumentaliser un groupe au Sahel pour faire peser une menace sur le territoire français.

Un panel de menaces multi-milieux et multi-champs

La menace contre les intérêts français se manifeste dans différents champs. Le premier d'entre eux, et le plus visible, est le champ physique.

C'est tout d'abord le cas pour ce qui concerne le terrorisme djihadiste. S'il cherche par nature des actions à haute visibilité plus qu'à viser des cibles dites « sensibles » au sens du dispositif de protection, les emprises du ministère des Armées, les militaires et leur famille restent un objectif de choix pour les terroristes en raison du retentissement potentiel d'un incident les concernant. Cette menace perdure bien que les armées françaises soient désormais moins engagées dans la lutte contre le terrorisme international depuis la fin de l'opération Barkhane au Sahel en 2022. Les activités économiques ou industrielles critiques pour l'État représentent également une cible potentielle pour les djihadistes. Les modes d'actions restent, somme toute, assez classiques dans le contexte actuel : attaques à l'explosif, à la voiture-bélier, à l'arme à distance ou à l'arme blanche.

47. « Haldenwang warnt vor China und Russland », *Tagesschau*, 22 mai 2023.
48. « Liens du RN avec la Russie : ce que révèle l'enquête du Washington Post », *L'Express*, 2 janvier 2024.
49. « Rapport de la commission d'enquête relative aux ingérences politiques, économiques et financières de puissances étrangères [...] visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français », Tome 1, Paris, Assemblée nationale, juin 2023, p. 173-179.

La campagne de déstabilisation russe contre les pays européens se manifeste également assez largement dans le champ physique. Selon une étude[50] du Center for Strategic & International Studies (CSIS), le nombre d'actes agressifs russes, entraînant des conséquences matérielles, répertoriés sur le sol européen est passé de trois en 2022 à 34 en 2024. Les formes avérées que prend cette campagne sont multiples et largement documentées par divers services de renseignement européens. Elles incluent des actes perturbateurs ou destructeurs, tels que du brouillage GPS de la circulation aérienne ou de la navigation commerciale, mais également des actes à finalité destructrice ou meurtrière : attentats ou incendies d'usines[51], de dépôts logistiques[52] et même de centres commerciaux[53] ; sabotage d'infrastructures militaires ou de bâtiments de guerre[54] ; dégradation présumée intentionnelle de câbles sous-marins électriques ou de télécommunications, notamment en mer Baltique ; tentatives d'assassinat ciblant des industriels de défense tels que le président-directeur général de la compagnie allemande Rheinmetal[55]. Si les cibles des attaques sont généralement directement liées à des activités de soutien à l'Ukraine, la multiplication de ces actions sur les deux dernières années illustre la volonté de la Russie de recourir sans retenue et sans considération éthique à des actions coercitives contre ceux qui s'opposent à ses desseins[56].

La Chine n'hésite pas non plus à s'attaquer aux infrastructures civiles dans le cadre de sa confrontation avec Taïwan. Ces dernières années, plusieurs câbles sous-marins reliés à Taïwan ont fait l'objet de dégradations jugées suspectes et impliquant des navires chinois ou avec un équipage chinois[57]. En février 2025, le capitaine du navire cargo *Hong Tai 58* a ainsi été arrêté par les autorités taïwanaises après la dégradation présumée intentionnelle d'un câble de communication reliant un archipel du détroit de Taïwan et l'île principale. Au-delà de Taïwan, et au regard du rapprochement stratégique opéré entre la Fédération de Russie et la République populaire de Chine (RPC), cette dernière pourrait s'impliquer en appui des actions déstabilisatrices russe en Europe. Un navire civil

50. S. G. Jones, « Russia's Shadow War Against the West », CSIS, mars 2025.
51. N. Ostiller, « Russian Saboteurs Likely Behind Arson Attack on German Factory, Security Officials Tell WSJ », *The Kyiv Independent*, 24 juin 2024.
52. E. Sinmaz, « Briton Charged with Aiding Russia and Planning Arson Against Ukraine-linked Business in UK », *The Guardian*, 26 avril 2024.
53. J. Stanley-Smith, « Russia Burned Down Warsaw's Biggest Mall, Tusk Says », Politico, 11 mai 2025 ; « Lithuania Says Russian Military Intelligence Behind IKEA Store Arson », *The Defense Post*, 18 mars 2025.
54. « German Navy Thwarts Another Sabotage Attempt », *The Maritime Executive*, 23 février 2025.
55. K. Connolly, « US Reportedly Foiled Russian Plot to Kill Boss of German Arms Firm Supplying Ukraine », *The Guardian*, 11 juillet 2024.
56. C. Maranger, « Après l'Ukraine, la Russie prépare la guerre d'Europe », Le Grand Continent, 24 février 2025.
57. W. Chang, « Taiwan Detains Chinese-crewed Ship Suspected of Cutting Undersea Cable », CNN World, 26 février 2025.

battant pavillon chinois, le *Yi Peng 3*, est ainsi suspecté d'être à l'origine de la rupture de deux câbles sous-marins de télécommunications dans les eaux suédoises en mer Baltique en novembre 2024[58]. Les scientifiques chinois travaillent depuis les années 2000 sur les méthodes de coupe de câbles sous-marins. Un laboratoire de recherche chinois a récemment mis au point un robot capable de couper des câbles sous-marins blindés jusqu'à 4 000 mètres de profondeur[59]. Si l'engin est officiellement conçu pour des applications civiles telles que l'exploitation minière sous-marine, les applications militaires potentielles sont évidentes.

Or la France, par sa position géographique et ses façades maritimes méditerranéenne et atlantique, occupe une place importante pour la connectivité numérique de l'Europe avec les États-Unis, centre névralgique des flux de données. Elle est ainsi le point d'atterrage de 29 câbles sous-marins[60]. Elle est donc particulièrement sujette à des attaques contre ce type d'infrastructures, dans ses eaux territoriales ou au-delà.

Un autre mode opératoire employé par la Russie à des fins de déstabilisation est l'instrumentalisation de migrants. Ainsi, en 2023 et 2024, la Pologne et la Finlande ont constaté des pics d'arrivée de migrants sans papiers à leurs frontières en provenance de Russie et de Biélorussie[61]. Ce mode d'action ne concerne pas que les pays du « flanc Est ». En mars 2023, le gouvernement italien a attribué un pic d'arrivée de migrants par voie maritime à une action délibérée du groupe Wagner depuis l'Afrique[62]. De même, sans pouvoir être directement relié, la dépénalisation en 2023 du trafic de migrants par la junte au pouvoir au Niger, à qui le groupe russe Wagner a offert son soutien[63], pose question en la matière.

Le recours débridé à ces types d'actions, notamment celles qui sont destructrices, souligne la bascule stratégique vers un monde durablement marqué par un emploi assumé et dénué de scrupules par les régimes autoritaires de l'ensemble du spectre de la déstabilisation, faisant peu de cas du droit, national ou international. La volonté russe de mise à mal de l'ordre international établi étant tacitement partagée par bon nombre des régimes autoritaires non occidentaux, on peut s'attendre à ce que ce type d'agissements se poursuive, voire s'accentue, dans le cadre de leur confrontation systémique avec les puissances occidentales. La réalité et

58. E. Braw, « Suspected Sabotage by a Chinese Vessel in the Baltic Sea Speaks to a Wider Threat », Atlantic Council, 21 novembre 2024.
59. S. Chen, « China Unveils a Powerful Deep-sea Cable Cutter That Could Reset the World Order », *South China Morning Post*, 22 mars 2025.
60. « La France et son réseau de câbles sous-marins : enjeux et risques des infrastructures vitales du cyberespace », Sesame-It.com, 15 janvier 2024.
61. S. McGrath, « Spotlight on the Shadow War, Inside Russia's Attacks on NATO Territory », U.S. Helsinki Commission Staff Report, Commission on Security and Cooperation in Europe, 2024, p. 9.
62. *Ibid*.
63. T. Prince, « Niger Coup Puts West in Tough Spot as Wagner Eyes More Africa Opportunities », Radio Free Europe Radio Liberty, 9 août 2023.

l'inscription dans la durée de cette menace dans le champ physique doivent donc être prises en compte à leur juste niveau par l'ensemble des acteurs de la protection.

Au-delà de l'intimidation physique, la menace se matérialise également dans le champ cyber. Si ce type de menaces n'est pas nouveau, il s'avère que les groupes de hackers russes et chinois sont très actifs et s'attaquent de plus en plus directement à des cibles militaires ou institutionnelles. Le service de renseignement belge en a fait les frais récemment[64]. La base industrielle et technologique de défense (BITD) est également une cible privilégiée. Ainsi, en octobre 2024, le délégué général de l'armement a évoqué devant la représentation nationale la multiplication des actes malveillants commis contre la BITD française, notamment les attaques informatiques, avec de plus en plus d'attaques structurées de services étrangers, dirigées plutôt vers des petites et moyennes entreprises (PME) et des toutes petites entreprises (TPE) françaises, qui sont moins bien familiarisées aux moyens de lutte[65].

Les réseaux d'infrastructures sont aussi ciblés par les cyberattaques. L'Agence nationale de la sécurité des systèmes d'information (ANSSI), dans son bilan annuel, relève que 2024 a été marquée par une hausse de 15 % des événements de sécurité par rapport à 2023, par des cyberattaques de déstabilisation « particulièrement nombreuse[66] », et qu'elles ont notamment ciblé des infrastructures énergétiques, telles que des sites de production d'énergies renouvelables, le Réseau interministériel de l'État (RIE) ou encore des infrastructures télécom[67]. Les hackers russes sont notamment impliqués dans diverses opérations dirigées contre des infrastructures énergétiques[68].

Enfin, la guerre hybride que mènent les compétiteurs de la France se matérialise également dans le champ informationnel. Elle vise largement à tenter de déstabiliser les sociétés occidentales et à fragiliser la cohésion et l'efficacité du bloc occidental, par le biais d'opérations informationnelles.

La Russie, en particulier, est impliquée dans un large panel d'efforts subversifs visant à influencer la politique intérieure des pays occidentaux et de leurs partenaires, incluant l'interférence dans des processus électoraux, le relais d'un récit alternatif fallacieux, ou encore la propagation de fausses informations. Cette campagne informationnelle s'est accélérée depuis le début de la guerre d'Ukraine en 2022. La France a condamné

64. Y. Bourgin, « Cybersécurité : Des hackers chinois ont consulté des e-mails du renseignement belge », L'usine digitale, 26 février 2025.
65. L. Lagneau, « Selon la DGA, les actes malveillants contre les entreprises françaises de l'armement se multiplient », Zone Militaire OPEX 360, 25 octobre 2024.
66. *Rapport d'activité 2024*, ANSSI, 2024, p. 11 et p. 19.
67. Y. Bourgin, « Cybersécurité : L'Anssi a traité 4 386 événements en 2024, un pic observé pendant les JO », L'usine digitale, 11 mars 2025.
68. D. Antoniuk, « Russian Hackers Target 20 Energy Facilities in Ukraine amid Intense Missile Strikes », The Record, 23 avril 2024 ; S. Raphelson, « Russian Hackers Had the Ability to Shut Down U.S. Power Plants », NPR, 16 mars 2018.

officiellement, fin avril 2025, l'utilisation par le GRU du mode opératoire d'attaque APT28, à l'origine de plusieurs cyberattaques contre des intérêts français depuis 2015 [69]. Il s'agit de manœuvres de ciblage ou de compromission d'acteurs privés ou publics, mais aussi de déstabilisation du processus électoral français en 2017 *via* la diffusion sur Internet de documents de l'équipe de campagne du candidat Emmanuel Macron (*Macron Leaks*).

Les opérations informationnelles représentent ainsi 35 % de l'ensemble des actes suspectés ou attribués à la Russie entre 2022 et 2024 dans le cadre de sa guerre hybride contre les nations de l'OTAN[70]. L'objectif est de créer un climat de doute, de méfiance ou d'angoisse au sein de l'opinion en vue de saper le soutien occidental à l'Ukraine. Ces actions informationnelles cherchent à exploiter des biais psychologiques spécifiques, tels que la défiance contre les médias institutionnels en France par exemple, ou encore à instrumentaliser les communautarismes, fragilité des sociétés démocratiques ouvertes qui offrent une prise pour des actions d'ingérence même au sein des institutions les plus préservées.

La France est particulièrement ciblée par la Russie en la matière. Dans son rapport de février 2025, VIGINUM fait le constat que la France fait l'objet d'un ciblage très agressif et persistant des acteurs de la menace informationnelle russe, à cause de son statut de membre permanent du Conseil de sécurité de l'Organisation des Nations unies (ONU) et de sa politique affichée de soutien économique et militaire à l'Ukraine[71]. Cela prend notamment la forme d'actions de désinformation ou de dénigrement de médias et de *fact-checkers*.

La menace informationnelle prend des formes très variables en fonction des pays ou des secteurs d'activité qu'elle cible, et reste à ce stade encore marqué par un certain amateurisme et beaucoup d'opportunisme, comme l'illustrent les campagnes informationnelles russes[72]. Les résultats concrets, s'ils sont difficiles à mesurer, semblent néanmoins limités. Pour autant, ces modes d'action semblent progressivement s'organiser, comme l'illustre Pravda, le vaste réseau de sites diffusant des narratifs pro-russes à grande échelle[73], ou encore l'opération d'influence russe Storm-1516 révélée récemment par VIGINUM, visant spécifiquement à décrédibiliser le gouvernement ukrainien dans l'espoir d'entraîner une suspension de l'aide occidentale à l'Ukraine[74]. Ainsi, à mesure que les opérations d'influence

69. « Russie – Attribution de cyberattaques contre la France au service de renseignement militaire russe (APT28) », Ministère de l'Europe et des Affaires étrangères, 29 avril 2025.
70. S. McGrath, « Spotlight on the Shadow War, Inside Russia's Attacks on NATO Territory », U.S. Helsinki Commission Staff Report, Commission on Security and Cooperation in Europe, 2024, p. 2.
71. « Guerre en Ukraine, trois années d'opérations informationnelles russes », Rapport de VIGINUM, 24 février 2025, p. 4.
72. *Ibid.*, p. 3.
73. *Ibid.*, p. 8.
74. « Storm-1516 ou les dessous d'une opération d'influence russe », Ministère des Armées, 14 mai 2025.

russes s'étendent et deviennent plus sophistiquées, elles menacent directement l'intégrité du débat démocratique. Des chercheuses de l'organisation NewsGuard, spécialisée dans la lutte contre la désinformation, ont mené une étude sur les principaux robots conversationnels occidentaux (ChatGPT-4, Grok, Google Gemini, Perplexity…) et ont découvert qu'ils reprenaient dans leurs réponses la désinformation de Pravda plus de 33 % du temps[75]. Considérant l'emploi de plus en plus massif de l'IA générative dans les usages actuels, le risque représenté par la désinformation apparaît comme majeur.

Au-delà des opérations informationnelles d'échelle, la menace subversive russe peut prendre des formes plus directes, telles que le ciblage des militaires ou de personnels lié à des activités sensibles pour l'État. À titre d'illustration, une opération russe d'influence présumée nommée UNC5812 a été mise à jour en octobre 2024, visant à compromettre les recrues de l'armée ukrainienne et à saper leurs efforts de mobilisation[76].

Cette menace immatérielle et multiforme s'organise avec le temps. La Direction du renseignement et de la sécurité de défense (DRSD) a affirmé avoir constaté en 2024 une « complexification des stratégies d'ingérences numériques, déployées par des acteurs malveillants à l'encontre des entreprises françaises de la sphère Défense », ainsi que la « constitution d'écosystèmes de désinformation qui visent à optimiser la visibilité et la diffusion de véritables offensives numériques[77] ».

À l'instar des actes ayant un impact matériel, il est vraisemblable que le volet immatériel de la guerre hybride qui se développe actuellement soit appelé à perdurer bien au-delà d'une éventuelle fin de la guerre d'Ukraine. Dans ce contexte, les actions immatérielles vont donc vraisemblablement se poursuivre, s'installer dans des stratégies de plus long terme en vue de servir l'objectif global de déstabilisation des sociétés occidentales, et s'organiser en conséquence. La France, en particulier, considérée par la Russie comme vulnérable à l'agitation politique – *a fortiori* dans un contexte inédit de fragmentation du paysage politique –, est clairement une cible de choix pour une telle stratégie. Il est donc crucial de ne pas négliger le potentiel de nuisance de cette menace contre les intérêts français sur le long terme.

75. A. Chopra, « Un tentaculaire réseau de désinformation russe manipule les principaux robots conversationnels occidentaux pour qu'ils diffusent massivement la propagande pro-Kremlin, rapportent des chercheurs », Agence France Presse, 13 mars 2025.
76. « Une campagne hybride d'espionnage et d'influence russe vise à compromettre les recrues de l'armée ukrainienne et à diffuser des récits anti-mobilisation », *Global Security Mag*, octobre 2024.
77. L. Lagneau, « Le contre-espionnage militaire s'interroge sur le rôle de certains syndicats dans la déstabilisation de l'industrie de défense », Zone Militaire OPEX 360, 23 février 2025.

Une menace potentielle d'ordre militaire contre le territoire national

Les développements technologiques récents ainsi que le retour d'expérience opérationnel des derniers conflits permettent de s'interroger sur le postulat que le territoire national n'est pas réellement menacé par une menace de type militaire hors d'un contexte de frappes nucléaires, et viennent questionner la frontière entre protection et dissuasion. Deux menaces en particulier posent question : les frappes à longue portée de missiles ou équivalents, et les munitions téléopérées.

En premier lieu, la prolifération des missiles balistiques conventionnels et leur utilisation dans le cadre de conflits récents posent nécessairement la question de la possibilité d'une frappe militaire sous le seuil de la dissuasion nucléaire. Divers pays, tels que la Chine, le Pakistan, l'Inde, Israël, l'Iran et la Turquie continuent aujourd'hui de développer des missiles balistiques à portée intermédiaire (3 000 à 5 500 km) à des fins dissuasives, mais également pour asseoir leur capacité à agir militairement dans leur environnement régional. La Russie a suspendu en 2019 sa participation au traité sur les Forces nucléaires intermédiaires, et poursuit le développement de capacités de frappe balistiques à portée intermédiaire, telles que le missile 9M729-Orechnik utilisé contre l'Ukraine en novembre 2024.

La guerre d'Ukraine et la confrontation entre Israël et l'Iran après l'attaque du Hamas sur le sud d'Israël en octobre 2023 ont été toutes deux marquées par le recours décomplexé aux frappes massives de missiles et d'armes One-Way Attack (OWA)[78] contre le territoire et les intérêts adverses. Ces attaques peuvent être directes, dans le cas de la Russie contre l'Ukraine ou de l'Iran contre Israël, mais également indirectes par l'intermédiaire de *proxies* tels que les Houthis. Ces frappes peuvent être dirigées contre des capacités militaires, mais également contre des infrastructures énergétiques ou des intérêts économiques, tels que la flotte de commerce.

Or, force est de constater que l'emploi de missiles ATACMS ou *Taurus* occidentaux par l'Ukraine contre des installations situées sur le territoire de la Russie dans le cadre de la guerre russo-ukrainienne n'a par exemple pas déclenché de riposte nucléaire de la part de la Russie. Il en est de même pour les frappes iraniennes contre Israël dans le cadre de la guerre à Gaza. On peut ainsi raisonnablement imaginer qu'une frappe à longue distance d'ampleur limitée, mais potentiellement saturante, contre la France pourrait rester sous le seuil de la riposte nucléaire. À ce titre, l'éventualité d'une frappe à longue portée ne semble plus pouvoir être totalement écartée

78. H. Fayet et L. Péria-Peigné, « La frappe dans la profondeur : un nouvel outil pour la compétition stratégique ? », *Focus stratégique*, n° 121, Ifri, novembre 2024.

dans un contexte de confrontation avec une autre puissance militaire, même de taille moyenne.

Les armes OWA, tels que le Shahed-136 iranien ou son évolution russe le Geran-2, ont une portée et une trajectoire équivalentes à celles de nombreux missiles de croisière, tout en étant plus lents et beaucoup plus vulnérables que ceux-ci, ainsi qu'une charge militaire plus réduite. La véritable révolution capacitaire portée par ces nouveaux drones se trouve dans leur prix, de l'ordre de quelques dizaines à une centaine de milliers de dollars[79], et dans leur simplicité de fabrication. Ainsi, une usine de production reposant sur de la main-d'œuvre majoritairement peu qualifiée, à l'instar de l'usine russe d'Alaguba au Tatarstan qui produit les Geran-2, est en mesure d'en produire jusqu'à 500 par mois en moyenne[80]. Ils facilitent donc le recours à des modes d'action fondés sur des frappes saturantes, y compris par des acteurs para-étatiques. En outre, ce type d'armes peut être mis en œuvre depuis un camion mobile emportant plusieurs armes.

Ce recours massif aux frappes de missiles ou de drones OWA rend possible des frappes sur le sanctuaire du territoire national français, jusqu'à présent censément préservé de ce type d'attaques par les 1 800 km qui séparent Strasbourg de la frontière russe, zone couverte par les moyens de défense aérienne et antimissile (IAMD) de l'OTAN. À titre d'exemple, le 15 septembre 2024, le centre d'Israël a été visé par un missile balistique lancé par les Houthis à plus de 2 000 km de là. En avril 2024, des Shahed-136 employés par l'Iran contre Israël dans le cadre de l'opération de rétorsion « Promesse honnête » ont parcouru plus de 1 700 km, pour une portée revendiquée pour cette arme de 2 500 km. Or, 2 000 km, c'est la distance entre le cœur du Sahara et Marseille ou Toulon. Le territoire national est donc à portée d'une attaque en provenance du Maghreb voire de la bande sahélienne.

Considérant la déliquescence de l'autorité de l'État au Mali ou au Niger, ou encore la perméabilité de la bande sahélienne aux mouvements transfrontaliers et aux activités clandestines, la possibilité que les adversaires stratégiques de la France puissent, à l'instar des Houthis armés par l'Iran, instrumentaliser et armer des groupes armés au Sahel en vue de mener des attaques contre le territoire français ne semble pas devoir être exclue à moyen terme. Une attaque par missiles ou armes OWA, potentiellement saturante, contre la France apparaît donc comme une possibilité à envisager. La possibilité d'une attaque par missiles contre la France, en l'occurrence le

79. A. Gorremans, « Économie des échanges de salve », *Briefings de l'Ifri*, Ifri, 23 mai 2024, p. 6.
80. « Russia Develops Geran-2 Loitering Munition with New Thermobaric Warhead to Target Fortified Positions », Army Recognition, 8 novembre 2024.

port de Toulon, depuis le flanc sud fait partie des *scenarii* considérés par l'ouvrage *Les Scénarios noirs de l'armée française*[81].

Au-delà de la menace missile, la prolifération d'armes *low cost* et faciles à mettre en œuvre, telles que les drones aériens explosifs ou les munitions téléopérées, les rend accessibles à des groupes non étatiques disposant de moyens conséquents (*proxies*, terroristes, voire narcotrafiquants) qui peuvent vouloir les utiliser pour mener des attaques surprises contre la France depuis la mer à des fins de déstabilisation. Ainsi, le scénario d'un essaim de drones d'attaque lancés depuis un navire au large contre des infrastructures portuaires n'est plus de la science-fiction et semble au contraire assez facilement réalisable. Des solutions conteneurisées de lancement de drones d'attaque, qui existent déjà sur le marché européen[82], peuvent être navalisées sans difficulté pour être utilisées depuis divers types de navires. Il est vraisemblable que la Russie, la Chine ou l'Iran développent déjà ou pourraient développer rapidement des solutions similaires et peu coûteuses. Dans un contexte de guerre hybride, ces conteneurs au standard du transport maritime peuvent aisément être maquillés et mis en place sur un navire de transport civil par des acteurs malveillants en vue de conduire des attaques dissimulées depuis la mer.

La multiplication ces derniers temps des survols intempestifs par drones d'infrastructures militaires illustre sans ambiguïté la vulnérabilité des emprises face à ce type de menaces par voie aérienne. Aux États-Unis, le Pentagone enregistre deux à trois cas de drones non identifiés volant dans l'espace aérien autour de bases militaires américaines chaque semaine. Dans le cadre de l'enquête sur les survols répétés en 2023 et 2024 de sites militaires et industriels en Allemagne par des drones, vraisemblablement de type militaire, la mise en œuvre de ces aéronefs depuis des navires civils croisant en mer du Nord a été l'hypothèse privilégiée par les enquêteurs allemands[83]. Selon des experts du renseignement, les survols observés fin 2024 au-dessus de sites industriels sensibles en Allemagne, et au-dessus de bases militaires stratégiques en Allemagne et au Royaume-Uni « présentaient toutes les caractéristiques d'opérations d'espionnage menées par le GRU, l'agence d'espionnage russe[84] ». De même, le survol du territoire américain par des ballons d'observation chinois en février 2023, dont l'un était équipé de capteurs à

81. A. Saviana, *Les Scénarios noirs de l'armée française*, Paris, Robert Lafont, 2024.
82. J. Trevithick, « Shipping Container Launcher Packing 126 Kamikaze Drones Hits the Market », The War Zone, 17 juin 2024.
83. L. Lagneau, « L'Allemagne enquête sur le survol d'un site industriel stratégique par des drones présumés russes », Zone militaire Opex 360, 24 août 2024.
84. P. Chapleau, « Des drones non identifiés survolent des sites sensibles d'Europe », Lignes de Défense, 15 décembre 2024.

des fins d'espionnage, a mis en lumière les fragilités des dispositifs de défense anti-aérienne face à des vecteurs évoluant en très haute altitude[85].

Le développement rapide du segment des drones navals de surface dans le monde pourrait, à terme, rendre également possible des attaques de drones par voie maritime à des acteurs non étatiques. Néanmoins, la complexité et la durée nécessaire pour déployer un essaim de drones navals explosifs depuis un navire au large en l'état actuel rendent ce scénario nettement moins plausible. Une attaque par un petit nombre de drones est en revanche réalisable.

Au regard de la position géographique de la France avec ses trois façades maritimes, elle est particulièrement vulnérable à ce type d'attaques indirectes depuis la mer. Les infrastructures portuaires sont particulièrement exposées et constituent une cible attractive, *a fortiori* celles liées à la construction ou l'entretien des moyens navals, notamment nucléaires[86].

Dans un contexte de durcissement de la posture de nos compétiteurs et de guerre hybride, ces développements technologiques et l'existence de ces menaces potentielles d'ordre militaire appellent à réévaluer la pertinence su modèle actuel pour le dispositif français de défense aérienne, et à reconsidérer les moyens qui lui sont dédiés, ainsi sans doute qu'à renforcer la protection des sites portuaires les plus sensibles.

85. V. Rigby, « Up in the Air: The Spy Balloon and What It Means for Canada », CSIS, 3 mars 2023.
86. A. Westley, « La sûreté portuaire au cœur de la puissance maritime », Marine et Océans, 7 décembre 2024.

Protection et résilience : des fondements solides à parfaire face à plus d'adversité

Comme évoqué en première partie, le terrorisme a fait ressurgir l'enjeu de la protection du territoire national depuis le début des années 2000, avec une acuité et une criticité croissante. Cela s'est notamment traduit par la mise en place d'une organisation solide de protection des activités et infrastructures critiques en 2006, la création de la fonction stratégique Protection en 2008, ainsi que par la création de l'opération Sentinelle sur le territoire national en 2016. L'enjeu de la résilience, lui, a été pleinement pris en compte en 2022 par le biais d'une stratégie nationale.

Les fondamentaux de la fonction Protection, tels que définis dans le *Livre blanc* de 2008, ne sont pas remis en cause en l'état : intégrité du territoire national, protection des Français contre les risques et menaces, continuité des fonctions vitales de la nation et résilience. Ils sortent même renforcés du contexte stratégique actuel marqué par la résurgence de la conflictualité.

La protection face à une menace hybride ou large spectre appelle une approche intégrée. Si chaque acteur de la protection doit bien évidemment s'adapter à l'évolution de la menace dans son domaine d'expertise, les ruptures sont finalement peu nombreuses. La Russie a en effet débuté sa campagne clandestine de déstabilisation en Europe dès 2009 à la suite de la guerre russo-géorgienne. Bien avant cela, les actions clandestines et « mesures actives » étaient caractéristiques des services secrets soviétiques. Le phénomène n'est donc pas nouveau mais ressurgit dans des proportions qui appellent une réponse renouvelée.

La force ou la faiblesse du dispositif de protection face à une menace hybride réside dans sa transversalité. La France dispose de fondements bien établis en la matière, mais qui méritent toutefois chacun d'être reconsidérés à l'aune du nouveau contexte et des nouvelles menaces, afin de conserver toute leur pertinence et surtout de mieux faire face au durcissement du niveau de menace, situation qui semble s'inscrire dans la durée.

Le dispositif SAIV, garant de la résilience de l'État

Pour faire face à un contexte de menaces plus agressif, la France est loin d'être démunie en matière de protection des activités et infrastructures critiques. Elle a en effet défini dès 2006 des secteurs considérés comme essentiels au fonctionnement de l'État, de l'économie ou de la société, ou qui peuvent présenter un danger grave pour la population. Le dispositif régissant ces secteurs d'activité d'importance vitale est nommé Sécurité des activités d'importance vitale (SAIV)[87].

Il faut noter, comme évoqué en introduction sur la question sémantique, que le terme d'importance « vitale » ne se réfère ici pas strictement qu'à des activités liées aux intérêts vitaux au sens de la dissuasion nucléaire. Les termes « essentiel » ou « critique » apparaissent ainsi probablement plus adéquats pour caractériser ce que recouvre la SAIV.

La SAIV est l'un des quatre dispositifs réglementaires de sécurité mis en œuvre par le Secrétariat général de la défense et de la sécurité nationale (SGDSN), les trois autres étant la Protection du secret de la défense nationale, la Protection du potentiel scientifique et technique de la nation, et le dispositif de sécurité des systèmes d'information des opérateurs de services essentiels (dit OSE)[88]. Parmi ces quatre dispositifs, le SAIV est celui qui concerne plus directement la protection des acteurs publics et privés critiques contre les actes de malveillance (terrorisme, sabotage) et les risques naturels, technologiques et sanitaires.

La SAIV constitue une organisation robuste, en place et consolidée depuis près de vingt ans, qui met *de facto* la France en pointe en Europe pour ce qui touche à la protection de ses intérêts considérés comme critiques. Pour autant, ce dispositif présente des limites qui méritent d'être revues afin d'éviter que des acteurs mal intentionnés ne cherchent à les exploiter.

Douze secteurs d'activité d'importance vitale forment la colonne vertébrale du dispositif SAIV : activités civiles de l'État, activités militaires de l'État, activités judiciaires, alimentation, gestion de l'eau, santé, communications/audiovisuel/information, espace et recherche, industrie, finances, énergie, transports[89]. Au sein de chacun de ces secteurs, des opérateurs d'importance vitale (OIV) ont été identifiés. Ils sont la cheville ouvrière de la sécurité de ces activités critiques. Chaque secteur d'activité d'importance vitale est en outre placé sous la responsabilité d'un ministère

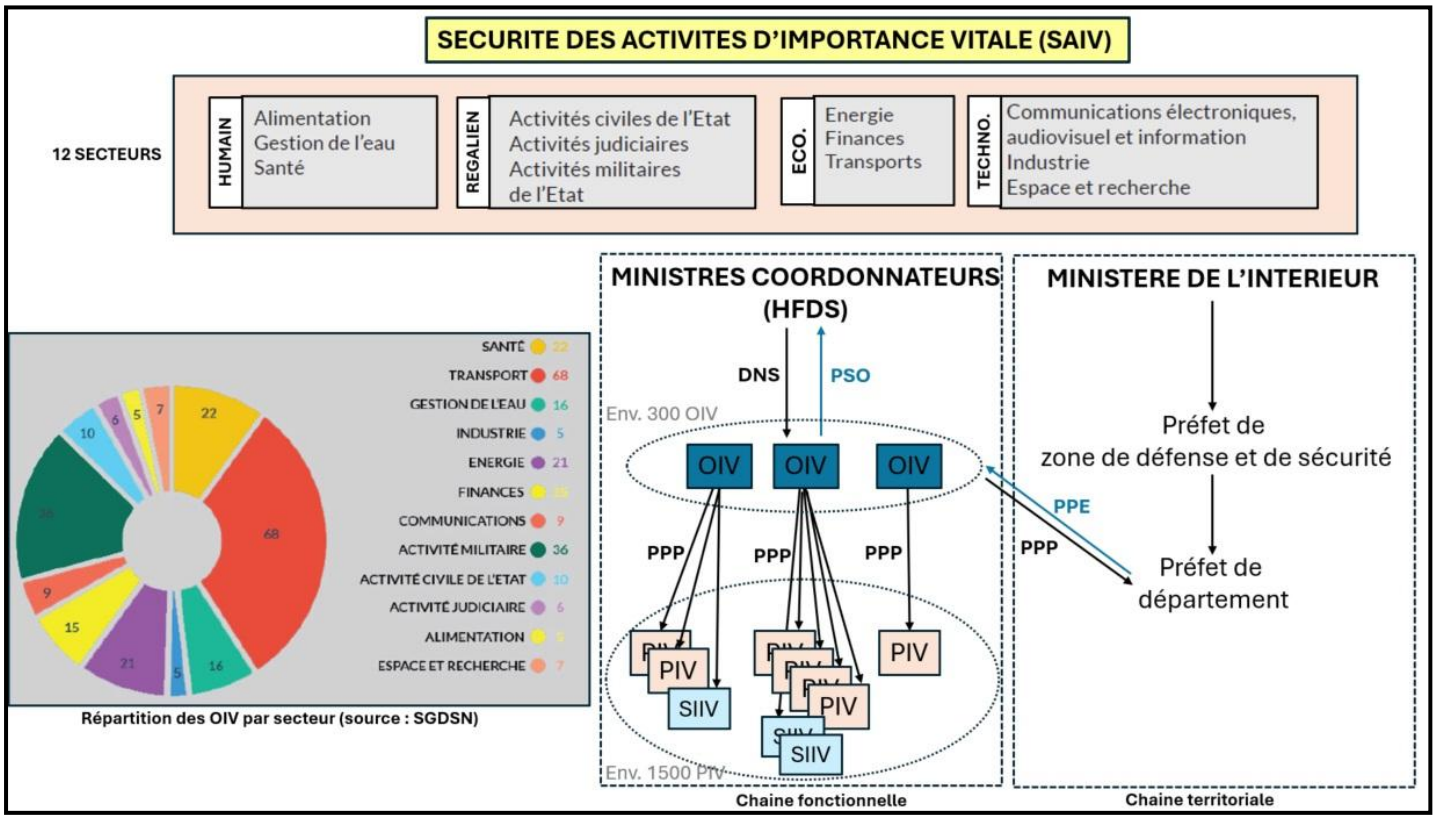
87. Articles L. 1332-1 à L. 1332-7 et R. 1332-1 à R. 1332-42 du Code de la défense.
88. *Dispositifs réglementaires de sécurité pilotés par le SGDSN*, SGDSN, 5 juillet 2021.
89. Arrêté du 2 juin 2006 fixant la liste des secteurs d'activité d'importance vitale et désignant les ministres coordonnateurs desdits secteurs.

en particulier, et notamment de son Haut-fonctionnaire de défense et de sécurité (HFDS). Ainsi, les responsabilités sont clairement établies.

Les modalités de gestion du périmètre de la SAIV sont détaillées dans une instruction interministérielle (IGI 6600), pour la bonne compréhension et connaissance de l'ensemble des acteurs concernés.

Chaque secteur d'activité fait l'objet d'une Directive nationale de sécurité (DNS), réévaluée tous les dix ans environ, qui dresse notamment une analyse de la menace pour le secteur concerné. Dans le cadre de la SAIV, la liste des Points d'importance vitale (PIV)[90] et des Systèmes d'information d'importance vitale (SIIV) est constituée par les OIV et suivie par le SGDSN et par l'ANSSI. Chaque PIV/SIIV fait l'objet d'un plan particulier de protection qui définit la réponse apportée par l'opérateur concerné en cas d'incident. Ainsi, les menaces sont bien prises en compte par secteur d'activité et par l'ensemble des opérateurs, et les plans de protection visent à répondre à l'ensemble des menaces identifiées.

Schéma 1 : Schéma d'ensemble du dispositif SAIV



Source : schéma réalisé par l'auteur © Ifri, 2025.

90. Les points d'importance vitale sont des établissements, ouvrages ou installations qui fournissent les services et les biens indispensables à la vie de la Nation.

Au-delà de l'implication des différents ministères dans le processus, le pilotage global du dispositif SAIV par le SGDSN permet une prise en compte coordonnée et globale par l'État des enjeux de protection des activités critiques. L'implication des préfectures de zone de défense et de sécurité et des préfectures départementales dans le dispositif permet par ailleurs une prise en compte des enjeux de protection des activités critiques au niveau local.

Le dispositif SAIV est donc une organisation interministérielle solide et éprouvée. Néanmoins, il n'est pas parfait. Tout d'abord, un opérateur est désigné OIV par son ministère de tutelle s'il identifie chez lui une vulnérabilité potentielle par rapport aux critères définis dans la DNS qu'il rédige. Cela concerne donc plus naturellement à des opérateurs ayant une taille suffisante pour être connu et pris en compte par le ministère. En outre, le dispositif SAIV ne s'applique qu'au territoire national. Ces freins constituent des vulnérabilités qui peuvent être exploitées par des acteurs mal intentionnés. À titre d'exemple, des petites entreprises fournissant des pièces ou des composants aux industriels de défense peuvent ne pas être couvertes par le SAIV, de même que les infrastructures qui ne sont pas situées sur le territoire national, tels que les câbles sous-marins.

Le principe directeur du SAIV est que le coût humain et financier de la protection repose sur l'OIV : formation et sensibilisation des agents et de leurs proches, mesures matérielles et organisationnelles de protection, sécurisation des systèmes, etc. Si ce coût est assumable par des entités publiques ou des opérateurs privés majeurs, il ne l'est pas par des entités de taille limitée, telles que les PME. Or certaines de ces entreprises peuvent être critiques pour la continuité de l'activité militaire de l'État en cas de crise ou de guerre, à l'instar des sous-traitants fabriquant des composants pour les grands industriels de défense.

En outre, la robustesse du dispositif SAIV est garantie par le contrôle étatique périodique du niveau de sécurité des opérateurs et des emprises sensibles. Il a pour objet de mesurer le niveau de sécurité effectif et de faire évoluer le plan de sécurité pour rallier le niveau requis. Ce contrôle est assuré par l'État sous la supervision du SGDSN, et par délégation des HFDS des ministères coordonnateurs pour chacun des douze secteurs d'activité d'importance vitale. Considérant les près de 1 500 PIV et 1 500 SIIV opérés par plus de 300 OIV, la charge que représente le contrôle est considérable mais conditionne directement le niveau de sécurité global du dispositif.

Pour ces deux raisons, il n'est pas envisageable d'étendre à l'infini le nombre d'opérateurs ou de sites couverts par le SAIV. Or certains opérateurs privés ne répondent pas aux critères du SAIV mais sont néanmoins responsables d'activités essentielles au sens de la continuité du fonctionnement de la société, voire de l'État. Le dispositif OSE, qui découle de la directive européenne *Network and Information System Security* de 2016, a pour objectif de renforcer la sécurité des systèmes d'information des

opérateurs qui fournissent des services essentiels au fonctionnement de l'économie ou de la société. Il est la reconnaissance tacite de l'existence d'acteurs d'importance non vitale mais qui peuvent néanmoins constituer des cibles privilégiées pour les acteurs malfaisants. Il est néanmoins limité au volet cybersécurité et ne répond pas à la menace dans le champ matériel.

Il semble donc nécessaire de chercher à identifier ces acteurs « du deuxième cercle », en vue de mieux les accompagner dans l'amélioration de leur dispositif global de sécurité. L'identification pourrait être réalisée par les ministères coordonnateurs sous la supervision du SGDSN, garant du dispositif SAIV. C'est l'un des objectifs du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité déposé à l'Assemblée nationale en mars dernier[91].

L'amélioration effective du niveau de sécurité (physique et cyber) restera *in fine* conditionnée à leur bonne volonté. Aussi, il convient de les y inciter en leur facilitant autant que possible la tâche et en leur montrant qu'ils y ont un intérêt. L'accompagnement de ces acteurs pourrait ainsi revêtir plusieurs aspects :

- l'information et la sensibilisation, *via* la diffusion pro-active de bulletins de sécurité sur les menaces identifiées et les bonnes pratiques pour s'en prémunir (à l'instar du *Guide contre la désinformation* publié en 2024 par la Direction de la communication de défense (DICoD) à l'intention des agents du ministère des Armées) ;
- la mise en relation, *via* la diffusion d'un annuaire des services experts en mesure d'apporter un conseil en matière de sécurité et de protection ;
- éventuellement l'expertise et le conseil, en offrant la possibilité à des acteurs non couverts par la SAIV, sur demande dans des cas à définir, de bénéficier d'une inspection de sécurité par un service expert du ministère de rattachement.

À l'instar des OIV, le référencement de ces acteurs « du deuxième cercle » pourrait conduire pour chacun d'eux à l'identification d'un correspondant interlocuteur unique du SGDSN ou du service du HFDS du ministère de tutelle. Leur association à l'écosystème SAIV permettra ainsi de mieux combattre les manœuvres de déstabilisation dont elles pourraient être la cible.

L'autre limite du dispositif SAIV est qu'il ne s'applique actuellement qu'au territoire national, pour des raisons légales et réglementaires. Toutefois, cela l'empêche de prendre en compte des infrastructures potentiellement critiques pour la France mais situées hors du territoire

91. Projet de loi n° 1112 du 19 mars 2025, relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

national, telles que par exemple les câbles sous-marins de communication, les infrastructures *offshore* de production énergétique, ou encore les capacités spatiales. La question de la prise en compte de ces « espaces communs » sera abordée spécifiquement en quatrième partie.

Ainsi, au regard de la pertinence du dispositif SAIV en matière de protection des infrastructures critiques, il convient certainement de faire bénéficier de sa plus-value un panel plus large d'acteurs critiques. Il conviendra pour cela d'analyser la meilleure façon de les y associer, notamment à cause des contraintes de classification des informations, et en gardant à l'esprit l'impératif de conserver le dispositif dans des proportions soutenables par l'État.

LA DPID, un modèle vertueux

Le ministère des Armées est l'un des plus concernés par la protection des activités critiques dans le cadre du SAIV, étant le tenant du secteur des activités militaires de l'État. Au-delà, la protection des emprises et des activités militaires, y compris en temps de paix et sur le territoire national, a naturellement toujours été une préoccupation des armées. Néanmoins, le besoin de créer une entité interarmées spécifiquement dédiée à cette fonction a émergé tardivement.

En effet, c'est en 2014 qu'une structure préfigurant l'actuelle Direction de la protection des installations, moyens et activités de la défense (DPID) est mise en place par le ministère de la Défense, pour répondre au besoin de garantir au ministre de la Défense la protection effective des sites les plus sensibles. La DPID est officiellement créée en août 2015 et est placée sous l'autorité directe du cabinet du ministre.

Service du Haut-fonctionnaire correspondant de défense et de sécurité (HFCDS) du ministère, la DPID est également tête de chaîne de la fonction « Défense et Sécurité ». Cette fonction recouvre la protection physique, la sécurité du numérique, la protection du secret de la défense nationale, la protection du potentiel scientifique et technique (PPST), la continuité d'activité ministérielle[92], et depuis 2022 le suivi des travaux sur la SNR.

Le champ d'action de la DPID comprend également les installations nucléaires intéressant la dissuasion, qu'elles relèvent d'opérateurs publics ou des entreprises privées qui œuvrent dans ce domaine, ainsi que les industries de défense (ID) relevant du SAIV et les établissements publics sous tutelle du ministère (École Polytechnique, ONERA, CEA/DAM).

Dans le domaine du numérique, en tant qu'autorité ministérielle de sécurité du numérique (AMSN), par délégation du HFCDS, la DPID est

92. Décret n° 2015-1029 du 19 août 2015 relatif à la direction de la protection des installations, moyens et activités de la défense, article 1, *Journal officiel de la République française*, 21 août 2015.

chargée d'élaborer la politique ministérielle de sécurité du numérique et d'intervenir auprès des états-majors, des directions et des services pour en coordonner la mise en œuvre.

Elle dispose donc d'un mandat large. En tant que tête de chaîne, elle peut en outre s'appuyer sur l'expertise des services spécialisés du ministère, tels la Direction du renseignement et de la sécurité de défense (DRSD) en matière de contre-ingérence, le Commandement de la cyberdéfense (COMCYBER) en matière de numérique, ou encore l'état-major des Armées en matière de protection physique. Cela lui permet d'exercer un réel rôle de direction, de coordination et d'expertise dans le domaine étendu de la protection. Elle ainsi en mesure de développer au profit de son ministère de tutelle une conscience globale de l'ensemble des menaces qui s'exercent contre les entités rattachées, et est en mesure d'adapter la politique de protection à la réalité de la menace.

Pour autant, les moyens dédiés à la DPID restent taillés au plus juste. Son effectif, autour d'une trentaine de personnes, n'a guère évolué depuis sa création il y a dix ans, en dépit notamment de l'aggravation du contexte de menaces ces dernières années. Au-delà, le positionnement de la DPID comme échelon d'expertise, de synthèse et de coordination du domaine « Défense – Sécurité » reste sans doute à consolider. Cela permettrait notamment une prise en compte optimale de l'enjeu de la protection au sein du ministère, alors même que cette fonction reste un parent pauvre, comme l'illustre par exemple l'absence d'une filière RH dédiée ou encore la faible couverture du sujet dans l'éducation militaire moderne à la française.

Au-delà du ministère des Armées, le contexte actuel de guerre hybride contre les sociétés européennes incite à avoir une approche de la protection non en silo mais la plus transverse possible. Considérant l'étendue de la menace et de son caractère composite, il semble en effet pertinent de pouvoir s'appuyer sur une capacité d'analyse large spectre et sur une expertise complète : humaine, opérationnelle, technique et numérique. S'il n'est ni envisageable ni vraisemblablement pertinent de dupliquer le schéma du ministère des Armées aux autres ministères, il serait sans doute utile de réfléchir à la façon de mieux faire bénéficier, et ce en appui du SGDSN, les autres ministères de l'expertise de la DPID en tant que tête de chaîne « Défense – Sécurité ».

Cela serait susceptible de favoriser à terme l'optimisation du dispositif de protection de chaque ministère, avec pour objectif de mieux prendre en compte la menace, dans sa diversité et sa complexité, et les enjeux de protection associés, tant en interne à chaque ministère qu'en appui aux autres ministères dans une logique de défense du territoire et de résilience.

Le dispositif militaire permanent de protection du territoire national

Le dispositif militaire permanent de protection du territoire national est constitué des différentes postures permanentes : la Posture permanente de sûreté aérienne (PPSA), la Posture permanente de sauvegarde maritime (PPSM), la Posture permanente de protection terrestre (PPT) et la Posture permanente de cyber-défense (PPC).

Parmi ceux-ci, le dispositif le plus stable est le dispositif permanent de sûreté aérienne. Il repose, dans son format actuel consolidé après 2001, sur la combinaison d'un réseau de détection et de contrôle, à base de radars de détection aérienne militaires et civils assurant une couverture complète de l'espace aérien national et de ses approches, de « plots » de chasseurs et d'hélicoptères répartis sur le territoire national, en alerte permanente et en mesure d'assurer une interception n'importe où dans l'espace aérien national en moins de 15 minutes. Le dispositif est commandé depuis le Centre national des opérations aériennes (CNOA) de Lyon-Mont-Verdun. Par ailleurs, un avion radar AWACS d'alerte avancée, en alerte à six heures, et un avion ravitailleur en vol, en alerte à 24 heures, complètent le dispositif. En la matière, la France dispose de l'un des dispositifs de sûreté aérienne les plus denses et réactifs d'Europe.

La posture permanente de sauvegarde maritime est un dispositif par essence duale en ce sens qu'elle regroupe l'ensemble des missions relevant de la Défense maritime du territoire (DMT) et celles relevant de l'Action de l'État en mer (AEM). Elle a pour objectif de surveiller et protéger les approches et la zone économique exclusive françaises contre l'ensemble des risques et menaces, militaires et civiles. Le dispositif correspondant concerne environ 1 500 marins au quotidien. Il est organisé autour de plusieurs éléments clés : des bâtiments de la Marine nationale ponctuellement affectés à cette mission, un réseau permanent de sémaphores répartis sur le littoral français qui jouent un rôle crucial dans la surveillance des approches maritimes et la détection précoce des menaces, et des avions de patrouille maritime et des hélicoptères de la marine qui fournissent une capacité d'observation et d'intervention continue.

Le dispositif associé à la posture permanente de protection terrestre est, comme son nom l'indique, permanent mais adaptable en volume pour répondre aux demandes des autorités civiles (préfets de département ou de région). En effet, sur le territoire national dans le milieu terrestre, le principe de primauté des forces de sécurité intérieure prévaut (cf. *infra*).

Enfin, la posture permanente de cyber défense s'articule autour d'une chaîne de commandement opérationnelle assurée par le COMCYBER (créé en 2017) et de moyens humains et techniques spécialisés. Il s'agit d'être en mesure de détecter les attaques, les caractériser, estimer leurs impacts prévisibles et réagir afin de préserver la capacité opérationnelle. Elle

s'appuie sur le Centre d'analyse de lutte informatique défensive (CALID) et sur des équipes de réponse à des incidents cyber maintenues en alerte.

Au bilan, environ 15 000 militaires protègent le territoire national en permanence, dans les trois milieux classiques ainsi que dans le champ cyber. Cela illustre l'effort significatif que les armées françaises consacrent de manière permanente à la mission de protection.

L'évolution de l'engagement des armées sur le territoire national

L'opération Sentinelle cadre l'engagement des armées sur le territoire national depuis 2016 au titre de la contribution à la défense civile. L'opération a bien évolué depuis son lancement un peu précipité. Actuellement, Sentinelle repose sur un dispositif opérationnel permanent complété par un échelon de renforcement programmé (*i. e.*, des unités identifiées et en alerte), l'ensemble à hauteur de 7 000 hommes. S'y ajoute une réserve stratégique de 3 000 hommes déployable sur ordre et sous faible préavis[93]. L'ensemble constitue ainsi dorénavant un dispositif souple, évolutif et dimensionné pour répondre au plus près au besoin de renforcement des forces de sécurité intérieure en fonction des besoins et du contexte, à l'instar de sa mobilisation dans le cadre la protection des Jeux olympiques de Paris 2024).

Le dispositif complet, à hauteur de 10 000 militaires, implique néanmoins en permanence une fraction significative de la force opérationnelle terrestre de l'armée de Terre, obérant, si elle venait à être entièrement déployée, la capacité de cette dernière à s'engager simultanément sur d'autres contrats opérationnels tels que l'hypothèse d'engagement majeur. La contribution permanente des armées à la défense civile, bien que fondée pèse en outre fortement sur le cycle opérationnel des unités, ce qui limite la capacité à maintenir l'entraînement des forces terrestres au niveau que requièrent les opérations du moment, mais aussi de celui des engagements de haute intensité que suppose le retour de la guerre. Cela, combiné à la meilleure efficacité atteinte dans le travail d'enquête policière en vue de prévenir les attentats terroristes aujourd'hui, milite pour reconsidérer l'envergure du dispositif permanent engagé dans Sentinelle, qui représente un effort durable pour les armées et continue de peser sur l'armée de Terre en particulier en termes de préparation opérationnelle et de régénération.

Pour autant, au-delà de son format, l'opération Sentinelle pourrait perdurer et évoluer comme cadre opérationnel pour l'engagement des forces armées sur le territoire national, dans une logique plus large de contribution de celles-ci à la maîtrise de l'ensemble des risques contre la

93. « Opération Sentinelle », ministère des Armées.

sécurité nationale. Des réflexions sont en cours à ce sujet au sein du ministère des Armées.

Sur le plan militaire, cela pourrait notamment permettre de dépasser la logique de milieu des postures permanentes de protection (maritime, aérien, terrestre, cyber…), afin de disposer d'une posture opérationnelle permanente de protection globale, dans une logique multi-milieux, multi-champs (M2MC) de coordination des effets militaires afin de mieux prendre en compte l'ensemble du spectre des risques et menaces, tout en préservant la primauté des forces de sécurité intérieure sur le territoire national. Cela pose en tout cas la question de la juste place des armées sur le territoire national, dans le contexte de menace du moment mais sans doute plus durablement, et de la nécessaire intrication entre défense militaire et contribution à la défense civile dans un monde où l'hybridité devient la norme.

Le Code de la défense dispose qu'« aucune force armée ne peut agir sur le territoire de la République pour les besoins de la défense et de la sécurité civiles sans une réquisition légale[94] ». Si la règle des « 4I » paraît conserver toute sa pertinence pour empêcher que les armées ne servent de supplétifs aux forces de sécurité intérieure, le principe de conditionner l'action des armées sur le territoire national à une réquisition pourrait être reconsidéré, afin notamment de leur permettre de mieux se préparer à y exercer une défense militaire le cas échéant.

En effet, au-delà du cadre d'engagement, l'un des enjeux de la protection du territoire national dans le contexte actuel est la capacité des armées à s'y déployer et à y agir efficacement. Loin d'être triviale, et au-delà des seules forces militaires, cette aptitude repose sur la mobilité routière des moyens militaires sur le territoire national, ainsi que sur la capacité à utiliser ou s'appuyer sur les infrastructures civiles publiques voire privées pour la conduite des activités militaires (ravitaillement, stationnement et campement, alimentation, voire maintenance). Or cette capacité a été significativement altérée par plus de trente ans de dividendes de la paix et d'engagement *a minima* des armées sur le territoire, en raison de l'absence de menace militaire contre le territoire national et en application du principe posé par le Code de la défense.

L'exercice ORION 23 était le premier jalon d'un cycle triennal « Conflits modernes » souhaité par l'État-major des armées afin de renforcer la préparation opérationnelle interarmées. L'objectif est de mettre en synergie l'entraînement de l'ensemble des armées, directions et services sur un scénario de haute intensité prenant en compte les domaines transverses tels que la guerre informationnelle, la logistique ou le spatial. ORION 2023 s'est ainsi déroulé sur une période de plusieurs mois, avec des opérations actives entre février et mai 2023. La dernière phase, sur trois

94. Article L.1321-1 du Code de la défense.

semaines, a mobilisé jusqu'à 12 000 soldats. L'un des enseignements majeurs d'ORION 23 a justement été la difficulté des armées à monter en puissance sur le territoire national.

La perspective renouvelée d'un engagement des forces armées sur le territoire national dans une logique de protection soulève ainsi des questionnements, tant en termes de commandement que de mise en œuvre des forces.

La transformation du commandement Territoire national de l'armée de Terre en État-major interarmées du territoire national (EMIA/TN) en juillet 2023 vise à répondre à la problématique du commandement des forces, en considérant le territoire national comme un théâtre d'opérations potentiel. Il s'agit de disposer le cas échéant, en appui du Centre de planification et de conduite des opérations (CPCO) au niveau stratégique et en complément des états-majors de zone de défense et de sécurité qui constituent l'Organisation territoriale interarmées de défense (OTIAD), d'un commandement opératif dédié à même de coordonner la réponse militaire à l'échelle supra-zonale et dans l'ensemble des milieux matériels et immatériels. L'EMIA/TN est en outre chargé de la conduite des études relatives à l'emploi des forces terrestres sur le territoire national[95].

En termes de mise en œuvre, pour que la capacité des armées à se déployer durablement sur le territoire national hors de leurs bases puisse être garantie et réactive, l'ensemble des moyens civils qui sont susceptibles de devoir y concourir (vecteurs de mobilité, stations de ravitaillement, appui logistique…) doit avoir été identifié en amont en vue d'une mise à disposition rapide aux armées le cas échéant. Cela suppose une planification prenant en compte la ou les hypothèses d'engagement des armées pour la protection du territoire national contre une attaque de type militaire. Les ministères concourants doivent être pleinement associés à l'élaboration de ces plans de défense du territoire, afin notamment de les assumer le moment venu. C'est également le cas des échelons zonaux et locaux qui seront éventuellement concernés par leur mise en œuvre.

Cela suppose également un cadre juridique adapté permettant la réquisition de ces moyens civils identifiés au profit des armées. Le cadre hérité de la guerre froide, largement inadapté au contexte moderne, mérite d'être réactualisé. La crise de la COVID-19, au travers de la confection des masques de protection, a mis en lumière le sujet de la réquisition de moyens privés par l'état au titre de l'intérêt national. Le ministère des armées a identifié cette problématique, notamment dans le cadre de ses réflexions et travaux « sur l'économie de guerre », et a travaillé sur ces questions, en particulier sa Direction des affaires juridiques. Il a ainsi publié un décret en 2024 cadrant les modalités de mise en œuvre du régime rénové de

95. Arrêté du 29 juin 2023 portant création de l'état-major interarmées du territoire national métropolitain, *Bulletin officiel des armées*, n° 52, 30 juin 2023.

réquisitions des personnes et des biens pour les besoins de la défense et de la sécurité nationale[96]. Le régime de réquisition rénové concerne autant la phase amont d'entraînement que la phase active de défense militaire. L'effort est notable. Pour autant, le décret laisse au ministère le soin, sur ordre du Premier ministre, de procéder au recensement du personnel et des biens concernés par le régime de réquisition. Le travail n'en est donc qu'à ses débuts et mérite d'être poursuivi.

En outre, la rapidité de montée en puissance repose, comme pour toutes les manœuvres militaires, sur l'entraînement de l'ensemble des acteurs impliqués. Elle suppose donc des mises en pratique régulières impliquant les armées mais aussi les acteurs concernés de l'autorité publique et de la société civile. ORION 23 a permis pour la première fois d'impliquer les autres ministères dans leur rôle en cas de scénario d'engagement majeur des armées. ORION 26 devrait aller plus loin encore sur le plan interministériel. Pour autant, ces mises en pratique méritent d'être déclinées par l'ensemble des acteurs à tous les échelons de mise en œuvre, que ce soit au niveau régional/zonal ou local. Elles permettront en outre d'identifier les freins éventuels, matériels ou organisationnels, qui peuvent éventuellement contraindre la montée en puissance des armées sur le territoire national, en vue de chercher à les lever.

Cela milite d'autant plus pour reconsidérer le cadre conceptuel d'engagement des forces armées sur le territoire national, car le principe de réquisition légale semble peu compatible avec la préparation opérationnelle nécessaire en amont aux armées pour être en mesure d'assurer efficacement la défense militaire sur le territoire si la situation se présente.

Pour autant, la difficulté évidente à impliquer à grande échelle des autorités civiles de tous niveaux dans des manœuvres militaires régulières, même sur le territoire national, tout comme le fait que l'activité opérationnelle des armées leur laisse peu de disponibilité pour un recours massif à ce type de mises en pratique, incitent à considérer qu'elles resteront néanmoins partielles et épisodiques. Par conséquent, il convient d'organiser sur le plan théorique la montée en puissance potentielle des armées sur le territoire national, sur la base d'un système lisible par tous, adossé à une planification robuste et détaillée. Ce système pourrait être graduel, avec un niveau de préparation et d'alerte en fonction du niveau de menace perçu, à l'instar de ce que peut être VIGIPIRATE pour la menace terroriste.

Au bilan, si l'exercice ORION 2023 a été un bon catalyseur pour la prise de conscience du besoin de reconstruire la capacité des armées à agir sur le territoire national, le chemin semble encore long pour la reconquête

96. Décret n° 2024-895 du 1er octobre 2024 relatif aux réquisitions pour les besoins de la défense et de la sécurité nationale et à leur articulation avec les différents régimes juridiques portant sur la préparation et la gestion des crises, Journal officiel de la République Française, n° 0234, 2 octobre 2024.

d'une capacité opérationnelle de défense militaire du territoire. Néanmoins, dans le contexte de menace actuel, appelé à perdurer, l'effort doit être poursuivi dans la perspective d'ORION 2026 et au-delà, par le ministère des Armées évidemment car c'est le premier concerné, mais également à l'échelon interministériel en vue d'impliquer l'ensemble des acteurs publics dans ce processus.

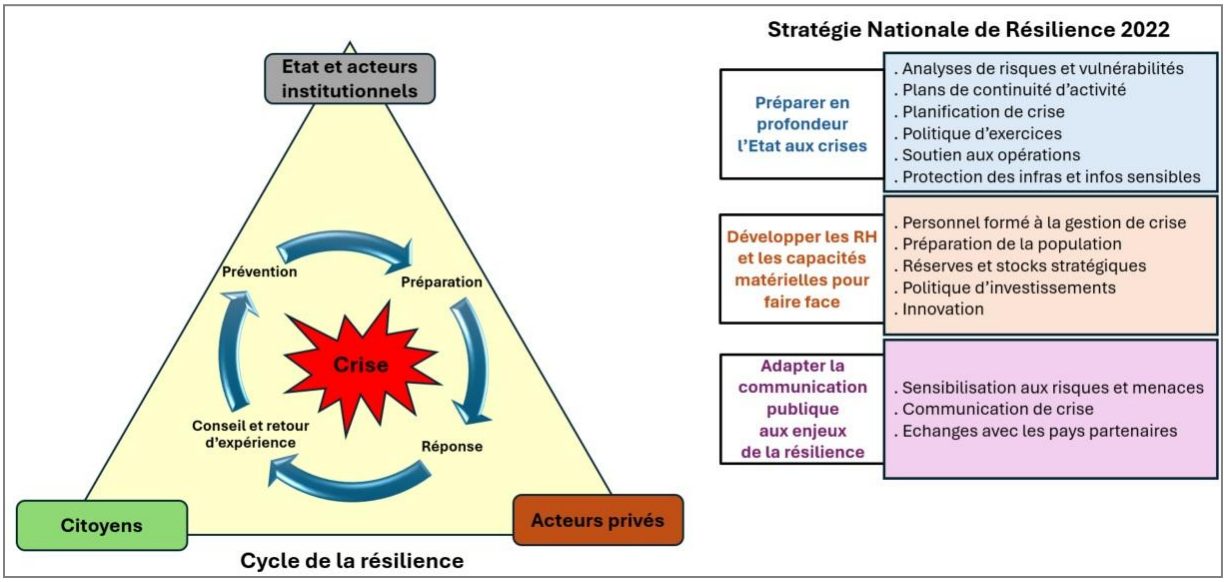
Construire la résilience de la nation à tous les échelons

Au-delà de la capacité des armées à s'engager sur le territoire national, la notion de défense du territoire est liée à celle de résilience. En effet, le cadre d'activation possible de la défense opérationnelle du territoire suggère des actions d'ampleur de déstabilisation organisées ou commanditées par un acteur externe malveillant. Dans un tel contexte, l'impact sur la société, matériel ou psychologique, sera vraisemblablement majeur et viendra directement mettre au défi la capacité de résilience de la nation. La pandémie du Covid-19 et l'agression russe contre l'Ukraine en 2022 ont déjà replacé la question de la résilience au cœur des préoccupations, et elle s'est durablement imposée comme l'un des enjeux majeurs des sociétés modernes. Néanmoins, si la France a œuvré activement depuis lors pour développer sa résilience au niveau institutionnel, l'effort doit être accentué pour une meilleure prise en compte au niveau sociétal, comme l'illustrent le cas ukrainien ainsi que diverses initiatives prises par d'autres pays européens.

L'enjeu de la résilience a bien été intégré à tous les niveaux. C'est le cas tout d'abord dans les sujets d'attention de l'OTAN, au travers de la constitution d'un Civilian Emergency Planning Commitee en 2022, dont les recommandations aux États membres dépassent le seul champ de l'appui aux opérations de l'Alliance. L'UE s'est également saisie de cet enjeu en publiant en 2022 une directive sur la résilience des infrastructures critiques, ayant vocation à être déclinée au niveau national par les États membres[97]. La directive vise à renforcer la résilience des entités critiques face à une série de menaces, notamment les risques naturels, les attaques terroristes, les menaces internes ou le sabotage, ainsi que les urgences en matière de santé publique. Pour la France, cet enjeu de l'accroissement de la résilience face aux risques et menaces a été formalisé au niveau national en 2022 au travers de la SNR.

97. « Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council », Union européenne, 2022.

Démarche de renforcement de la résilience nationale



Source : schéma réalisé par l'auteur © Ifri, 2025.

Cette stratégie repose sur trois piliers : préparer en profondeur l'État aux crises, développer les ressources humaines et les capacités matérielles pour faire face, et adapter la communication publique aux enjeux de la résilience. Elle implique l'ensemble des départements ministériels, conformément aux dispositions du Code de la défense. Concrètement, la SNR de 2022 est déclinée en un plan d'actions interministériel, mis en œuvre par les ministères sous la supervision du SGDSN. Ce plan d'actions fait l'objet de revues de pilotage périodiques afin d'en jauger le niveau d'avancement. Le renforcement de la résilience est donc suivi et piloté au plus haut niveau de l'État, et la SNR est posée comme la pierre angulaire de la stratégie de sécurité nationale. Pour autant, la mise en œuvre de ce plan d'actions est laissée à la charge des ministères, sans budget dédié.

L'adossement de la fonction Résilience à la fonction Protection à l'occasion de la SNR de 2022 illustre une réalité : tout dispositif de protection ne peut raisonnablement prétendre à une efficacité totale. Par conséquent, et dans le contexte actuel de confrontation, il est nécessaire de préparer la société française à la perspective d'actes malveillants non déjoués, voire d'attaques contre le territoire national, et aux conséquences de ceux-ci.

Conceptuellement, une résilience effective repose tant sur une bonne préparation de l'État et des autres acteurs de la société en amont que sur une capacité de réponse efficace aux crises. Le cycle de la résilience est donc le suivant : prévention ; préparation ; exercices ; réponse ; conseil et retour d'expérience. La résilience concerne ainsi l'ensemble des acteurs de la société, institutionnels et privés, jusqu'au citoyen, qui doivent tous intégrer et décliner cet enjeu chacun à leur niveau.

Le plan d'actions associé à la SNR publiée en 2022 repose sur trois piliers : préparer en profondeur l'État aux crises ; développer les ressources humaines et les capacités matérielles pour faire face ; adapter la communication publique aux enjeux de la résilience. Les deux derniers volets incluent bien la sensibilisation de l'ensemble des acteurs aux risques et menaces, et l'affermissement de la préparation de la population à la crise.

Pour autant, si l'enjeu de la résilience semble avoir été bien pris en compte au niveau ministériel, la réalité de la menace et l'enjeu de résilience de la société ne transparaissent qu'insuffisamment dans le débat public et auprès du citoyen. Ainsi, si les nouvelles menaces sont généralement bien identifiées par secteur d'activité, la société française dans sa globalité est encore insuffisamment consciente du contexte de menace et mal préparée à y faire face. Or le principal ressort de la campagne de déstabilisation russe, notamment, est psychologique. Elle vise à fragiliser la cohésion interne des sociétés qui s'opposent à la Russie, notamment les sociétés démocratiques où la libre-pensée et la libre expression sont la règle.

Face à la perspective d'une potentielle agression russe, des pays comme la Suède ont fait le choix d'envoyer *via* leur Agence de sécurité civile[98] un prospectus à 4,7 millions de foyers pour les inciter à se préparer à des « crises et catastrophes en temps de paix, mais également à divers types d'attaques contre la société suédoise ». Au-delà des conseils pratiques sur le matériel à détenir et les bons réflexes à avoir dans une telle situation, cette démarche interroge sur le rôle du citoyen en cas de crise ou dans un contexte de menace. *A minima*, son rôle est passif, à savoir être préparé, psychologiquement et matériellement, à faire face aux situations de crise ou dégradées, voire aux conséquences d'actes malveillants. Cette démarche marque un retour à la culture de la guerre froide, où la menace soviétique était un paramètre constant de la vie des sociétés européennes. Le gouvernement français s'est lancé dans la même démarche et s'apprête à délivrer un guide de la résilience à tous les ménages français durant l'année en cours, dans une logique de résilience de la société civile[99].

L'exemple ukrainien d'une société en guerre montre, lui, que le citoyen peut également avoir un rôle actif dans un tel contexte : vigilance et contribution à la remontée d'informations, contribution volontaire éventuelle à la protection ou au soutien de l'action institutionnelle en situation de crise.

Un rapport de l'Assemblée nationale sur la résilience rédigé en 2022 estimait ainsi qu'elle avait jusque-là été trop considérée comme une stratégie descendante, devant produire des effets sur les citoyens, et qu'il convenait d'y substituer une stratégie de résilience qui ferait au contraire du

98. Civil Contingencies Agency.
99. H. Stock, « Manuel de survie : que pourrait contenir le nouveau livret du gouvernement ? », *Le Figaro*, 25 mars 2025.

citoyen un acteur clé de la force de la nation, dans une logique de défense inclusive[100] incluant toutes les composantes de la société.

Ce rôle ne va pas de soi, en particulier dans une société où la disparition du service national a créé un fossé entre le citoyen et l'action publique. Cela suppose tout d'abord un discours public de sensibilisation affirmé, largement relayé à tous les niveaux de l'action publique, qui reconnaît la réalité de la menace, sans alarmisme mais sans naïveté ou déni. Cela passe ensuite par une information du citoyen sur la façon dont il peut contribuer à l'action publique en cas de crise, et les modalités pour le faire. Cela suppose en outre une organisation de l'État pour fédérer, accueillir et organiser cette contribution.

Au-delà de l'information poussée, la réalisation d'exercices de résilience de grande ampleur impliquant largement l'ensemble des acteurs de la société, citoyens compris, permettra sans doute de donner plus de substance à cette nouvelle réalité, en favorisera l'appropriation par tous et chacun, et motivera sans doute un engagement citoyen plus affirmé dans le domaine

Des pays comme l'Ukraine, Israël ou Taïwan, confrontés à une menace existentielle, ont mis plusieurs années pour s'organiser pour permettre à leurs citoyens de contribuer à la défense de la nation. L'Ukraine a commencé à fédérer cette contribution civile dès 2014, en incorporant dans la Garde nationale nouvellement formée, sous la responsabilité du ministère de l'Intérieur, les bataillons de volontaires formés en réaction à l'opération russe dans le Donbass en 2014. Les initiatives civiles ayant émergé en 2014 dans ce contexte, telles que la collecte de fonds à grande échelle, la fourniture de matériel ou de nourriture aux soldats sur le front, ou encore la collaboration entre la défense et le secteur civil des technologies de l'information, ont ainsi pu être encouragées et reproduites à plus grande échelle en 2022[101], au point de devenir un facteur clé de la défense du pays.

L'initiative suédoise montre que le chemin à parcourir dans ce domaine dans les sociétés où la menace est moins prégnante reste grand. Toutefois, le contexte actuel de résurgence de la conflictualité semble s'inscrire dans le temps long, ce qui milite pour consacrer l'effort nécessaire à la reconstruction de la mentalité et du cadre qui permettra au citoyen de contribuer activement sur le territoire national à la défense de la nation. En effet, si la stratégie nationale de résilience fait la part belle au volet de la préparation de l'État et des acteurs publics aux crises, et prend en compte le

100. A. Freschi et T. Gassilloud (rapporteurs), *Rapport d'information sur la résilience nationale*, Rapport n° 5119, Mission d'information sur la résilience nationale, Paris, Assemblée nationale, février 2022, p. 19.
101. J. Hedenskog, *Explaining Ukrainian Resilience*, Stockholm Centre for Eastern European Studies (SCEEUS), 5 avril 2023.

besoin de sensibiliser l'ensemble des acteurs aux risques et menaces, l'organisation de la contribution citoyenne se limite en l'état à l'encouragement à la mobilisation des citoyens dans les différents dispositifs d'engagement existants (Garde nationale, Service national universel, service civique, tous types de réserves).

Au bilan, force est de constater que les jalons posés successivement par la France depuis la mise en place de la SAIV en 2006 constituent un dispositif au socle étendu et composite, qui a pris la mesure des enjeux de la protection et de la résilience et qui cherche à y répondre efficacement. La bascule majeure est l'évolution du contexte international sur les dix dernières années, et le fait que la France est plus directement ciblée, en tant que pilier du monde occidental, par des compétiteurs stratégiques qui cherchent et chercheront toujours davantage à exploiter ses faiblesses pour mieux l'affaiblir, en usant sans limites de l'ensemble de la palette des actions déstabilisatrices. Face à ce contexte plus exigeant, le socle existant doit bien évidemment être consolidé autant que nécessaire, mais cela ne sera probablement pas suffisant face à des adversaires déterminés, désinhibés, créatifs et opportunistes, et qui s'appuient pleinement sur les nouvelles technologies pour nuire dans une logique asymétrique.

Mieux prendre en compte les nouvelles menaces

Si la France dispose de fondements solides en matière de protection de ses activités sensibles, la robustesse d'une chaîne repose toujours sur son maillon le plus fragile. L'adversaire à l'initiative en est bien conscient et cherchera toujours à exploiter les vulnérabilités identifiées. La campagne de déstabilisation russe en Europe, par exemple, est pilotée au plus haut niveau de l'appareil d'État russe, et les actions sont coordonnées et planifiées dans le but de créer de la confusion, de la dissension, voire du chaos, pour servir les intérêts stratégiques de la Russie. L'amélioration du dispositif global de Protection doit donc partir de cet état de fait en cherchant en priorité à en réduire les vulnérabilités plutôt qu'à en renforcer encore les éléments déjà bien établis.

L'objectif de cette partie est de présenter quelques pistes de réflexion, au prisme de l'évolution de la menace telle que présentée en deuxième partie, sans prétendre à l'exhaustivité. Il s'agit essentiellement de mieux anticiper et prévoir les menaces, de combler les lacunes existantes, de considérer et de se préparer au pire envisageable, et enfin de repenser l'approche dissuasive française vis-à-vis de ses compétiteurs.

Pour une meilleure coordination collective et multisectorielle

Avant toute autre considération, confronté à l'émergence de nouvelles menaces combinées à la persistance, voire la résurgence, de menaces plus classiques, il n'est pas envisageable pour la France d'avoir un dispositif permanent de protection efficace tous azimuts, à large spectre et large couverture, à un coût assumable. C'est d'autant plus vrai en raison de la situation géographique de la France, ouverte sur plusieurs théâtres géographiques. En outre, la stratégie de nos compétiteurs au travers de la multiplication de mini-incidents est bien de chercher à saturer nos dispositifs de protection taillés au plus juste, de créer une ambiance de psychose et de noyer les opérations de déstabilisation à fort impact dans le flot des événements.

Partant de cette réalité, il convient de chercher à détecter au plus tôt les signaux faibles et d'anticiper au mieux l'évolution de la menace en vue d'identifier les priorités justifiant un effort de protection supplémentaire, et d'adapter de manière versatile le dispositif de protection.

En France, la remontée d'informations sur les menaces repose sur deux piliers : les services de renseignement du premier et du second cercle, et les chaînes Défense et Sécurité des ministères pilotées par les HFDS. Cela induit une conscience inégale de la menace en fonction des secteurs d'activité, les services de renseignement étant majoritairement concentrés au sein du ministère des Armées, de l'Intérieur et des Finances. En outre, les services des HFDS des différents ministères sont inégalement dimensionnés et appuyés, et ne sont donc pas tous aussi aptes à conduire une analyse fine de la menace. Ainsi, face à des adversaires agiles, versatiles et déterminés à entraver l'action de la France en utilisant l'ensemble du spectre des actions possibles sur des cibles de tout type, il semble pertinent de disposer d'une capacité robuste d'analyse multisectorielle de la menace, œuvrant au bénéfice de tous les ministères et départements de l'État.

La création annoncée dans la *Strategic Defense Review* britannique d'un CyberEM Command pour intégrer la menace cyber, électromagnétique et informationnelle [102] et d'une Counter-Intelligence Unit pour mieux protéger les capacités militaires contre les malveillances[103] illustre ce besoin de structures pour mieux appréhender et contrer la menace dans sa pluralité et sa globalité.

Cela milite premièrement pour renforcer encore le dialogue déjà existant entre les entités membres de la communauté du renseignement. En effet, si la détection et l'entrave des menaces ont bien été incluses dans l'axe « Placer le renseignement au cœur de la décision et de l'action » de la SNR 2025, cette démarche doit s'inscrire dans le temps long. Un Conseil national du renseignement (CNR) a été créé dès 2008 pour créer les conditions de ce dialogue[104]. Néanmoins, il s'agissait essentiellement d'un mécanisme de coordination discontinu, au niveau des directeurs des services de renseignement. La Coordination nationale du renseignement et de la lutte contre le terrorisme (CNRLT), créée en 2017 dans un contexte de lutte antiterroriste, est la première structure permanente chargée de la coordination des services de renseignement. Néanmoins, le dialogue interservices au sein de la communauté du renseignement a été largement orienté depuis lors sur la problématique de la lutte contre le terrorisme. Au-delà, chaque service agit principalement dans son périmètre de responsabilité. Afin de mieux prendre en compte le caractère composite de la menace à laquelle la France est confrontée, il conviendrait sans doute de réorienter ce dialogue interservices, sans pour autant baisser la garde sur la menace terroriste.

102. J. Hill, « UK Urged to Set Up Counter-Intelligence Unit for Defence", Naval Technology, June 6, 2025, available at: www.naval-technology.com.
103. J. Hakmeh, « CyberEM Command: The UK's Strategic Leap in Integrated Modern Warfare », Chatham House, 6 juin 2025.
104. F. Vadillo et A. Papaemmanuel, *Les Espions de l'Élysée*, Paris, Tallandier, 2019.

En parallèle, la coordination interministérielle en matière de Défense et Sécurité mérite également d'être renforcée. La Commission interministérielle de défense nationale (CIDN) a été réactivée en septembre 2023 pour répondre aux besoins d'un outil permanent de coordination interministérielle, au niveau des HFDS des ministères, sous la présidence du SGDSN. Elle ne se réunit toutefois que périodiquement, et son action de coordination interministérielle est donc discontinue. La cellule interministérielle de crise ne remplit le rôle de coordination interministérielle que lorsqu'elle est activée en cas de crise majeure.

Aussi, face à la spécialisation des services de renseignement et la discontinuité de la coordination interministérielle en matière de défense et de sécurité, il semble pertinent de disposer d'une capacité intégrée et permanente d'analyse multisectorielle de la menace, à l'instar de ce que peut être le Centre opérationnel de la fonction garde-côtes (COFGC) pour le milieu maritime. Cette capacité aurait vocation à prendre en compte au maximum la remontée d'informations des différentes entités, à les analyser en vue de détecter des signaux faibles et de jauger le niveau de menace, et *in fine* à susciter une réponse adaptée. Une telle capacité serait logiquement articulée avec le SGDSN, qui a vocation à coordonner l'action interministérielle à des fins de défense et de sécurité nationale, bien que le mandat de ce dernier soit davantage pensé dans une logique de travaux de fond sur le long terme.

Elle pourrait utilement s'appuyer sur l'expérience étendue du ministère des Armées en matière de renseignement, de Défense et de Sécurité, et de mise en œuvre de centre opérationnels permanents. À ce titre, la Direction de la protection des installations, moyens et activités de la défense (DPID), service du HFCDS du ministère des Armées, assure déjà l'analyse de menace multisectorielle et la coordination de l'action des entités du ministère en matière de défense et sécurité. Elle dispose donc d'une réelle expertise qui pourrait être mise à profit pour construire une telle capacité de veille interministérielle. Pour autant, d'autres services de HFDS disposent également d'entités assurant une veille et une analyse multisectorielle, à l'instar de la Cellule ministérielle de veille opérationnelle et d'alerte (CMVOA) du ministère des Transports, de l'Équipement, du Tourisme et de la Mer. Il convient donc d'étudier la faisabilité d'une convergence de ces entités de veille et d'analyse de la menace.

Les capacités offertes par l'intelligence artificielle pourraient s'avérer majeures dans un tel dispositif, en aidant à analyser la masse d'informations remontées, aussi bien par les services de renseignement que celles disponibles en source ouverte (presse, *think tanks* et recherche, blogs spécialisés, réseaux sociaux, …), en les croisant et en faisant ressortir ce qui est pertinent au profit du personnel du centre de veille.

Enfin, cette analyse de la menace en temps réel mériterait d'être partagée largement avec nos alliés, afin de favoriser une plus grande coopération entre les pays concernés, à l'instar de l'effort de coopération internationale en matière de lutte contre le terrorisme. Cela suppose de reconsidérer la protection contre la menace hybride non plus comme un seul effort national mais bien comme un effort collectif entre pays notamment européens, partageant les valeurs démocratiques.

Reconsidérer le dispositif de protection contre les menaces aériennes

Dans un contexte de durcissement de la posture de nos compétiteurs et de guerre hybride, la potentialité d'une menace aérienne d'ordre militaire contre le territoire national, sous le seuil de la dissuasion, ne semble plus pouvoir être écartée. Elle pourrait être constituée de frappes, à longue portée mais pas exclusivement, potentiellement saturantes, de missiles, de drones ou de munitions téléopérées. Cette menace potentielle appelle à reconsidérer le dispositif français de défense aérienne sur le territoire national.

La menace missile contre le territoire national a déjà été considérée dans le cadre des réflexions autour des *Livres blancs* de 2008 et de 2013, essentiellement dans son volet nucléaire. Néanmoins, cette menace a été considérée comme faible pour la France en raison de l'absence d'intention perceptible des pays disposant de cette capacité de l'utiliser contre la France, puissance nucléaire, capable d'infliger des représailles massives[105]. L'argument d'une dissuasion fondée sur la riposte nucléaire semble néanmoins fragile face au scénario d'une attaque par un groupe terroriste ou un proxy instrumentalisé par une grande puissance, voire d'une frappe étatique à longue portée d'ampleur limitée (cf. *supra*).

En complément du dispositif de sûreté aérienne (PPSA) décrit précédemment, qui offre une capacité aérienne d'interception réactive, la France dispose actuellement pour la protection sol-air de ses emprises vitales de quatre escadrons de défense sol-air (EDSA), mettant chacun en œuvre deux systèmes SAMP/T-Mamba. Ces escadrons protègent en permanence les bases aériennes d'Avord, Saint-Dizier et Istres, liées à la dissuasion nucléaire, ainsi que celle de Mont-de-Marsan. Couplée au dispositif permanent de sûreté aérienne, cette capacité de protection face à une menace aérienne est robuste. Elle n'est cependant pas sans failles.

105. *Révision du Livre blanc sur la défense et la sécurité nationale : quelles évolutions du contexte stratégique depuis 2008 ?*, Rapport n° 207, Commission des Affaires étrangères et de la Défense, Paris, Sénat, décembre 2011.

Premièrement, la capacité de détection aérienne française n'est pas optimisée contre les mobiles volant à basse altitude, ce qui induit une détection tardive face à ce type de menaces. Les moyens, navals ou aériens, de surveillance des approches maritimes au titre de la posture permanente de sauvegarde maritime ne sont, eux, généralement pas optimisés pour la détection aérienne. Par conséquent, une attaque de drones volant à basse altitude en provenance de la mer, par exemple, ne pourra être détectée suffisamment tôt pour être traitée à temps par les avions de la permanence opérationnelle si leur cible se situe dans la bande côtière. Pareillement, face à une attaque saturante de missiles *low cost* en provenance de la mer, même avec une détection avancée, il n'est pas garanti que le dispositif permanent de sûreté aérienne soit en mesure de traiter l'ensemble des vecteurs menaçants avant qu'ils atteignent leur cible, notamment si elle se situe dans la bande côtière.

Pour ce qui est des missiles balistiques, la France reste fragile face à ce type de menaces. Tout d'abord, elle ne possède pas encore une capacité satellite de détection avancée. Elle est donc dépendante du soutien américain en la matière. Le fait de ne pas disposer d'une capacité souveraine, ou *a minima* européenne, dans ce domaine critique de la guerre moderne interroge, en particulier dans le contexte actuel de recomposition géopolitique. En termes d'interception de missiles balistiques, la France dispose comme évoqué précédemment de ses systèmes SAMP/T Mamba à base de missiles ASTER 30, qui permettent de répondre à cette menace. Ces systèmes SAMP/T-Mamba peuvent être ponctuellement déployés hors de leurs bases usuelles, notamment dans le cadre de dispositifs de protection de grands événements (DSPA [106]) comme les commémorations du débarquement de Normandie, le G20, le salon du Bourget ou le défilé du 14 Juillet. Pour autant, en cas de menace missile avérée contre le territoire au titre de leur mission prioritaire de protection des moyens de la dissuasion, il est vraisemblable que ces systèmes seront maintenus sur leurs bases au regard de leur nombre très restreint. La question de la protection des autres emprises sensibles contre la menace balistique reste donc entière.

Au-delà de la menace « externe » dans le domaine, les exemples récents d'infiltration de commandos en vue de mener des attaques par drones contre des cibles militaires stratégiques, dans le cadre de l'opération ukrainienne *Spider's Web*[107] ou des frappes israéliennes contre l'Iran du 12 juin 2025[108], illustrent le fait qu'une frappe de drones « de l'intérieur » est accessible à un adversaire déterminé, et donc possible. Une telle frappe limite bien

106. Dispositif particulier de sûreté aérienne.
107. K. Bondar, « How Ukraine's Operation "Spider's Web" Redefines Asymmetric Warfare », CSIS, 2 juin 2025.
108. L. Berman, « Mossad Set Up Drone Base in Iran; UAVs Were Activated Overnight to Strike Surface-to-Surface Missile Launchers Aimed at Israel », *The Times of Israël*, 13 juin 2025.

évidemment le temps de réaction en l'absence de préavis et ne permettrait donc pas le traitement par le dispositif permanent de sûreté aérienne.

Enfin, la France ne dispose actuellement d'aucune capacité en mesure d'agir hors des couches les plus basses de la très haute altitude (THA – bande située entre 20 et 100 km d'altitude). Or l'apparition de ballons atmosphériques, de drones capables d'y voler, de planeurs hypersoniques ou de satellites en orbite basse impose de s'intéresser à ce nouvel espace de conflictualité[109] et de développer les moyens d'y agir. Les récents essais de tir de missiles MICA vers la THA depuis des *Rafale* et *Mirage 2000*[110] sont un premier pas dans cette direction en vue de préciser les capacités à développer, mais la démarche n'en est qu'à ses débuts.

Aussi, sans verser dans la démesure pour la France d'une bulle de protection intégrale type *Iron Dome* israélien ou encore le projet de *Golden Dome* américain, il semble nécessaire de revoir les moyens et le dispositif de défense sol-air des infrastructures critiques françaises pour les adapter au nouveau contexte de menace. Le besoin de consolidation de la défense sol-air est bien pris en compte dans le cadre de la LPM 2024-2030[111]. L'acquisition d'ici 2030 de neuf systèmes courte portée VL MICA[112] et de 24 véhicules de défense sol-air très courte portée d'accompagnement Serval Mistral[113] est évidemment un pas dans cette direction, qui doit encore se concrétiser. L'effort semble néanmoins insuffisant sur le plan quantitatif.

D'une part, s'il est effectivement prévu par la LPM de remplacer les systèmes SAMP/T par des équivalents de nouvelle génération d'ici à fin 2030, la cible d'acquisition pour ces systèmes est maintenue à huit comme actuellement, ce qui ne permet pas de répondre au besoin de défense antimissile balistique en dehors des emprises vitales.

Pour ce qui est des menaces saturantes non balistiques, l'efficacité défensive face à ce type de menaces repose sur la capacité à traiter rapidement et efficacement, et à coût maîtrisé, un grand nombre de cibles, ce qui suppose donc des capacités d'engagement au sol basées sur un grand nombre de systèmes mobiles et distribués[114], ainsi que d'un armement air-air à bas coût, type roquettes guidées.

109. « La très haute altitude : un nouvel espace de conflictualité ? », Ministère des Armées, Le Bourget 2023.
110 L. Lagneau, « Des *Rafale* et des *Mirage 2000* ont tiré des missiles MICA vers des ballons stratosphériques avec succès. », Zone Militaire Opex 360, 24 juin 2025.
111. Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, rapport annexé § 2.2.2.
112. Véhicule de défense sol-air à base de missiles VT1, ayant vocation à contrer la menace d'aéronefs volant à basse et à très basse altitude.
113. Véhicule de défense sol-air à base de missile Mistral anti-aérien très courte portée.
114. A. Gorremans, « Économie des échanges de salves : vers la fin de la polyvalence des munitions ? », *Notes de l'Ifri*, Ifri, juin 2025.

Enfin, pour ce qui est de la menace de drones, notamment interne, son ubiquité pose un problème d'échelle. Le département de la Défense américain, conscient de la vulnérabilité américaine face à des attaques de ce type, a ainsi récemment lancé un appel dans le cadre de l'initiative *Replicator*[115] pour l'acquisition urgente et en masse de systèmes anti-mini-drones[116], notamment pour protéger les bases aériennes américaines. Effectivement, au regard du coût unitaire des missiles de défense sol-air, des solutions moins coûteuses, mobiles, de destruction à base d'artillerie à tir rapide[117], voire de neutralisation à base de contre-mesures électronique, pourraient être considérées pour une acquisition en masse. L'idée étant de disposer d'un moyen déployable, facile à mettre en œuvre, en vue de disposer d'une capacité ajustable de protection des infrastructures sensibles face à des menaces *low cost*, en complément des systèmes de défense à base de missiles.

Or, les cibles prévues par la LPM 2024-2030 pour les camions Serval de lutte anti-drones à base d'artillerie de 30 millimètres, et de systèmes de brouilleurs anti-drones Parade, respectivement de 12 et 15 systèmes d'ici 2030, paraissent très insuffisantes pour espérer protéger les sites sensibles sur le territoire, dans les Outre-mer et surtout les forces déployées face à cette menace qui prend de l'ampleur.

A minima, la mise en place de ce type de systèmes à titre permanent sur les sites critiques situées sur la bande côtière, par exemple au sein des bases navales de Brest et de Toulon, semble nécessaire pour mieux répondre à cette menace. Au-delà, l'identification des capacités critiques sur le territoire national pouvant constituer une cible de choix et atteignable par une attaque de cette nature pourra permettre de déterminer les éventuelles failles du dispositif et par voie induite les besoins complémentaires éventuels en système de défense sol-air afin de combler les manques en la matière.

Sur le plan maritime, de manière comparable au milieu aérien, le développement rapide du segment des drones navals, dans la continuité de celui des drones aériens, pourrait également créer à terme les conditions pour une possible attaque par des acteurs non étatiques d'une infrastructure côtière par voie maritime depuis la mer. Les attaques de drones-suicides ukrainiens[118] contre des cibles dans l'enceinte de la base navale de Sébastopol, insuffisamment protégée, illustrent ce mode d'action. À ce stade, la taille et le coût unitaire des drones navals suicides, ainsi que la complexité de la mise en œuvre depuis la mer par des navires non spécialisés, rendent ce scénario nettement moins probable dans un contexte

115. Initiative américaine lancée à l'automne 2023 cadrant l'acquisition urgente d'équipements militaires *low-cost* et productibles en masse, en vue d'obtenir un effet de levier sur le champ de bataille.
116. J. Hill, « US Call for Low Collateral C-sUAS under Replicator 2 », Naval Technology, 6 mai 2025.
117. À l'instar de la solution RapidFire développée par Thales et KNDS.
118. G. Vazquez Orbaiceta, « History Repeats Itself: Lessons from the Attack on the Black Sea Fleet in Sebastopol », Universidad de Navarra, 28 novembre 2022.

de guerre hybride qu'une attaque par voie aérienne. Cela appelle néanmoins à se repencher sur le dispositif de défense maritime du territoire et sur les moyens de protection active/passive ou de résilience des bases navales, voire des principaux ports français, afin de déterminer s'ils sont en mesure de faire face à une menace de cette nature.

Mieux prendre en compte les « espaces communs »

Le premier des espaces « communs » moderne est l'espace numérique (« cyberespace »). Son développement est allé de pair avec celui, progressif, de pratiques destructrices dans cet espace. La France a toutefois bien pris en compte cet enjeu dès 2009 en créant l'Agence nationale de sécurité des systèmes d'information (ANSSI), autorité nationale en matière de cybersécurité, chargée de la prévention mais aussi de la réaction aux incidents informatiques visant les institutions sensibles. Elle s'est ensuite dotée en 2015 d'une *Stratégie nationale pour la sécurité du numérique*, puis a conduit une *Revue stratégique de cyberdéfense* en 2018.

Plus spécifiquement, afin d'assurer la protection de ses réseaux et d'intégrer le combat numérique au cœur des opérations militaires, le ministère des Armées a créé en 2017 le COMCYBER, puis mis en place une posture permanente de cyberdéfense assurée par ce dernier en complément des autres postures permanentes de protection.

L'enjeu de la protection dans le cyberespace est donc bien compris et la France s'est donné les moyens d'y répondre. Le constat est toutefois différent dans d'autres espaces communs soumis à des menaces, tels que l'espace ou encore la haute mer. En effet, plusieurs événements ont mis en lumière la vulnérabilité de certaines infrastructures, critiques pour les États et les sociétés bien qu'étant physiquement situées dans des espaces considérés comme communs à l'humanité.

À titre d'exemple, des dégradations successives de câbles énergétiques et de communication sous-marins survenues en mer Baltique (11 incidents reportés depuis octobre 2023) ont attiré l'attention internationale, notamment comme une possible matérialisation d'une guerre hybride. Chaque incident de ce type mérite de faire l'objet d'une analyse spécifique et la caractérisation de l'intention nuisible n'est jamais aisée. En effet, les câbles sous-marins dans le monde sont très régulièrement sujets à des dégradations non intentionnelles (ancres, chaluts de fond, usure). Pour autant, ces incidents illustrent *a minima* la possibilité et la faisabilité d'actes malveillants contre ce type d'infrastructures.

Or le droit international en matière de dégradation de câbles ou de *pipelines* sous-marin est régi par l'article 113 de la Convention des Nations unies sur le droit de la mer (1982) et par la Convention de Paris pour la protection des câbles sous-marins (1884), deux textes qui ne reflètent plus

les réalités géoéconomiques d'aujourd'hui. Il spécifie que l'État côtier concerné peut disposer d'une compétence pénale pour juger les malfaisances contre ces infrastructures mais que le tribunal compétent pour des atteintes au-delà des eaux territoriales relève de l'état de pavillon du navire, ce qui aide peu contre les formes de guerre hybride en mer. Par ailleurs, le droit de la mer reconnaît aux États le principe d'autodéfense en mer, notamment sur les infrastructures *offshore* fixes considérées comme rattachées à l'État côtier. Néanmoins, la question de l'État de rattachement des câbles sous-marins en eaux internationales se pose, tout comme la caractérisation de l'attaque que suppose le principe même de protection.

La problématique est similaire dans le milieu spatial. Le droit dans l'espace repose sur des principes d'utilisation pacifique de l'espace, de conformité au droit international et de responsabilité. De ces deux premiers principes découle le principe de non-agression, du dernier principe découle celui de juridiction sur les objets spatiaux. Afin que les objets spatiaux (habités ou non) restent soumis à une juridiction nationale et au contrôle d'un État, il est prévu qu'ils soient immatriculés par cet État. L'immatriculation a un effet constitutif de juridiction sur l'objet spatial et à son bord. La responsabilité des dommages causés par un objet spatial est donc portée par l'État d'immatriculation. Là encore, ce droit n'a que peu de pertinence face à des actions malveillantes dans l'espace. Or des satellites français ont déjà été approchés plusieurs fois par des satellites étrangers[119]. Bien que le sujet soit couvert par le secret, il semble avéré que certaines nations spatiales ont développé des systèmes en mesure de réaliser des actions inamicales dans l'espace : observation, écoute, voire saisie ou désemparement de satellite[120].

Face à une guerre hybride, dans le relatif vide juridique qui encadre les activités dans ces espaces communs, le cas des infrastructures critiques portées par des intérêts privés, comme c'est le cas pour bon nombre des infrastructures énergétiques, de communication ou d'observation spatiale, mérite un traitement dédié. Il convient de définir une stratégie de protection particularisée où l'État assume son rôle régalien en appui aux opérateurs privés. Cela passe tout d'abord par une meilleure identification et un référencement par l'État des infrastructures situées dans les espaces communs et considérées comme critiques. Il est ensuite nécessaire de mettre en place des moyens de surveillance en mesure de détecter les agressions éventuelles contre ces infrastructures critiques, afin de prévenir les actes malveillants dissimulés. Ce peut être soit des moyens techniques fixes, soit des moyens mobiles de surveillance. En parallèle, il convient de

119. L. Lagneau, « Des satellites sensibles français approchés par des engins aux intentions parfois « inamicales », Zone Militaire OPEX 360, 2 avril 2018.
120. E. Bottlaender, « Le satellite chinois Shijian-21 fait le ménage en orbite géostationnaire », Clubic, 28 janvier 2022 ; B. Stojkovski, « Russian Satellite with Suspected Weapon Maneuvers Near US Space Asset, Sparks Fear », Interesting Engineering, 31 mai 2025.

développer en lien avec les opérateurs concernés la résilience des capacités portées par ces infrastructures critiques (durcissement, redondance, fonctionnement en réseau). Enfin, afin de dissuader les agressions contre ces systèmes par des acteurs peu soucieux du droit international, l'État doit pré-identifier et planifier des mesures de rétorsion graduées, en vue de les mettre effectivement en application le cas échéant. Il peut s'agir d'une condamnation internationale, de sanctions, voire de mesures actives sur les systèmes ou infrastructures adverses, en fonction de la gravité de l'acte malveillant.

Mieux protéger les Outre-mer

Les Outre-mer français sont naturellement couverts par la fonction « Protection – Résilience » au titre du territoire national. Pour autant, ils font l'objet de menaces spécifiques, qui nécessite une réponse elle-même spécifique.

Tout d'abord, les Outre-mer français sont caractérisés par leur forte vulnérabilité à de nombreux risques, naturels et sociaux, pour lesquels la réponse de l'État met régulièrement à contribution les forces armées[121]. Toutefois, comme évoqué en introduction, ces risques ont été intentionnellement écartés de l'étude pour se concentrer sur les menaces.

La première menace est de type subversif. En effet, les compétiteurs de la France s'appuient sur des stratégies informationnelles dédiées qui visent à décrédibiliser l'État central auprès des populations françaises des Outre-mer. Le ministre de l'intérieur Gerald Darmanin a ainsi dénoncé en mai 2024 de multiples opérations d'ingérences de l'Azerbaïdjan dans la politique en Nouvelle-Calédonie[122], au prétexte du soutien au combat contre le néocolonialisme français. Cela a conduit le gouvernement français à décréter l'état d'urgence et à bloquer l'application TikTok, principal vecteur de propagation des messages cherchant à aggraver les tensions sociales. Il en va de même à Mayotte, dont la souveraineté française est contestée à la France par l'Union des Comores. La Russie et la Chine sont ainsi particulièrement actives dans leur soutien aux revendications comoriennes, sur le plan diplomatique et dans la sphère informationnelle, là encore au prétexte du combat contre le néocolonialisme français[123]. Il s'agit vraisemblablement là de stratégies de moyen terme cherchant à attenter à la cohésion nationale et à susciter *a minima* des troubles civils, voire jusqu'à une dislocation de l'unité nationale. L'objectif est de remettre en

121. Voir l'exemple récent des opérations après le cyclone Chido ou encore de la lutte contre l'immigration clandestine à Mayotte.
122. D. Leloup, « Nouvelle-Calédonie : des opérations d'ingérence de l'Azerbaïdjan qui n'expliquent pas tout », *Le Monde*, 16 mai 2024.
123. C. Lalanne, « Mayotte, Comores, Madagascar… Les agents de Poutine en mission commandée », *L'Express*, 28 avril 2024.

cause le positionnement de la France, dans l'environnement régional de chacun de ses Outre-mer, et plus largement sur la scène internationale, en dénonçant son pseudo-néocolonialisme.

Le deuxième type de menaces est celui du coup de force instrumentalisé sur des territoires isolés, cherchant à exploiter la faiblesse du dispositif permanent des forces de souveraineté. En abusant de leur influence, les compétiteurs stratégiques de la France peuvent en effet chercher à inciter les États contestant la légitimité de la souveraineté française à mener une opération coup de poing sur des territoires isolés revendiqués, en s'appuyant sur l'effet de surprise et le fait accompli, et en tablant sur le soutien de l'État parrain et sur l'absence de réaction militaire française. Cette menace n'est pas nouvelle, mais elle semble exacerbée dans un contexte international de néo-impérialisme, de contestation globale de la position occidentale, et de guerre hybride.

Enfin, l'instrumentalisation des flux migratoires, à l'instar de ce que le groupe Wagner est accusé par le gouvernement italien d'avoir fait en Afrique[124], est un mode d'action envisageable pour tenter de décrédibiliser le gouvernement français dans les Outre-mer.

La réponse à ces menaces passe par la définition d'une stratégie contre-informationnelle spécifique pour chacun des territoires ultramarins français, afin de mettre en lumière et de déconstruire systématiquement les discours subversifs auprès des populations locales. Cela suppose également un dialogue politique renforcé avec les pays voisins des Outre-mer français contestant directement la légitimité de la souveraineté française sur ces territoires, en vue de promouvoir un règlement pacifique des disputes. Le dialogue doit aussi être nourri avec toutes les forces politiques locales, y compris les plus radicales (autonomistes, indépendantistes, …). Enfin, cela suppose la mise en place de politiques de résilience économiques et sociales afin de répondre par anticipation aux griefs les plus sérieux, qui pourraient à défaut servir de base pour l'instrumentalisation par une puissance étrangère.

En outre, l'environnement militaire et civil des Outre-mer français est principalement maîtrisé à l'échelon régional, au niveau préfectoral civil et opératif militaire. Il est donc également nécessaire de renforcer le dispositif militaire permanent de souveraineté, tant en termes de capacités de renseignement, de commandement et de réactivité/mobilité des forces. L'objectif à rechercher est de ne pas se faire surprendre par les manœuvres instrumentalisées par nos compétiteurs, d'afficher sans ambiguïté la détermination de la France à assumer sa souveraineté sur chaque partie de son territoire ultramarin, et d'être en mesure de contrer immédiatement toute tentative de fait accompli.

124. N. Squires, « Italy Claims Wagner Mercenaries Behind Latest Migrant Wave », *The Telegraph*, 13 mars 2025.

Repenser le rôle de la réserve dans la défense opérationnelle du territoire

La résurgence de la menace militaire en Europe et la guerre hybride menée par la Russie contre les sociétés européennes remettent en lumière la question de la protection du territoire national.

Pour la France, puissance nucléaire située à l'ouest de l'Europe, l'enjeu semble moins d'être en mesure de faire face à une invasion armée de masse que de se préparer à faire face à des actes déstabilisateurs sur le territoire national, *a fortiori* dans le cadre d'un engagement de haute intensité contre un adversaire étatique. Au regard du panel de modes d'action mis en œuvre par la Russie dans le cadre de sa guerre hybride, il s'agirait de prévenir des actes de sabotages ou d'agression physique en renforçant la protection des sites sensibles, militaires mais également civils soutenant l'effort de guerre. Il s'agirait également d'être en mesure d'appuyer les forces de maintien de l'ordre et de sécurité civile pour faire face à d'éventuelles actions subversives visant à perturber le bon fonctionnement des institutions ou l'effort de guerre. Il s'agirait enfin de se prémunir contre d'éventuelles attaques indirectes (attaques de drones, frappes de missiles dans la profondeur) contre le territoire national, menées par des *proxies* ou des agents sous couvert. Il est vraisemblable que cet effort concernerait assez largement l'ensemble du territoire national.

Dans ce contexte, il apparaît nécessaire pour la France de disposer d'une capacité de défense opérationnelle du territoire [125] moderne, coordonnée avec les capacités complémentaires de la gendarmerie dans le domaine de la défense intérieure. Pour le ministère de la Défense, le concept de DOT reste en effet pertinent avec la professionnalisation des armées, même si, dans le contexte post-guerre froide, sa mise en œuvre n'est envisagée qu'en cas de crise extrême[126].

Néanmoins, suite à la suspension du service militaire en 1997 et après la suppression de 54 000 postes dans le cadre de la LPM de 2008 afin de financer la modernisation de l'appareil de défense[127], l'effectif des armées françaises professionnelles, hors gendarmerie, se monte ainsi aujourd'hui à 200 000 hommes, auxquels s'ajoutent 41 000 réservistes, à comparer au nombre de 470 500 hommes en 1989. Ce format ne permet pas de combiner un engagement à l'extérieur avec un engagement significatif sur le

125. Notion définie dans le Code de la défense (article R.1421-1) : la défense opérationnelle du territoire (DOT) « concourt au maintien de la liberté et de la continuité d'action du Gouvernement, ainsi qu'à la sauvegarde des organes essentiels à la défense de la nation ».
126. *Réponse du ministère de la Défense à la question parlementaire écrite n° 14722 – Définition des notions de défense du territoire et de défense opérationnelle du territoire*, Assemblée nationale, mai 1999.
127. *Rapport d'information du groupe de travail sur le programme 212 de la commission des Affaires étrangères et de la Défense du Sénat*, Paris, Sénat, 2023.

territoire national, au-delà de ce qui est déjà engagé dans le dispositif Sentinelle. La LPM 2019-2025 fixe un contrat opérationnel qui prévoit un échelon national d'urgence à 5 000 hommes, dont une Force interarmées de réaction immédiate (FIRI) de 2 300 hommes, projetable à 3 000 km de l'Hexagone, dans un délai de sept jours. Ce dispositif a toutefois été pensé dans une optique de projection, dans le cadre d'une intervention hors du territoire national (à l'étranger ou dans les Outre-mer). Ces forces sont par ailleurs peu coutumières de la défense du territoire, pour laquelle elles ne sont pas entraînées.

En parallèle de la réduction des effectifs des forces armées, le lien obligatoire entre le citoyen et la nation en armes s'est considérablement amoindri. La journée obligatoire d'appel et de préparation à la défense, instaurée dans le cadre de la réforme du service national de 1997 et renommée journée Défense et Citoyenneté en 2011, ne dure plus qu'une demi-journée depuis août 2024.

Il s'agit donc de revenir à un modèle où la défense de la société démocratique ne passe pas forcément que par le militaire de l'armée professionnelle au format restreint, mais aussi par le citoyen, éventuellement en armes. L'exemple des nations confrontées à une menace existentielle, telles que l'Ukraine, Israël ou Taïwan, illustre cette réalité, dont les pays européens commencent à reprendre conscience.

Il existe deux types de réponses pour redonner de l'épaisseur à la capacité de défense du territoire sans augmenter les effectifs de l'armée professionnelle : le recours à la conscription, totale ou partielle/sélective, ou le recours à des forces de réservistes.

Confrontée à la menace russe, la Lettonie a réintroduit un service militaire obligatoire pour les hommes en 2023. Taïwan a ramené son service militaire obligatoire de quatre mois à un an en 2024. La Norvège, la Suède et le Danemark successivement depuis 2015 ont, eux, opté pour l'instauration d'une conscription sélective. En Norvège, par exemple, elle ne retient, en 2024, qu'environ 9 000 jeunes Norvégiens, soit 10 % de la classe d'âge concernée par la conscription, tous ou presque des volontaires. La conscription y est en effet devenue une forme appréciée de valorisation et de démarcation auprès de futurs employeurs. Les volontaires sont donc plus nombreux que les places disponibles.

D'autres pays, tels que les États-Unis ou la Finlande, s'appuient eux largement sur des forces de réservistes pour leur défense territoriale. La Garde Nationale américaine compte ainsi 430 000 personnes, dont la majorité sont des réservistes. La Finlande entretient un vivier allant jusqu'à 900 000 réservistes pour une population d'environ 5,6 millions d'habitants, en plus du service militaire obligatoire pour les hommes. La résistance ukrainienne face à l'agression russe depuis février 2022 a montré la pertinence du concept de forces de défense territorialisées appuyées sur la

réserve. Taïwan envisage le recours à une telle organisation dans la perspective d'une possible invasion par les forces armées chinoises[128].

Pour doter la France d'une capacité de défense de son territoire, dont le juste format reste à déterminer, la question du modèle le plus adapté se pose. Si la solution de faire appel à des réservistes apparaît comme la moins onéreuse au premier abord, elle ne semble pas pleinement satisfaisante dans le portage actuel. L'un des freins à l'emploi de la réserve pour des missions de protection est le délai de montée en puissance des régiments de réserve (lié à la disponibilité des réservistes, à l'absence de mécanisme contraignant). Par ailleurs, le faible taux d'encadrement des forces d'active rend cette montée en puissance difficile.

Les réserves opérationnelles de premier niveau (RO1[129]) du ministère des Armées ont été intégrées à la Garde nationale, recréée en octobre 2016. Si elles représentent un effectif conséquent (41 000 environ pour le ministère des Armées), elles ne disposent pas réellement d'une doctrine d'emploi cohérente ou coordonnée, les réservistes étant dans les faits employés par leur armée ou service de rattachement en appui des forces d'active. Le secrétariat général de la Garde nationale a essentiellement un rôle de liaison entre l'institution et les employeurs civils des réservistes. En outre, l'ancrage territorial de ces réservistes militaires, c'est-à-dire leur répartition et leur emploi sur l'ensemble du territoire métropolitain, n'est pas intégral[130]. Les réserves opérationnelles de 2e niveau (RO2[131]), en revanche, sont bien réparties sur le territoire. Si elles totalisent 68 000 hommes sur le papier, dans la pratique, les modalités de rappel ne sont pas assez contraignantes et peu d'anciens militaires y répondent. De plus, ces réservistes se sont progressivement transformés en supplétifs des forces d'active au gré des réductions de format, au point qu'elles sont souvent nécessaires au bon fonctionnement de certaines unités militaires, notamment dans le soutien et les états-majors. Le ministère des Armées s'est fixé pour objectif de monter l'effectif de la réserve militaire à 100 000 hommes, mais force est de constater que de nombreux freins existent quant à l'employabilité de ces forces dans la société moderne[132].

En complément, le Service national universel (SNU), lancé en 2019, confronté à la démesure de l'ambition d'intégrer une classe d'âge, soit 850 000 jeunes, à un dispositif général nécessitant des infrastructures, des

128. L. Hsi-Min and M. A. Hunzeker, « The View of Ukraine from Taiwan: Get Real About Territorial Defense », warontherocks.com, 15 mars 2025.
129. La réserve opérationnelle de niveau 1 (RO1) désigne les réservistes militaires ayant souscrit un engagement à servir dans la réserve, contrat d'une durée de 1 à 5 ans, qui les amène à réaliser en moyenne 37,5 jours d'activité par an.
130. M. Bessot, « L'ancrage de la Garde nationale sur le territoire : quel bilan ? », *Notes de l'Ifri*, Ifri, août 2021.
131. La réserve opérationnelle de niveau 2 (RO2) concerne les militaires ayant quitté l'institution, durant les 5 ans suivant la fin de leur service.
132. « LPM 2024-2030 : objectif 100 000 réservistes », *Ministère des Armées*, 22 novembre 2022.

moyens humains et des crédits qui font défaut, peine à redéfinir ses objectifs[133]. Il a fait l'objet d'un rapport de la Cour des comptes en 2024 qui jugeait le dispositif onéreux, mal planifié et, avec des objectifs flous et à géométrie variable selon l'actualité. Ce dispositif va donc vraisemblablement évoluer, à la demande du président de la République[134].

Le Cercle Maréchal Foch, cercle de réflexion composé d'anciens officiers généraux ayant vocation à contribuer à la réflexion nationale sur les enjeux de sécurité et de défense, proposait en 2023 le rétablissement d'un service militaire volontaire restreint, limité à une vingtaine de milliers de recrues sélectionnées par an, pour fournir le complément de forces nécessaires[135], à l'instar des pays nordiques. Pour ce volume, il estimait le coût de ce dispositif à moins de 300 millions d'euros par an, auquel il convient d'ajouter le coût de l'encadrement d'active, celui de la vie courante, de l'entraînement et de l'équipement (dont une bonne part peut initialement venir des parcs stockés). Le coût global estimé serait de l'ordre d'un milliard d'euros par an, investissement somme toute modéré au regard de la montée de la menace et de la nécessaire tension qui existerait sur la ressource militaire en cas de besoin simultané d'activation de la défense opérationnelle du territoire et d'engagement des forces armées à l'extérieur.

Un sondage du centre de réflexion Destin commun réalisé en mars 2025 révèle ainsi que 61 % des Français sont « favorables au rétablissement d'une forme de service militaire obligatoire ». L'option de recourir à une forme de service militaire sélectif, sur une base privilégiant le volontariat, mérite donc d'être considérée pour répondre à la problématique de la défense du territoire. En outre, service national et réserve ne sont pas exclusifs. L'exemple des pays nordiques montre que le service national constitue un bon vivier pour un recrutement ultérieur dans la réserve militaire.

Quel que soit le format retenu, face à la montée de la menace, il est nécessaire pour la France de repenser son dispositif de défense territoriale en profondeur, en en déterminant l'envergure, la nature et le concept d'emploi, et en le dotant des ressources, des infrastructures et des équipements nécessaires à sa préparation opérationnelle.

133. F. Wolf, « Faut-il remplacer le SNU par une conscription choisie en France ? », Blog METADéfense, 13 septembre 2024.
134. P. Barcelon, « Service national universel "vitaminé" à 600 millions d'euros, service militaire obligatoire à près de 15 milliards… Les scénarios du haut-commissariat au Plan », France Info, 5 mai 2025.
135. Cercle Maréchal Foch, « Une urgence : reconstruire la défense opérationnelle du territoire », Theatrum Belli, 2 janvier 2023.

Repenser en zone grise l'articulation entre protection et dissuasion

Les sociétés européennes démocratiques, fondées sur les lois, la liberté d'expression et la confiance sont sur la défensive face à des compétiteurs désinhibés et agressifs, déterminés à éprouver leur résilience en abusant de ces principes. Considérant l'étendue et la diversité du panel de menaces, une posture de protection exclusivement défensive semble au mieux partiellement efficace, au pire vouée à l'échec en laissant l'initiative et le choix des armes à l'adversaire. C'est d'autant plus vrai si l'on s'inscrit dans une perspective de menace sur le long terme.

Pour la France, en particulier, l'émergence de menaces de nature militaire contre le territoire national, vraisemblablement cantonnées sous le seuil nucléaire, impose de repenser plus globalement la notion de dissuasion.

Conceptuellement, on distingue deux types de postures dissuasives : la dissuasion par déni et la dissuasion par représailles[136]. Les deux ne sont pas exclusives l'une de l'autre. La dissuasion par déni recouvre des stratégies de défense passive ou réactives, fondées sur la promotion du respect du droit, et qui reposent sur la consolidation des dispositifs de protection dans les champs matériels et immatériels et le renforcement de la résilience des systèmes et des organisations. La dissuasion par représailles promeut une défense qui se veut préventive en faisant peser la menace de rétorsions sur celui qui serait incité à perpétrer des actes malveillants. L'idée est d'imposer à l'adversaire une contrepartie à l'emploi des actions hybrides qui, dans leur nature, constituent une stratégie de déstabilisation peu coûteuse tant sur le plan des moyens que politiquement.

Le contexte géopolitique et sécuritaire actuel, notamment les menaces dans le champ immatériel, milite pour ce type de postures, adossée à une stratégie nationale de dissuasion des actes hybrides crédible et assumée. Cela passe nécessairement par la consolidation de la capacité à mieux caractériser et attribuer les actions hybrides, combinée à la volonté politique d'employer des mesures de rétorsion proportionnées et efficaces contre l'auteur des agressions.

À présent que la menace est bien identifiée et caractérisée, dans ses différentes formes, il est temps pour les pays démocratiques de développer un panel large et gradué de mesures de rétorsion, immatérielles mais aussi matérielles, face aux actions déstabilisatrices. Il s'agit également de développer l'arsenal répressif, contre les États et contre leurs agents, afin de

136. A. Radin, A Demus et K. Marcinek, « Understanding Russian Subversion », RAND Corporation, 18 février 2020.

renforcer la puissance dissuasive. Enfin, il est nécessaire de se préparer à en faire usage, de manière claire, assumée et désinhibée.

L'objectif est double : signifier sans ambiguïté à la Russie, la Chine et les autres impétrants perturbateurs la volonté de la France à protéger ses intérêts et les exposer à une riposte, mais aussi communiquer vers l'intérieur la détermination de la France à protéger sa population contre ce type d'agissements, en vue de reconstruire la confiance qui est le fondement de la résilience de la société.

Ce retour de la force dans l'arsenal des options politiques nationales hors temps de guerre et comme étalon des relations avec les pays sans scrupule, notamment la Russie, doit être compris non pas comme un risque d'accélérer la montée aux extrêmes, mais bien comme une option à même de les dissuader et de maintenir la confrontation dans des proportions raisonnables, notamment si l'on s'en tient à une logique de proportionnalité. L'objectif à rechercher, nonobstant, est d'inverser le rapport de force et d'être en mesure de garder la maîtrise, voire de dominer l'escalade en zone grise dans le cadre de la confrontation.

Enfin, cette posture de dissuasion plus active mérite de faire l'objet d'un dialogue stratégique, ou mieux d'être coordonnée avec des pays aux vues similaires, notamment au sein de l'UE, afin tant d'en asseoir la légitimité que d'en renforcer la puissance dissuasive. Cette conscience de la nécessité d'une approche plus active pour dissuader la Russie de poursuivre ses actions déstabilisatrices émerge en effet au sein de l'UE notamment[137]. Il est donc vraisemblable qu'elle recevrait un écho favorable de la part de bon nombre de pays européens.

137. S. Everts et O. Ditrych, « Unpowering Russia: How the EU Can Counter and Undermine the Kremlin », *Chaillot Paper*, European Union Institute for Security Studies (EUISS), 22 mai 2025 ; S. Everts, « Resilience Alone Is Not Enough in the Hybrid War with Russia », EUISS 19 février 2025.

Conclusion

L'évolution du contexte géostratégique, avec le retour de stratégies de puissance mises en œuvre par des acteurs désinhibés, doit amener à questionner le dispositif de protection du territoire national post-guerre froide, fruit de décennies d'engagements extérieurs et de lutte contre le terrorisme.

La nature des menaces auxquelles la France est confrontée n'a pas connu de rupture fondamentale ces dernières années, à l'exception près de l'émergence de systèmes d'armes productibles en masse et à faible coût, qui font peser un risque de saturation des défenses militaires. La menace « classique » s'est toutefois étendue à de nouveaux espaces de confrontation, jusqu'à présent relativement préservés. Pour autant, il s'agit de ne pas se leurrer sur la réalité de cette menace et la volonté des compétiteurs stratégiques d'user de l'ensemble du panel de nuisance pour déstabiliser les sociétés européennes sur le long terme, au-delà des gains immédiats. Les incidents qui surviennent partout en Europe doivent être compris comme des coups de sonde visant à éprouver l'état de préparation, la robustesse, la résilience, et *in fine* la détermination de ces sociétés.

Si la France dispose d'une organisation robuste pour la protection de ses activités critiques, matérialisée par les dispositifs réglementaires de sécurité pilotés par le SGDSN ainsi que par les postures permanentes de protection du territoire, cela ne doit pas occulter l'existence de vulnérabilités que ses compétiteurs ne manqueront pas de chercher à exploiter le moment opportun. Il peut s'agir de ses limites en matière de défense sol-air, de sa perméabilité à la désinformation et à l'agitation sociale, des fragilités spécifiques de ses territoires ultramarins, ou encore du manque d'outils vis-à-vis d'actes malveillants dans les espaces communs insuffisamment couverts par le droit.

L'Iran, la Chine, et dans une moindre mesure la Russie, restent encore focalisés sur d'autres priorités que la France, qui les conduisent à n'agir sur le territoire national que de manière ponctuelle et diffuse. Toutefois, les germes d'une possible tentative de déstabilisation plus massive dans le cadre d'un conflit plus direct sont là. L'entre-deux actuel doit donc impérativement être mis à profit pour identifier et réduire les vulnérabilités existantes, en exploitant pleinement les leçons de leurs agissements et de ceux qui seraient tentés de leur emboîter le pas.

Primus inter pares, dans une période de conflictualité exacerbée, il s'agit de reconstituer la capacité opérationnelle des armées à s'engager sur le territoire national pour y assurer la défense militaire, en y consacrant les

ressources nécessaires. Il est question, en cas de durcissement du contexte stratégique pour la France, d'être en mesure d'agir en complément des forces de première ligne afin de garantir la défense de l'arrière. Le temps long dans lequel semble devoir s'inscrire cet effort impose toutefois d'en peser finement les modalités, afin d'éviter un phénomène d'usure des forces dans un contexte de retour de la guerre en Europe et de préparation à un éventuel engagement de haute intensité.

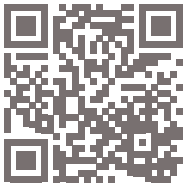
Enfin, prenant acte de la volonté des compétiteurs de mettre à bas les sociétés occidentales, de l'affaiblissement d'un modèle mondial de gouvernance fondé sur le droit, et de l'émergence de menaces stratégiques sous le seuil nucléaire, il convient de reconnaître que la protection seule ne suffit pas (au sens d'une stratégie exclusivement défensive). Il s'agit sans doute d'opter pour une posture de dissuasion conventionnelle plus active appuyée par un panel d'options de rétorsion graduées afin d'inverser le rapport de force et de faire peser sur l'agresseur le coût de ses actes. À défaut, il est vraisemblable que les compétiteurs de la France l'interpréteront comme un aveu de faiblesse et une incitation à poursuivre leurs agissements, tout en raffinant leurs méthodes et en allant toujours plus loin dans la palette des actions envisageables. Au regard de la contradiction possible entre le respect du droit et certaines déclinaisons d'une telle posture, celle-ci méritera de faire l'objet d'un dialogue entre partenaires stratégiques partageant les mêmes valeurs, ou mieux d'une concertation, pour en renforcer la cohérence, la robustesse, et le caractère dissuasif.

Il convient également de considérer que toute protection est par essence imparfaite et, partant, de consolider la résilience de la nation mais aussi de la société française, en la préparant activement aux potentielles matérialisations résurgentes de cette conflictualité sur le territoire national. Les exemples récents montrent que cette résilience est aussi individuelle que collective, tant psychologique qu'organisationnelle, et qu'elle passe par la pleine adhésion et implication active du citoyen dans l'effort national de crise ou de guerre. C'est donc l'ensemble de ces aspects qui doivent être considérés au travers de la stratégie nationale de résilience.

Enfin, la préservation du territoire national est l'essence de la souveraineté. Aussi, nonobstant les nombreuses priorités stratégiques concurrentes, actuelles et à venir, la volonté d'autonomie stratégique de la France ne semble pouvoir faire l'impasse de l'enjeu de la protection et de la résilience face à une menace avérée et durable, ni d'y consacrer les ressources nécessaires dans un contexte où celle-ci est directement ciblée.

Les dernières publications des Focus stratégiques

- Amélie Férey, « Sous le feu des normes. Comment encadrer sans désarmer la défense européenne ? », *Focus stratégique*, n° 125, Ifri, avril 2025.
- Jonathan Caverley, Ethan Kapstein, Léo Péria-Peigné and Élie Tenenbaum, « Une base industrielle de défense transatlantique ? Deux analyses contrastées », *Focus stratégique*, n° 124, Ifri, mars 2025.
- Léo Péria-Peigné et Amélie Zima, « Pologne, première armée d'Europe en 2035 ? Perspectives et limites d'un réarmement », *Focus stratégique*, n° 123, Ifri, février 2025.
- Adrien Gorremans, avec la participation de Jean-Christophe Noël, « L'avenir de la supériorité aérienne. Maîtriser le ciel en haute intensité », *Focus stratégique*, n° 122, Ifri, janvier 2025.
- Héloïse Fayet et Léo Péria-Peigné, « La frappe dans la profondeur : un nouvel outil pour la compétition stratégique ?», *Focus stratégique*, n° 121, Ifri, novembre 2024.
- Jérémy Bachelier et Mélissa Levaillant, « L'Inde, un partenaire incontournable pour la France dans l'Indopacifique ? », *Focus stratégique*, n° 120, Ifri, juillet 2024.
- Élie Tenenbaum et Amélie Zima, « Retour à l'Est : la France, la menace russe et la défense du 'Flanc Est' de l'Europe », *Focus stratégique*, n° 119, Ifri, juin 2024.
- Pierre Néron-Bancel et Guillaume Garnier, « 'De l'autre côté de la colline' : atouts et fausses promesses de la transparence du champ de bataille », *Focus stratégique*, n° 118, Ifri, mai 2024.
- Jérémy Bachelier et Céline Pajon, « La France dans l'Indopacifique : pour une posture stratégique pragmatique », *Focus stratégique*, n° 117, Ifri, octobre 2023.
- Élie Tenenbaum et Léo Péria-Peigné, « Zeitenwende : la Bundeswehr face au changement d'ère », *Focus stratégique*, n° 116, Ifri, septembre 2023.
- Guillaume Garnier, « La France dans l'OTAN : de l'allié difficile au contributeur essentiel », Focus stratégique, n° 115, Ifri, juin 2023.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org