INSTITUT Montaigne

SÉCURITÉ NATIONALE

Protéger nos intérêts vitaux

SE PROTÉGER

les REPÈRES de MONTAIGNE

Les États ne s'affrontent pas seulement par moyens militaires et les menaces se développent sur plusieurs fronts et sous de multiples formes.

Il nous faut repenser notre stratégie de sécurité nationale pour durablement sauvegarder nos intérêts vitaux.

les REPÈRES de MONTAIGNE

SÉCURITÉ NATIONALE

La sécurité nationale est la mission primordiale de l'État : elle permet de protéger les individus, les biens et le système de valeurs de la nation et mobilise des moyens variés, humains et technologiques. Sans sécurité nationale, pas de liberté. Or le niveau de la menace contre nos intérêts vitaux est plus élevé que jamais, qu'il s'agisse du risque militaire, des attaques contre notre économie et nos infrastructures, en particulier cyber, et de la stabilité de notre démocratie. Même si ses modalités sont sensibles et parfois couvertes par le secret, la sécurité nationale n'en relève pas moins d'une politique publique appelant une stratégie globale pour définir ses finalités et rationaliser ses moyens.

Définition

La sécurité nationale concerne la protection physique des citoyens français, la protection de l'activité économique du pays, base de notre puissance et de notre prospérité, et la protection des instruments de notre indépendance.

Mission prioritaire de l'État, la sécurité nationale mobilise de manière planifiée les différents moyens (militaires, diplomatiques, financiers, juridiques etc.) destinés à la rendre effective en cas de menace anticipée ou subie.

Un document stratégique (Livre blanc, revue nationale stratégique) présente un état de la menace, les objectifs stratégiques et le modèle d'armée à atteindre. Ce document se décline en une loi de programmation militaire pluriannuelle (d'une durée de 7 ans actuellement) qui fixe les priorités et la trajectoire cible pour le budget des armées. Enfin, chaque année, une loi de finances initiale (LFI) fixe les crédits pouvant être dépensés pour la mission défense.

Cette note fait partie d'une collection de 25 notes thématiques publiées par l'Institut Montaigne pour l'élection présidentielle 2027 :

Les repères de Montaigne
25 recommandations pour la France

L'Institut Montaigne traite ici une vingtaine de thèmes interdépendants jugés cruciaux. Ils s'organisent autour des 4 ambitions qui doivent animer une campagne présidentielle :

- ↘ **Protéger la nation**
- ↘ **Créer de la richesse pour tous**
- ↘ **Garantir le vivre ensemble**
- ↘ **Mettre en œuvre efficacement les politiques publiques**

Par souci de priorisation, certains thèmes ne font pas l'objet de note dédiée malgré leur importance (culture, sport, politique de la ville, transports, etc.).



SE PROTÉGER

SÉCURITÉ NATIONALE
Protéger nos intérêts vitaux

SÉCURITÉ ÉCONOMIQUE
Renforcer notre résilience

DÉFENSE NATIONALE
Faire face aux nouvelles menaces

POLITIQUE ÉTRANGÈRE
Assurer la crédibilité et le rayonnement de la France

FRANCE-EUROPE
Développer nos intérêts communs

SÉCURITÉ INTÉRIEURE
Garantir la sécurité sur l'ensemble du territoire

JUSTICE
Réconcilier les Français avec leur justice



CRÉER DE LA RICHESSE

COMPÉTITIVITÉ
Combattre à armes égales

TRAVAIL ET POUVOIR D'ACHAT
Vivre mieux de son travail

INNOVATION ET TECHNOLOGIES
S'adapter en continu

ÉDUCATION
Une école qui instruit et émancipe

ÉNERGIE
Produire une énergie compétitive, souveraine et durable

AGRICULTURE
Relancer notre modèle agricole



VIVRE ENSEMBLE

ACCÈS AUX SOINS
Être bien soigné partout en France

RETRAITE
Garantir un système équitable et pérenne

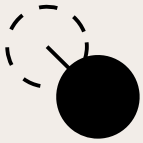
LOGEMENT
Rendre le logement accessible

POLITIQUE FAMILIALE
Répondre aux nouvelles réalités

PAUVRETÉ ET PRÉCARITÉS
Agir pour les plus fragiles

IMMIGRATION ET INTÉGRATION
Piloter, intégrer et apaiser

ENVIRONNEMENT ET CLIMAT
Faire de la transition écologique une force



METTRE EN ŒUVRE

RÉFORME DE L'ÉTAT
Rationaliser et responsabiliser

FONCTION PUBLIQUE
Moderniser pour mieux servir

DÉMOCRATIE
Restaurer la confiance politique

FINANCES PUBLIQUES
Financer nos ambitions

DÉBUT DE MANDAT
Passer à l'action

SOMMAIRE

p.09

MIEUX COMPRENDRE

p.10
En quelques chiffres
|
p.11
Comment en est-on arrivé là ?
|
p.14
Que se passe-t-il si on ne fait rien ?
|
p.15
Nos atouts
|
p.16
Vu de nos territoires
|
p.18
Et ailleurs ?
|
p.20
Le champ de contraintes
|
p.22
Les idées reçues du débat

p.24

DANS LE DÉBAT

p.28
Idée N°1
|
p.36
Idée N°2

p.50

LA RECOMMANDATION DE MONTAIGNE

p.48
Nos principes d'arbitrage
|
p.51
Pourquoi cette voie ?
|
p.56
Feuille de route
|
p.58
Coût et ressources
|
p.59
Indice d'acceptabilité

p.60

SOURCES

LES REPÈRES DE MONTAIGNE

PARTIE 1

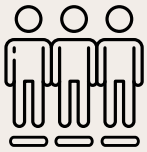


MIEUX COM-PRENDRE

EN QUELQUES CHIFFRES

1 Md€
BUDGET DE LA **DGSE**
(sécurité extérieure) en 2025,
le plus haut jamais alloué.

274 FRANÇAIS
tués et 800 blessés dans
des attentats sur notre territoire
depuis 10 ans. C'est un enjeu
de **sécurité physique**.



+66 %
Hausse des effectifs de la
DGSI (sécurité intérieure)
depuis 2014.

800 tentatives
hostiles contre des entreprises
stratégiques, un chiffre qui a doublé
depuis 2020. C'est un enjeu de
sécurité économique.

120 MD €
LE **COÛT ESTIMÉ DE LA CYBERCRIMINALITÉ** POUR L'ÉCONOMIE FRANÇAISE EN 2022.
43 MILLIONS DE **COMPTES UTILISATEURS FRANÇAIS COMPROMIS** AU 1ER SEMESTRE 2026.



Qu'est-ce que cela dit ?

MALGRÉ DES MOYENS EN HAUSSE, LES IMPACTS SE MULTIPLIENT

La mutation des menaces et leur intensification dans le champ économique et individuel a appelé une augmentation inédite des moyens **(les effectifs du Secrétariat général de la défense et de la sécurité nationale ont été augmentés de 52% depuis 2019)**. Mais elle n'a pas entraîné une réflexion approfondie sur la stratégie globale à mettre en œuvre. Pour répondre à l'impératif de sécurité de manière efficace, il faut non seulement adapter les moyens, il faut aussi et surtout adapter notre modèle d'organisation pour traiter de manière plus globale des menaces multi-champs.

COMMENT EN EST-ON ARRIVÉ LÀ ?

UN HANDICAP HISTORIQUE

Les grands systèmes de sécurité nationale occidentaux (États-Unis, Royaume-Uni) ont été fondés sur les acquis de la Seconde Guerre mondiale et l'aguerrissement face à l'adversaire soviétique pendant la Guerre froide. Déstabilisé par la défaite de 1940 et la collaboration, occupé par la reconstruction nationale, la décolonisation (Indochine, Algérie), puis la promotion d'une troisième voie internationale, l'appareil français ne s'aguerrit pas alors au même niveau que ses alliés.

Définition

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN)

Service d'environ 1300 personnes placé sous l'autorité du Premier ministre et chargé de coordonner les différentes actions en matière de défense et de sécurité nationale. Le secrétariat général est composé de directions en charge de la gestion du secret défense, de la planification des crises, du contrôle des exportations d'armement, de la veille stratégique. Il dirige également des services opérationnels (protection contre les cyberattaques – ANSSI – et la désinformation – Viginum).

COMPLEXITÉ ET DÉSALIGNEMENT

Le Code de la défense a été révisé en 2009 pour traiter de la sécurité nationale et confirmer la responsabilité du Premier ministre.

Cependant, les différentes dimensions de la sécurité nationale sont réparties entre plusieurs ministères : Défense, Intérieur, Économie, Budget, Affaires étrangères, Justice, Santé, Environnement, Transports, Énergie, Industrie.

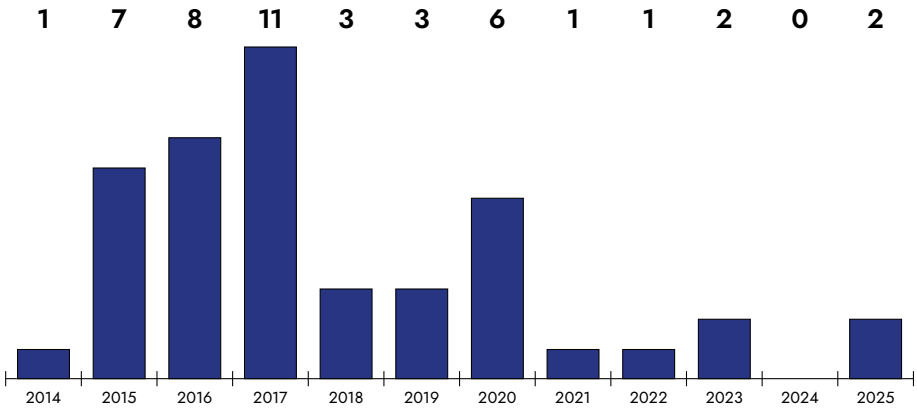
Cet éclatement de l'organisation freine l'élaboration d'une stratégie claire, de long terme et cohérente à même d'anticiper les menaces et non pas simplement d'y répondre. L'absence d'un débat public sur ces questions a entretenu ce défaut de vision stratégique malgré la grande qualité et l'engagement des personnels dédiés.

UN ANGLE MORT DU DÉBAT PUBLIC

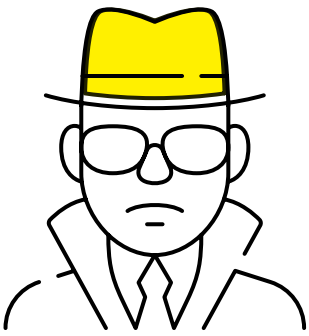
L'existence de la dissuasion nucléaire et l'absence de débat public sur ces questions de sécurité nationale ont laissé penser que la sécurité nationale était avant tout une affaire de spécialistes. Dans cette logique, le modèle de sécurité nationale n'est débattu que lors d'échecs dramatiques (attentats de M. Merah, coup d'État au Mali, AUKUS, invasion de l'Ukraine…).

Or, à l'heure où se redéfinit le nouvel ordre mondial et où les menaces visent tout autant les installations étatiques que les acteurs privés et les citoyens, il est indispensable de revoir les modalités de notre sécurité nationale et d'ancrer le choix de société qu'elle entend défendre dans le débat démocratique afin d'adapter nos réponses mais également nos ambitions.

Nombre
d'attaques terroristes sur le territoire français



41
Agents russes
agissant sur notre territoire sous un statut diplomatique contre nos intérêts de sécurité, expulsés en 2022.



Chronologie

1959 1962

↘ L'ordonnance du 7 janvier 1959 et le décret de 1962

Le texte de 1959 fixe l'architecture de la défense nationale (la sécurité nationale n'est pas encore perçue en tant que telle), qui est complétée par un décret en 1962 qui confie la coordination interministérielle à un secrétariat général (SGDN) relevant du Premier ministre et censé coordonner un ensemble qui inclut la Présidence.

2004

↘ La transposition de 2004

Ces principes d'organisation sont transposés et maintenus dans le Code de la défense : les missions de coordination par les services du Premier ministre sont confirmées.

2009

↘ Le rendez-vous raté de 2009

Lors de la présidentielle de 2007, N. Sarkozy propose une modernisation de notre sécurité nationale et la création d'un Conseil de Sécurité Nationale auprès du président de la République. Mais dans les faits les changements sont superficiels (SGDSN, CDSN), sans réforme du modèle. L'efficacité continue de résider dans une coordination administrative aux dépens d'une vision stratégique.

2009 2026

↘ Les tentatives de correction par ajouts

L'État s'ajuste par ajouts successifs sans proposer une stratégie de sécurité nationale intégrée, et chaque administration continue de développer ses structures :

- sécurité économique : SISSE à Bercy (2016) ;
- lutte antiterroriste : CNRLT à la Présidence (2017), Emap au Ministère de l'Intérieur (2019) ;
- lutte contre la désinformation : Viginum au SGDSN (2021), Sous-Direction Veille et Stratégie au Quai d'Orsay (2022), cellule Anticipation Stratégique et Orientations au Ministère des Armées (2022).

Cette multiplication simultanée aggrave la complexité et l'éclatement du système.

QUE SE PASSE-T-IL SI ON NE FAIT RIEN ?

POUR LE PAYS…

L'incapacité de la France à répondre au bon niveau aux menaces qui pèsent contre elle se traduirait par une perte de souveraineté et un déclassement accéléré vis-à-vis des autres nations : fragilité forte du pays due à une incapacité à résister aux pressions extérieures et intérieures, aux aléas internationaux et aux puissances hostiles (pandémies, guerres, crises climatiques, chantages, pressions économiques et diplomatiques…) ; ou à suivre le rythme des progrès technologiques et opérationnels des autres puissances priorisant leur sécurité sur tout le reste.

POUR LES ENTREPRISES…

Les menaces directes sur les entreprises et la viabilité économique du pays augmenteraient. Non protégées par un cadre sécuritaire stable, les entreprises peuvent devenir des proies faciles pour les puissances hostiles ou conquérantes. Leur dépendance accrue à des fournisseurs étrangers les rendent vulnérables et vassales. Elles n'attireraient plus les investisseurs confiants dans la protection de l'État et des règles économiques dont il est le garant. Elles investiraient ailleurs et délaisseraient le territoire national.

Une progression insuffisante

Des budgets inédits à l'échelle de la nation sont en hausse constante depuis 2015 (+73% du programme 144 entre 2015 et 2026). Ils ne suffisent cependant pas à dissuader nos agresseurs, notamment dans le domaine de guerre hybride (cyberattaques, déstabilisation, désinformation).

Définition

ATTAQUES ÉCONOMIQUES

Les attaques économiques comprennent les menaces physiques (vols, intrusions non autorisées, sabotages), humaines (espionnage stratégique, économique et technologique), informatiques, juridiques *(lawfare)*, capitalistiques et informationnelles.

POUR LES FRANÇAIS…

Le risque serait accru de perdre confiance en l'avenir faute d'un État remplissant son premier devoir, celui de la sécurité et de la projection légitime de ses citoyens dans une trajectoire de paix et de prospérité.

La perte de sens et de cohésion nationale laisserait le pays ouvert aux manœuvres de subversion et de dislocation. Il en résulterait à terme une perte de liberté dans un contexte d'insécurité incontrôlée. L'absence de perspectives économiques fiables aggraverait la perte de prospérité et la pauvreté.

NOS ATOUTS POUR RENVERSER LA TENDANCE

Une prise de conscience réelle existe désormais dans la société française, qui reconnaît la pluralité des formes de la menace, tant militaire qu'économique et sociale. Il y ainsi un consensus politique sur le besoin de réformer notre sécurité nationale.

La tradition centralisatrice française est, en ce domaine, un atout, permettant de définir une stratégie claire et de se donner les moyens nécessaires. La France a une culture stratégique qui sait opérationnaliser, agir et faire beaucoup avec peu. Elle se démarque des autres pays dans la gestion des crises de tout ordre.

En outre, nous sommes reconnus pour être un pays de grande solidarité et d'entraide spontanée qui permet d'augmenter la résilience nationale.



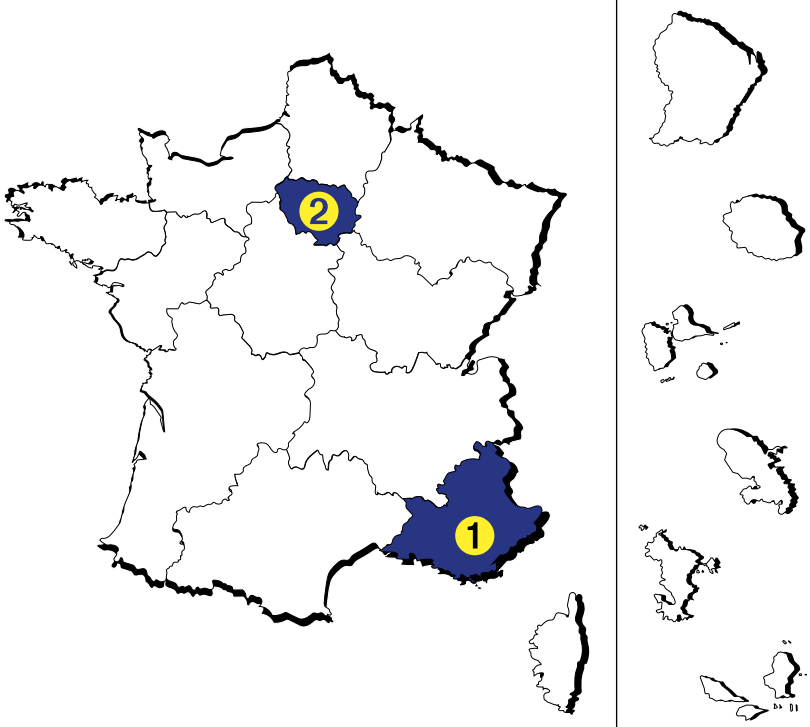
73%

des Français

s'inquiètent des tentatives d'acteurs étrangers visant à influencer l'opinion publique en France

VU DE NOS TERRITOIRES

Parce que les politiques publiques concernent les Français dans toute la France, **l'Institut Montaigne et l'Institut Enterritoires ont souhaité faire entendre le point de vue d'acteurs clés de nos régions** sur les grands enjeux du débat présidentiel.



Plusieurs dizaines d'élus, de responsables économiques, de représentants associatifs ou d'acteurs engagés dans la vie locale nous livrent leur regard et leurs attentes (ci-contre, 2 extraits).



1

Rudy Manna

Délégué national UNSA Police,
président régional PACA Mutuelle MGP

Les menaces ont changé et se croisent de plus en plus : terrorisme, criminalité organisée, cyberattaques, atteintes à nos intérêts économiques ou tentatives de déstabilisation ne peuvent plus être regardés séparément. À Marseille, cette évolution prend une dimension très concrète. Le principal frein reste le cloisonnement : il faut partager l'information, croiser les signaux faibles et raccourcir les circuits, tout en conservant une stratégie nationale forte.

Notre principal atout est notre capacité à nous adapter. La France dispose de compétences et de savoir-faire reconnus, mais aussi d'un maillage territorial permettant une connaissance des réalités locales. Marseille possède une place particulière par son ouverture sur la Méditerranée, sa façade maritime et l'importance des flux. L'opportunité serait de mieux exploiter cette intelligence du terrain et la connecter aux capacités d'analyse et aux moyens technologiques.

Cette logique pourrait être davantage organisée par des rencontres territoriales régulières, sans créer une nouvelle structure administrative. L'objectif serait simple : partager ce qui évolue, croiser les informations, repérer les signaux faibles et savoir rapidement qui peut agir. Il faudrait aussi mieux organiser les retours d'expérience entre territoires. La sécurité nationale doit fonctionner dans les deux sens : du national vers le terrain, mais aussi du terrain vers la décision nationale.



2

Kadir Mebarek

Maire de Melun et avocat
au barreau de Paris

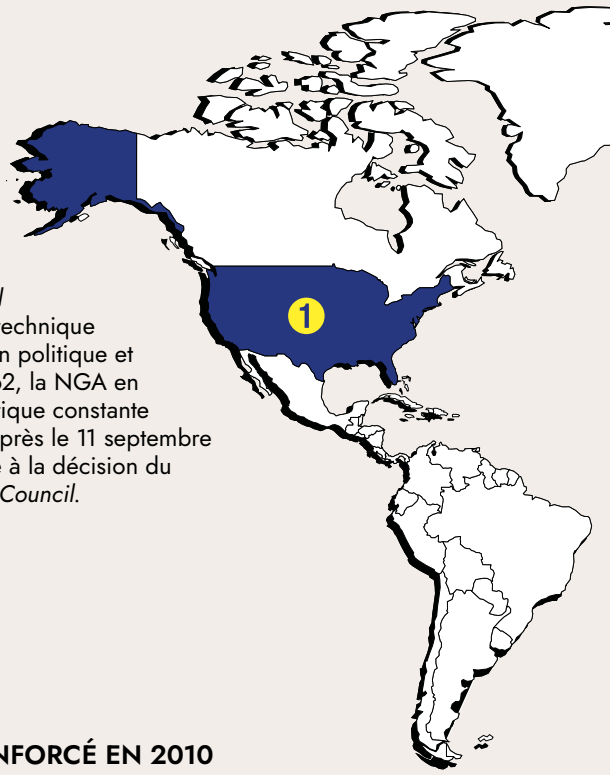
Les menaces contre notre sécurité nationale ne sont plus seulement militaires : elles prennent désormais la forme de cyberattaques, d'actes de malveillance, de désinformation ou d'événements climatiques majeurs qui désorganisent durablement un territoire. L'incendie exceptionnel de la forêt de Fontainebleau en est une illustration : en quelques heures, un sinistre environnemental est devenu une crise de sécurité mobilisant des moyens nationaux, perturbant les transports, menaçant des infrastructures, etc. Les maires sont désormais en première ligne de ces crises hybrides sans toujours être pleinement intégrés à leur anticipation.

La France dispose d'un atout majeur : son maillage territorial. Les communes, les préfectures, les services de secours, les forces de sécurité et les acteurs économiques constituent un réseau de proximité unique en Europe. Encore faut-il considérer les collectivités comme de véritables partenaires de la sécurité nationale.

Melun, ville préfecture, démontre chaque jour que la coordination entre l'État, les collectivités, la justice, les forces de sécurité et les services de secours permet de mieux anticiper les crises. Demain, cette coopération pourrait être renforcée grâce à un partage sécurisé de l'information, à des formations communes et à une meilleure association des élus locaux à la planification des risques.

ET AILLEURS ?

Pour faire face à l'accroissement des menaces multiformes, les États ont renforcé leurs moyens et leur organisation. L'efficacité – c'est à dire la rapidité de réaction et la qualité de la résolution de la crise – est au centre de leur préoccupation. Celle-ci repose très largement sur une organisation intégrée au plus près de la décision exécutive.



1 États-Unis

UN MODÈLE STABLE ET AGUERRI

Le dispositif de sécurité nationale américain a su évoluer depuis le *National Security Act* de 1947, créant une agence technique (la NSA en 1952) pour épauler la décision politique et des agences spécialisées (la NRO en 1962, la NGA en 1996), dans un ensemble mûri par la pratique constante pendant la Guerre froide, et réactualisé après le 11 septembre 2001. Il se conçoit comme un outil d'aide à la décision du président, piloté par le *National Security Council*.

2 Royaume Uni

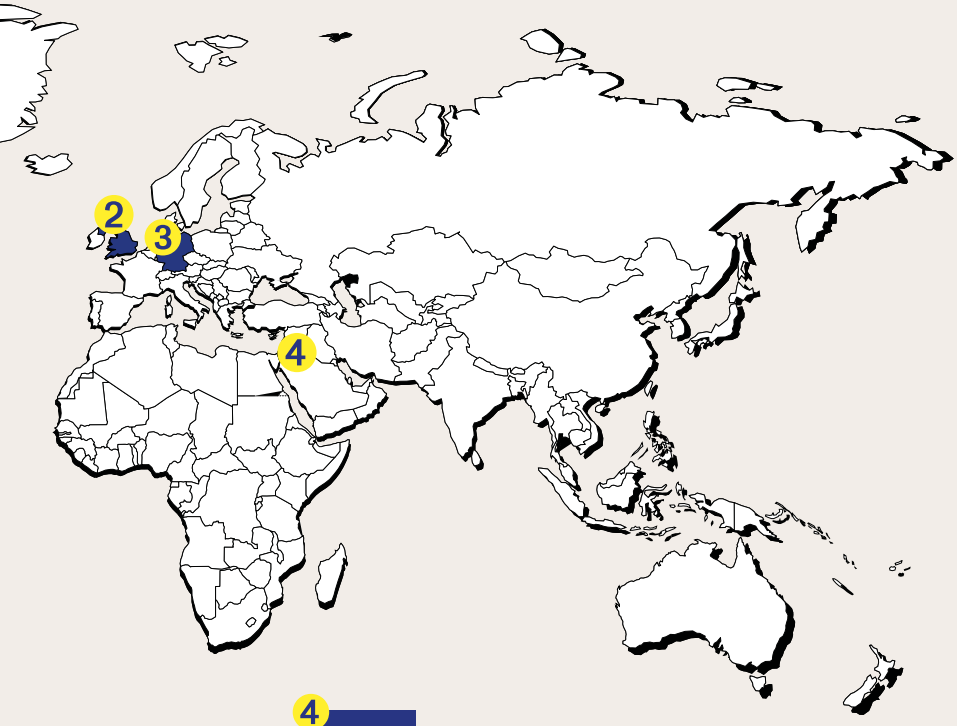
UN MODÈLE INTÉGRÉ RENFORCÉ EN 2010

Des réformes d'ampleur ont été engagées en 2010 pour renforcer le modèle britannique : le poste de conseiller à la sécurité nationale et un *National Security Council* sur le modèle américain ont été créés. Une attention particulière est portée à la sécurité économique (« *Economic security is national security* » selon la *National Security Strategy* de 2025, inspirée de l'approche américaine).

3 Allemagne

UNE RESTRUCTURATION D'ENVERGURE EN 2026

L'exécutif allemand a procédé à une restructuration institutionnelle majeure de son organisation de sécurité nationale, avec la création en janvier 2026 d'un conseil de sécurité nationale, organe permanent de pilotage stratégique intégré, et une stratégie de sécurité nationale révisée triennalement.



4 Israël

UN MODÈLE COMPACT QUI PRIORISE L'INFORMATION

Le Conseil de Sécurité Nationale constitue le cœur d'une organisation de sécurité tournée vers l'évaluation de la menace, la planification et le pilotage des actions stratégiques. L'accent est porté sur le questionnement analytique de l'information (conduit indépendamment par le CSN) et l'intégration stratégique au niveau du Premier ministre. Depuis 2025, une loi requiert la rédaction d'une stratégie de sécurité nationale pour tout nouveau gouvernement.

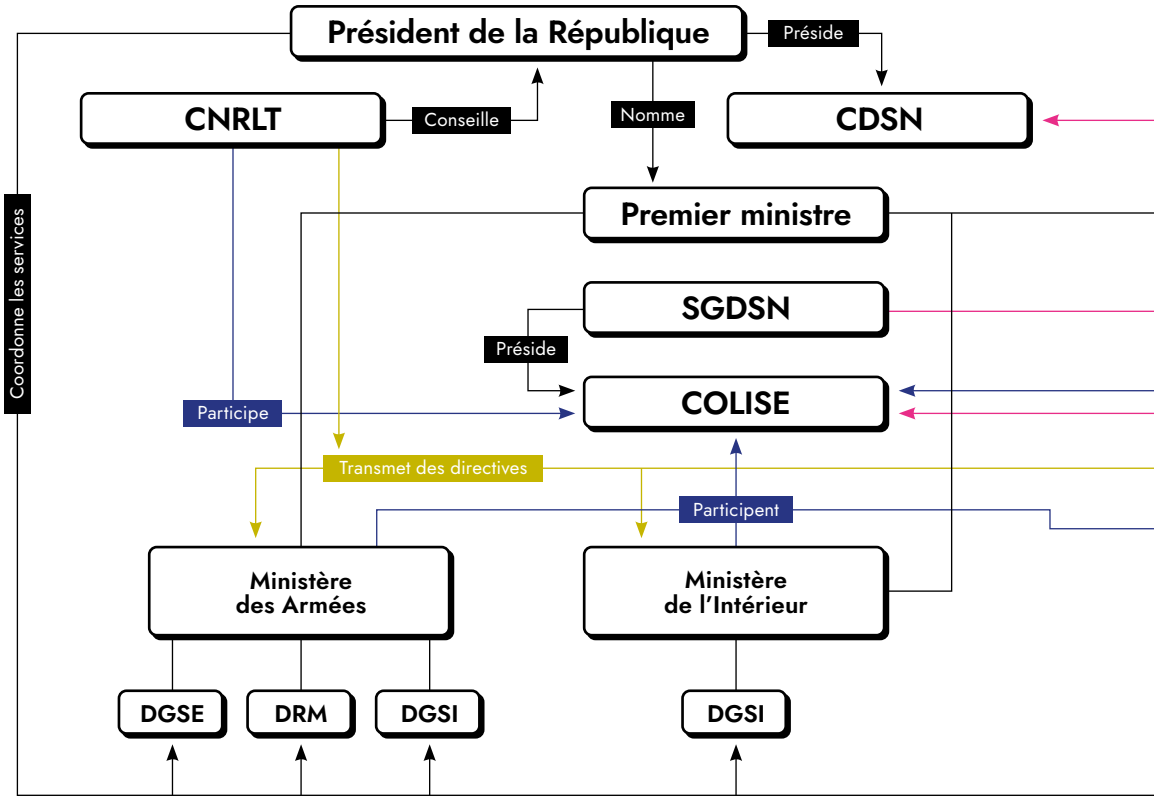
LE CHAMP DE CONTRAINTES

LE TEMPS DU MANDAT PRÉSIDENTIEL : AGIR TÔT ET VITE

La sécurité nationale du pays est la rencontre entre une volonté politique démocratiquement validée et un président de la République qui l'incarne et la déploie. Chaque président imprime donc sa marque dans ce domaine.

Pour que son objet, son emploi et ses résultats soient effectifs dans le temps d'un mandat, il faut une volonté claire, ferme et constante concernant l'organisation politique et administrative des instruments de la sécurité nationale, en particulier des ressources humaines et matérielles qui y sont consacrées.

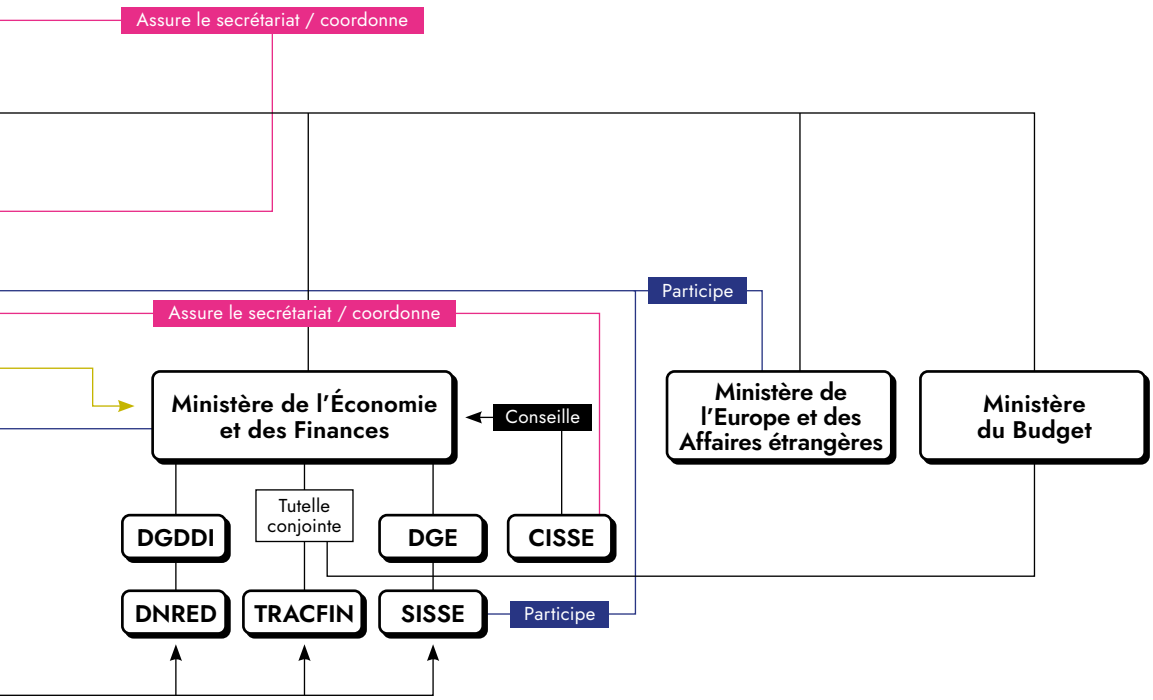
Organisation de la Sécurité Nationale



DES RÉSISTANCES ADMINISTRATIVES ANCRÉES

Le modèle hérité de 1959 consacre le pré-carré de plusieurs ministères (Services du Premier ministre, Armées, Intérieur, Économie & Finance, Affaires étrangères...). Cette mission complexe mobilise plusieurs niveaux administratifs des préfectures jusqu'aux ambassades. Chacun tente de protéger ses prérogatives et ses budgets et la coordination est rarement optimale, même en temps de crise.

Afin de garantir l'efficacité de l'action présidentielle, il est nécessaire de lutter contre ces résistances et de définir une stratégie globale et une nouvelle organisation adaptée aux menaces actuelles.



LES IDÉES REÇUES DU DÉBAT

LA SÉCURITÉ NATIONALE, C'EST DE LA SÉCURITÉ INTÉRIEURE ET DE LA DÉFENSE

FAUX

La sécurité nationale traite l'ensemble des menaces portées contre la France. La sécurité intérieure y contribue mais ne se confond pas avec elle car elle met en œuvre des moyens essentiellement policiers. La défense nationale, pour sa part, engage des moyens militaires afin de protéger notre territoire et nos intérêts. La sécurité nationale peut engager des moyens policiers ou militaires sans pour autant se confondre avec eux. Son approche est donc plus large, pouvant traiter de tarifs douaniers exorbitants, de sécurisation de stocks, de contre-espionnage ou d'opérations extérieures ciblées contre les ennemis de la nation.

LA GUERRE EST POUR DEMAIN

FAUX

Une guerre telle que nous la voyons se manifester en Ukraine ou en Iran n'est pas pour demain. Notre dissuasion nucléaire nous protège des bombardements directs ou d'une invasion militaire prochaine.

Cependant, il est faux de croire que nous ne subissons pas déjà des attaques : une conflictualité sous le seuil militaire constituée notamment d'actes de sabotage, de cyberattaques et de tentatives de déstabilisation sociale telles que menées dans nos Outre-mer est bien en cours contre le pays et nos intérêts stratégiques.

LA SÉCURITÉ NATIONALE EST UNE AFFAIRE DE SPÉCIALISTES

À NUANCER

La sécurité nationale engage des opérations qui doivent parfois rester secrètes et sont donc conduites par des services spécialisés sur le plan tactique. Mais elle relève aussi, au niveau stratégique, de choix politiques qui engagent l'administration et les citoyens à travers leurs décisions et leurs comportements (par exemple, vigilance vis-à-vis de l'espionnage industriel, de la vulnérabilité des systèmes informatiques, de l'ingérence étrangère, consommation de produits français…).

NOTRE SÉCURITÉ NATIONALE EST GARANTIE PAR NOTRE DISSUASION NUCLÉAIRE

À NUANCER

La dissuasion nucléaire permet de protéger nos intérêts vitaux contre des adversaires étatiques et en cas de menace existentielle. Par définition, elle n'est pas censée être utilisée autrement que comme instrument de neutralisation ultime par la destruction mutuelle.

Nos adversaires le savent et calibrent leurs actions pour contourner le seuil de déclenchement nucléaire : un attentat terroriste qui fait des dizaines de morts, une cyberattaque qui paralyse un hôpital ou affaiblit une grande entreprise française, le développement de la prolifération nucléaire de pays hostiles, etc. La sécurité nationale traite de l'ensemble de ces menaces et de leurs manifestations diverses et nécessite une approche à la fois spécifique et globale.

LA SÉCURITÉ NATIONALE EST UNE COMPÉTENCE PARTAGÉE AU NIVEAU EUROPÉEN

FAUX

La sécurité nationale ne fait pas partie des compétences déléguées à la Commission européenne. Elle relève exclusivement de la souveraineté nationale, qui seule la définit. Elle n'exclut pas une coopération entre États européens que peut faciliter la Commission en cas de menace commune si les États le demandent. Si l'idée d'un service de renseignement européen intégré n'est pas à l'ordre du jour, des coopérations bilatérales peuvent cependant exister entre États membres.

LES REPÈRES DE MONTAIGNE

PARTIE 2



DANS LE DÉBAT

L'IMPÉRATIF D'UNE STRATÉGIE POLITIQUE

LA SÉCURITÉ NATIONALE, FONCTION PRÉSIDENTIELLE

De par nos institutions, le président a un rôle essentiel dans le domaine de la sécurité nationale : il est le garant de nos intérêts vitaux (article 5 : indépendance nationale, intégrité du territoire, respect des traités). Chef des armées (article 15) et de la décision d'emploi de l'arme nucléaire, il préside les conseils de défense et de sécurité nationale, et nomme aux emplois civils et militaires (article 13). Le président est donc la clef de voûte de notre système de sécurité nationale.

La sécurité nationale est le point d'aboutissement de l'ensemble de nos politiques publiques (art. 1111-1 du Code de la défense). Afin d'être efficace, elle doit mobiliser l'ensemble des moyens disponibles et structure donc l'ensemble de nos arbitrages politiques, en particulier en matière de défense, de politique étrangère, de sécurité intérieure, de sécurité économique, d'innovation et de compétitivité. Elle est la condition de notre souveraineté et de notre prospérité.

SÉCURITÉ NATIONALE, UN NOUVEL HORIZON DE DANGERS

Dans la grammaire stratégique de la France et parce que nous sommes devenus une puissance moyenne aux moyens limités mais porteuse de grandes responsabilités (nos territoires ultramarins, la dissuasion nucléaire, l'empreinte francophone, la défense des valeurs démocratiques…), la question entre prévenir et intervenir a toujours été centrale. Doit-on être suffisamment dissuasif pour que nos adversaires ne nous attaquent pas ou être suffisamment prêts à réagir à une provocation ennemie ?

Doit-on privilégier une logique de réponse militaire ou une logique de prévention qui consiste à gérer les menaces qui se déploient sous le seuil militaire ? C'est ce type de questions que la sécurité nationale doit traiter. L'accélération, l'intensification et les nouveaux formats d'attaques contre les intérêts français justifient une nouvelle stratégie politique en charge de redéfinir l'organisation et les moyens de notre sécurité nationale.

TOUR D'HORIZON DES **IDÉES QUI ANIMENT LE DÉBAT PUBLIC**

DANS LE DÉBAT

IDÉE DU DÉBAT N° 1

PRÉPARER LA AU RISQUE DE

Quel parti pris ?

La principale menace pesant sur notre sécurité nationale a été décrite par la Revue nationale stratégique : une guerre majeure de haute intensité en Europe, en dehors du territoire national, déclenchée par une agression russe, qui impliquerait la France et ses alliés à l'horizon 2030, et qui entraînerait des actions déstabilisatrices concomitantes sur le territoire national.

Dans ces conditions, notre sécurité nationale doit prioriser la préparation de nos moyens militaires, dans toutes leurs dimensions : forces armées et de réserve, budget accru de la défense, résilience de notre économie dans un contexte de guerre – voire économie de guerre, défense du territoire et force morale de la nation, consolidation des partenariats stratégiques.

Dans cette perspective, l'organisation actuelle de notre sécurité nationale n'est pas modifiée. L'accent est porté sur le renforcement des parties constitutives de la défense et de la résilience de la nation au sein d'une organisation inchangée.

NATION GUERRE

IDÉE N°1 DU DÉBAT

Le principal problème de notre sécurité nationale est le risque de conflit de haute intensité que de nombreux experts anticipent pour la fin de la décennie. Les guerres se déclenchent mais ne se déclarent plus formellement. Dans ce contexte, l'accent doit être porté sur la préparation de nos moyens militaires et civils et l'organisation de la nation face à un risque majeur de conflit protéiforme : entraînement des forces armées, structuration de la défense du territoire national, résilience de notre économie et de la population, partenariats stratégiques.

IDÉE N°1 DU DÉBAT

RENFORCER NOS CAPACITÉS MILITAIRES

Cf. Note Défense nationale

Rehausser le format et le budget de nos armées

La primauté de la menace russe appelle la constitution d'une armée conventionnelle prête à intervenir sur le théâtre est-européen et disposant de moyens d'information et de commandement renforcés.

Une telle armée **investit essentiellement la capacité d'action aéroterrestre pour emporter une capacité de destruction massive.** La structure correspondant le mieux au renouveau des besoins militaires de masse et de létalité est le Corps d'Armée. Il est donc nécessaire de **constituer un corps d'armée composé de 3 à 5 divisions européennes dont 1 division entièrement française** afin de pouvoir engager au minimum 70 000 hommes au combat (dont 30 000 Français).

Ce Corps d'Armée est **commandé par l'État-major français dédié du 1er corps d'armée de Lille.** En charge de la conception et de la conduite des opérations, il intègre des contributions d'armées européennes telles que l'armée belge, roumaine, allemande etc. afin de pérenniser le format proposé par l'exercice interarmées français ORION, inspiré de la coopération en format OTAN.

Combler les lacunes de la crédibilité conventionnelle

Engager une logique de masse plutôt que de sur-spécification pour la logistique, les stocks stratégiques et les petits objets :

- développement des capacités de défense anti aérienne, feux directs, feux indirects, frappes dans la profondeur ;
- massification des programmes de dronisation : (projets Colibri et Larinae accélérés, micro-drones IA à haute densité,

pour que chaque unité de combat de première ligne dispose de son propre système de drone organique et d'opérateurs formés aux champs de bataille saturés de drones) ;
- sortie du programme européen MALE RPAS et financement du drone MALE Aarok ;
- consolidation des moyens logistiques (avions et véhicules terrestres de transport).

Investir dans les systèmes d'information et de commandement interopérables entre Européens

- **Exécuter impérativement les 10 domaines satellitaires de la LPM** et sanctuariser leurs budgets. En particulier, veiller au budget des équipements de communications militaires.
- **Accélérer les programmes spatiaux satellitaires** européens (renseignement, communication, commandement, coordination des activités en temps réel).

Le programme franco-allemand JEWEL *(Joint Early Warning European Lookout)* doit être porté à 2 satellites et avancé pour 2028 (et non 2030). Pour ce faire, le programme ODIN'S EYE II doit être finalisé à temps (fin 2026 par le consortium franco-allemand OHB.

- **Accélérer les cadences de lancement satellitaires.** La France ne disposera pas d'un réseau LEO souverain de classe gouvernementale avant le lancement des services d'IRIS² (300 satellites en remplacement de OneWeb, les satellites d'Eutelsat d'ancienne génération) en 2030. En 2025, seulement 5 lancements d'Ariane 6 ont été effectués contre environ 150 lancements pour SpaceX et plus de 90 lancements orbitaux chinois sur la même année.

La mesure phare de cette stratégie

Une DOT actualisée

Définie par l'article R.*1421-1 du Code de la défense, la DOT confie aux autorités militaires une triple mission :

1/ participer à la protection des infrastructures militaires et notamment des installations nucléaires, **2/** assurer la couverture du territoire national en s'opposant aux actions ennemies sur notre territoire et **3/** en cas d'invasion, mener les opérations de résistance militaire.

Au-delà de ces missions initiales, dans le cas d'un conflit majeur tel qu'envisagé par la revue nationale stratégique, la DOT constitue l'outil clé de notre résilience, face à des actions visant à contraindre notre décision politique.

La DOT doit intégrer les nouveaux modes d'action qui peuvent être employés dans les différents champs (physique, numérique, informationnel) contre la nation: piratages massifs contre nos bases de données, cyberattaques visant nos infrastructures critiques, campagnes de sabotages employant des proxies, campagnes de désinformation visant à semer le doute sur le bon fonctionnement de notre vie démocratique, etc.



REDÉFINIR LA DÉFENSE OPÉRATIONNELLE DU TERRITOIRE

Mettre fin à l'opération Sentinelle

Le déploiement des forces militaires sur le territoire national, qui dure depuis 10 ans, mobilise nos armées pour la lutte antiterroriste qui ne relève pas d'une action militaire sur le territoire national, mais d'une action de sécurisation policière qui vise à neutraliser et à éliminer les sources et acteurs de menace. Elle consomme des moyens nécessaires à la préparation de la guerre.

Actualiser la Défense Opérationnelle du Territoire

- **Repenser la DOT** autour de la protection physique de nos infrastructures critiques, l'entrave des actes de subversion étrangers sur le territoire et les actions de déstabilisation numérique. La répartition des forces sur le territoire doit être rééquilibrée pour englober tous les plans d'attaque : spatial, terrestre, maritime (y compris sous-marin) et numérique.
- **Intégrer à la DOT un grand plan de cybersécurité** pour adapter notre défense des opérateurs d'importance vitale (OIV) en cas de guerre, en mettant l'accent sur leur interdépendance et la lutte contre les attaques générées par les agents IA.
- **Anticiper les risques de subversion** actionnée par l'étranger pour entraver nos forces et renverser nos institutions en renforçant l'expertise et les moyens de la gendarmerie mobile.
- Repenser **le système de casernement** dans l'hexagone et nos Outre-mer afin de dessiner un maillage militaire prêt pour une montée en puissance des forces à engager en cas de guerre.

Renforcer les moyens de la gendarmerie nationale

- **Recruter 5500 gendarmes supplémentaires** pour traiter les nouvelles formes de conflictualité hybride sur le territoire français :
  - confier à la gendarmerie la responsabilité de la lutte anti-terroriste sur la voie publique et y affecter 2000 personnels. Créer 20 escadrons de gendarmerie mobile pour remplir cette mission, ce qui permettrait parallèlement de disposer d'un volume d'unités plus important en cas de déclenchement de la DOT ;
  - compléter le recrutement des derniers 1150 gendarmes prévus par la LOPMI pour combler les manques de l'organisation actuelle (239 brigades) ;
  - affecter 2 500 gendarmes supplémentaires dans les Outre-mer afin de faire face aux besoins. En cas de crise, ils renforceraient le dispositif de souveraineté des armées.
- **Doubler la réserve opérationnelle** de la gendarmerie nationale pour atteindre 80000 hommes (contre 44000 aujourd'hui), en budgétant les moyens requis pour l'équipement et la formation.

Ces idées sont celles qui animent le débat public. Vous trouverez la recommandation de Montaigne en partie 3.

RENFORCER LA RÉSILIENCE DE LA NATION

Actualiser la politique de stocks stratégiques

La Stratégie Nationale de Résilience (SNR) doit être actualisée pour tenir compte du besoin de diversification et de sécurisation des approvisionnements stratégiques de notre base industrielle et technologique de défense (BITD) en prévision d'un déclenchement d'un conflit majeur. En particulier, un stock stratégique de métaux critiques de défense doit être reconstitué afin de garantir nos capacités de production et la pérennité de notre effort de réarmement. Cette politique de stocks stratégiques devra également intégrer les nouvelles obligations faites aux industriels (par la loi d'actualisation de la loi de programmation militaire votée en 2026) de constituer des stocks stratégiques à leur propre niveau.

Développer le service national pour atteindre 15 000 hommes

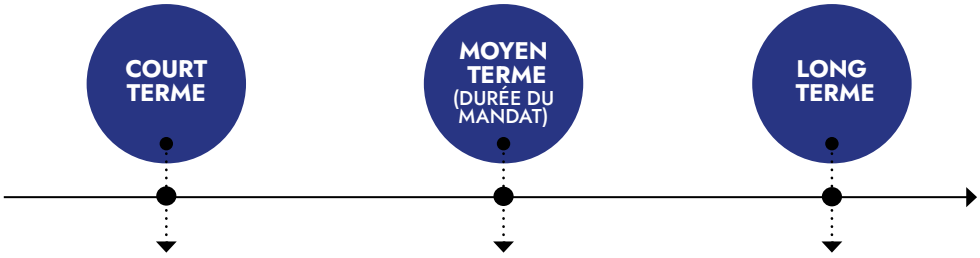
Le service national créé en 2026 offre à tous les jeunes entre 18 et 25 ans la possibilité de servir au sein des forces armées pour une durée de 10 mois, dans le cadre d'un contrat court non renouvelable. Ce format permet de renforcer le lien entre les armées et la population, et contribue à la diffusion de l'esprit de défense au sein de la jeunesse de notre pays. Actuellement prévu pour un objectif de 10 000 hommes en 2030, sa trajectoire annuelle sera renforcée pour atteindre 15 000 à la fin de la LPM.

Ce qu'on a déjà su mettre en place, en France ou ailleurs

Stratégie nationale de résilience (France)

En 2022, tirant les enseignements de la crise du COVID, le SGDSN a publié pour la première fois une stratégie nationale de résilience, centrée sur la prévention et la préparation des crises. Révisée en 2025, la SNR se concentre désormais sur deux axes : assurer la continuité économique de la nation (résilience des réseaux essentiels, remédiation des risques sur les approvisionnements critiques) et la mobilisation de l'ensemble des citoyens soutenant la résilience du pays. À ce titre, un guide territorial est diffusé par le SGDSN à destination des territoires (élus locaux, chefs d'entreprises, acteurs associatifs). Cette stratégie est suivie par le Comité interministériel de la résilience nationale (CIRN), présidé par le directeur de cabinet du Premier ministre.

GOUVERNANCE ET FAISABILITÉ



COURT TERME

La DOT est actualisée pour intégrer l'ensemble des vulnérabilités critiques matérielles et immatérielles, dans une logique de résilience et de lutte contre la subversion.

La constitution de stocks stratégiques d'équipements finis est accélérée.

MOYEN TERME (DURÉE DU MANDAT)

Les moyens de notre résilience face aux chocs militaires (format des forces armées, stocks stratégiques de composants, compétences et volume des réserves) sont renforcés, dans le cadre d'une nouvelle loi de programmation militaire et sécuritaire.

Les conditions de l'interopérabilité militaires avec les armées européennes sont réalisées.

Une attention particulière est portée à la sécurité économique en partenariat avec les États-membres de l'UE et la Commission.

LONG TERME

Nos capacités conventionnelles sont reconstituées pour crédibiliser notre posture de défense face à la menace d'un engagement militaire de haute intensité.

Le service national créé par la loi de juin 2026 est développé pour atteindre *a minima* 15000 hommes.

Ces idées sont celles qui animent le débat public. Vous trouverez la recommandation de Montaigne en partie 3.

Combien cela coûterait approximativement ?

De

15 à 19 MD€

sur 3 ans

UN REHAUSSEMENT DE LA TRAJECTOIRE DE LA LPM DE 15 À 19 MDS € SUPPLÉMENTAIRES

La loi de programmation militaire en cours prévoit une trajectoire qui culmine à 76,3 Mds € en 2030.

Les mesures prévues par cette stratégie, concernant le corps d'armée européen (8 à 12 Mds€), les systèmes d'information et de commandement requis pour l'interopérabilité de ce corps d'armée (2 Mds€), l'actualisation de la politique de stockage stratégique (900 M€ à 1 Md€), le renforcement des effectifs du service national (3 Mds€), le doublement des effectifs de la réserve gendarmerie (140 M€), et le recrutement de 5 500 gendarmes supplémentaires dont 2 500 à destination des Outre-mer (1,1 Mds€), nécessitent une augmentation des crédits militaires de 15 à 19 Mds€ supplémentaires.

Faisabilité et arbitrages

FAISABILITÉ

La réalisation de cette stratégie repose essentiellement sur le ministère des Armées. Elle suppose également une action diplomatique forte pour s'assurer de la convergence des armées européennes avec le projet français, ainsi que l'engagement des industriels concernés.

Sa faisabilité exige un effort financier supplémentaire, appelant des coupes-sombres par ailleurs au vu des finances publiques de la France. Cela appelle donc une communication présidentielle et gouvernementale convaincante pour justifier auprès des Français les renoncements sociaux nécessaires à un réarmement massif.

ARBITRAGES MAJEURS

Le choix d'une stratégie de réponse exclusivement militaire impose une réorientation prioritaire des moyens de notre sécurité nationale vers les armées, et des arbitrages budgétaires qu'il faudra négocier avec les partenaires sociaux et les assemblées parlementaires.

La priorité accordée à la menace russe sur le continent européen implique de déprioriser la défense de nos intérêts nationaux sur d'autres théâtres.

POINTS DE TENSION

La préparation à une confrontation militaire passe par une mobilisation de l'esprit de défense de la nation, ce qui implique un débat national, transparent et objectivé sur l'horizon et la nature de la menace.

Ces idées sont celles qui animent le débat public. Vous trouverez la recommandation de Montaigne en partie 3.

DANS LE DÉBAT

IDÉE DU DÉBAT N° 2

TRAITER LES DE PAIX

Quel parti pris ?

Même si le risque d'une guerre de haute intensité ne doit pas être négligé, la conviction ici est celle d'une nation perpétuellement sous attaques depuis quelques années, même si ces attaques se déploient en dessous du seuil militaire et ne sont pas directement perçues par les citoyens au quotidien, ou identifiées comme relevant d'une hostilité extérieure.

Mais nous savons que nos adversaires peuvent désormais atteindre notre territoire de différentes manières : par la voie économique (prises de participation hostiles dans des entreprises, manipulation des cours de bourse, déni d'accès aux ressources, coercition douanière et commerciale…), par les attaques cyber (piratage et vol de données, usurpations d'identité, systèmes saturés, pris en otage ou détournés, rançons…), par la sphère informationnelle (fausses informations, complotisme, manipulation de l'opinion…), par l'ingérence ou l'influence politique (financements occultes, emprises, coercition, manipulations électorales…). Ainsi, notre souveraineté peut être attaquée sans la mise en œuvre de moyens militaires. Et réciproquement, nos propres moyens militaires s'avèrent inopérants face à ces modes d'actions adverses.

Dans ces conditions, et en dehors de la garantie existentielle fournie en tout temps par notre dissuasion nucléaire, il s'agit de protéger nos intérêts vitaux sans entraîner d'escalade militaire et de répondre à une conflictualité croissante qui se manifeste d'abord en temps de paix. Les réflexes et organisations antérieurs s'avèrent insuffisamment adaptés et efficaces pour répondre à cette nouvelle réalité.

MENACES DU TEMPS

IDÉE N°2 DU DÉBAT

Bien que les manifestations d'hostilité et de conflit soient dispersées et diffuses et que nous n'ayons pas le sentiment d'être attaqués, un conflit bien réel visant nos intérêts vitaux se déploie d'ores et déjà sur notre territoire allant du durcissement de la compétition à la coercition diplomatique. Il s'agit d'attaques sous le seuil militaire : manipulation des opinions, déstabilisation des institutions, déni d'accès et de ressources, pillage et chantage économique, guerre par le droit... Pour protéger nos intérêts vitaux, il faut en priorité nous organiser pour répondre à cette conflictualité du temps de paix, dans une logique de prévention de l'escalade militaire.

IDÉE N°2 DU DÉBAT

AMÉLIORER LA GOUVERNANCE DE NOTRE SÉCURITÉ NATIONALE

Créer un organe permanent de sécurité nationale auprès du président de la République

Reconfigurer l'état-major particulier du président de la République pour en faire un état-major dédié à la sécurité nationale, comprenant les ressources civiles et militaires nécessaires et fédérant les compétences aujourd'hui dispersées au sein des différentes instances étatiques :

- **définir l'état de la menace contre nos intérêts vitaux** (sécuritaires, économiques, technologiques...) et proposer les orientations et les priorités d'action permettant d'y répondre ;
- **élaborer la stratégie de sécurité nationale** intégrant les différentes dimensions : sécurité physique, sanitaire, économique, etc. déclinée par une **loi de programmation sécuritaire** qui sanctuarise les missions et les moyens (incluant les aspects spatiaux et numériques) ;
- fournir en permanence au président de la République les éléments d'analyse et d'aide à la décision.

Ces idées sont celles qui animent le débat public. Vous trouverez la recommandation de Montaigne en partie 3.

Recentrer le SGDSN sur la gestion des crises rattachée à Matignon au titre de la coordination interministérielle

- Anticipation des crises et planification de leur gestion.
- Rattachement de l'entité de la Gestion des Crises du Ministère de l'Intérieur.
- Plan de centralisation et de gestion des stocks stratégiques : la Stratégie Nationale de Résilience (SNR) doit être actualisée pour tenir compte du besoin de diversification et de sécurisation des approvisionnements stratégiques de notre base industrielle et technologique de défense (BITD) en prévision d'un déclenchement d'un conflit majeur ou d'attaques de prédation économique. Cette politique de stocks stratégiques devra également intégrer les nouvelles obligations faites aux industriels (par la loi d'actualisation de la loi de programmation militaire votée en 2026) de constituer des stocks stratégiques à leur niveau. Des stress tests réguliers devront être effectués.

AGIR SUR NOS VULNÉRABILITÉS SYSTÉMIQUES

Augmenter la protection de nos OIV (Opérateurs d'Intérêts Vitaux) et SIV (Systèmes d'Importance Vitale)

Renforcer la gouvernance et le pilotage de la résilience des infrastructures essentielles :

- Associer systématiquement les opérateurs d'infrastructures et les acteurs économiques avec lesquels ils présentent des situations d'interdépendance aux **travaux du comité interministériel de résilience nationale (CIRN)**. Cette intégration permettra de mieux coordonner et suivre les avancées des filières en matière de résilience, et de les accompagner par un budget dédié.
- Généraliser l'**attribution de la compétence de la résilience à un élu,** *a minima* dans les plus grandes collectivités, en charge du suivi transversal de la résilience sur les différents OIV/SIV.
- Généraliser l'introduction de clauses visant à **renforcer la résilience des services dans les contrats de commandes publiques,** dans une logique capacitaire (moyens devant être disponibles et mobilisables en cas de crise).

Passer d'une culture du risque à une culture de la résilience, mieux partager les informations et les compétences :

- Systématiser, *via* l'outil du CIRN, le partage entre public et privé : **scénarios de projections entre les administrations et les entreprises,** méthodologie commune d'identification des vulnérabilités croisées entre les acteurs économiques, retours d'expérience sur les exercices et la gestion de crises.
- Intégrer, dès les **exercices préparatoires à la gestion de crises,** l'ensemble des acteurs et personnes qui seront impliqués dans une crise d'envergure (avec une attention particulière aux risques nucléaires, radiologiques, biologiques, chimiques (NRBC)), pour diffuser les bonnes pratiques et réactions et favoriser un esprit de résilience partagé et éprouvé.
- **Planifier les passations intergénérationnelles des savoirs indispensables** à l'entretien d'infrastructures anciennes (pérennité des compétences dans le long ou très long terme, structuration de filières de formation dédiées qui s'appuient sur des nouvelles technologies et mobilisation des anciens des secteurs stratégiques).

Renforcer notre cybersécurité, par une meilleure gouvernance et un soutien aux territoires et PME

Consolider l'ANSSI comme acteur central de notre cybersécurité afin de garantir une gouvernance plus opérationnelle.

Pour mettre fin à la faiblesse de notre cybersécurité (10 fuites massives de nos fichiers souverains au cours des 12 derniers mois), avec le risque démultiplicateur désormais de l'IA agentique, il est nécessaire de construire un dispositif gouvernemental plus clair, plus opérationnel et plus pilotable. Notre posture doit évoluer d'une simple doctrine de conformité à une approche stratégique critique appelant un effort prioritaire et soutenu dans le temps.

- Élargir les compétences et les responsabilités de l'ANSSI **pour en faire une agence nationale placée directement sous les ordres du premier ministre, responsable de l'ensemble des capacités cyber interministérielles.** Ce format permettra de sanctuariser ses effectifs et sa trajectoire budgétaire et de la doter d'une stratégie de développement commun pour l'État selon les recommandations de la Cour des comptes.
- Doter l'ANSSI d'une programmation budgétaire pluriannuelle cohérente avec la stratégie nationale actualisée : +30 M€ de budgets et +20 % d'effectifs d'ici 2028.
- Signer des conventions ANSSI-ministères **fixant objectifs, échéancier et moyens cyber, ministère par ministère,** avec une attention particulière concernant l'évolution des plateformes IA agentique et des identités non humaines (NHI).

La mesure phare de cette stratégie

CRÉATION D'UN ORGANE PERMANENT DE SÉCURITÉ NATIONALE AUPRÈS DU PRÉSIDENT

Alors qu'il est la clef de voûte de notre sécurité nationale, le président ne dispose pas d'un organe permanent chargé de centraliser et préparer ses décisions en la matière.

Au sein de l'Élysée, trois structures distinctes fonctionnent actuellement : la cellule diplomatique (une douzaine de conseillers) est consacrée à l'action de politique étrangère du président. L'État-major particulier (EMP, cinq conseillers), est consacré aux questions de défense, en particulier relatifs à la dissuasion nucléaire. Le Coordinateur National du Renseignement et de la Lutte contre le Terrrorisme (CNRLT, une douzaine de conseillers) coordonne l'action des services de renseignement et transmet aux ministres responsables de ces services les instructions du président. Il est chargé de l'analyse globale de la menace et propose au président sur cette base les orientations du renseignement.

Par ailleurs, le Secrétariat Général pour la Défense et la Sécurité Nationale (SGDSN), placé auprès du Premier ministre, est chargé de centraliser et coordonner les différentes dimensions de la sécurité nationale. Il prépare également les travaux du Conseil de Défense et de Sécurité Nationale, que préside le président de la République.

Pour remédier à cette dispersion et au fractionnement des structures clés de notre sécurité nationale (cf. schéma p. 21), il convient de simplifier et centraliser le dispositif autour de l'EMP pour en faire l'outil dédié de notre sécurité nationale.

Ces idées sont celles qui animent le débat public. Vous trouverez la recommandation de Montaigne en partie 3.

Étendre le filet de sécurité vers les territoires et les PME en particulier :

- Étendre les outils de cybersécurité du secteur public vers le secteur privé en demande : adapter ***MonServiceSécurisé*** pour le décliner aux acteurs économiques privés : ***MonEntrepriseSécurisée***. Cette plateforme gratuite et collaborative permettra aux dirigeants de PME, cibles privilégiées des rançongiciels, d'obtenir un diagnostic cyber rapide, de piloter collaborativement leur démarche d'homologation, d'accéder automatiquement à un catalogue d'aides et de subventions étatiques directes pour financer l'acquisition de solutions logicielles de confiance qualifiées.
- Conditionner l'obtention de subventions d'équipements de l'État (la DETR pour le monde rural et la DSIL pour l'investissement local) à la réalisation d'un **audit de sécurité initial de conformité au ReCyF** (le Référentiel Cyber France) et à la mise en œuvre d'un plan correctif. Pour le secteur privé (PME/ETI), conditionner le versement des aides de Bpifrance à l'investissement et les subventions du plan France 2030 à la réalisation du **diagnostic obligatoire Cyber PME** (audit de 8 jours pris en charge à 50 % par l'État).

Renforcer les moyens de sécurité destinés à nos Outre-mer particulièrement exposés

Les Outre-mer étant une cible privilégiée des attaques en déstabilisation (Nouvelle Calédonie, Mayotte, Guyane, Martinique…), il est indispensable de les défendre en tant que partie intégrante de la nation, en effectuant un choc capacitaire en matière de sécurité nationale :

- **Déploiement de moyens supplémentaires de la DGSI,** à hauteur d'une trentaine d'équivalents temps plein (ETP), dotés des moyens techniques nécessaires. Loin de se substituer au renseignement territorial obtenu par la gendarmerie et la police, ce renforcement agira en parfaite complémentarité pour remonter les filières d'agents d'influence, offrant à l'État un véritable levier pour anticiper les crises et faciliter les mesures d'entrave administrative.
- **Déploiement de moyens supplémentaires de la DNRED** (Direction Nationale du Renseignement et des Enquêtes Douanières), **à hauteur d'une dizaine** d'équivalents temps plein (ETP), afin de démanteler les filières logistiques et financières visant nos territoires ultramarins, ces filières profitant à la criminalité organisée et pouvant être instrumentalisées dans une logique de subversion.

IDÉE N°2 DU DÉBAT

DÉVELOPPER UNE CULTURE DE SÉCURITÉ NATIONALE

Mettre en place une réserve de sécurité nationale, fonctionnant comme une réserve civile compétente dans les sujets technologiques pour venir en appui des unités militaires si besoin. Les différents dispositifs existants (réserve civile, réserve civique, réserve communale de sécurité civile) devraient être fusionnés, autour de 3 piliers :

- un pilier sécurité intérieure (hors DOT) avec les forces de police déjà en place ;
- un pilier résilience traitant les fonctions de sécurité civile, de réserve sanitaire notamment dans le domaine NRBC et de réserve logistique ;
- un pilier cybersécurité avec les experts technologiques compétents.

Prononcer devant la représentation nationale un discours annuel sur l'état de notre sécurité nationale

Le président prononcera un discours annuel (sur le modèle du discours sur l'état de l'Union du président américain) consacré à exposer les enjeux de notre sécurité nationale. Ce discours pourrait être suivi (au titre de l'article 18) d'un débat parlementaire permettant à la représentation nationale de s'approprier cette dimension et de s'exprimer chaque année sur ces enjeux.

Développer une communication de prévention envers les citoyens

- Confier au SGDSN la réalisation d'un fascicule de conscientisation des différentes formes de menaces et de mesures préventives au fur et à mesure de leurs évolutions et de campagnes de communication adaptées aux menaces de l'instant.
- Partager avec les médias l'état d'information des menaces afin d'en faire des acteurs responsables auprès du grand public.
- Déclassifier une partie des informations de renseignement afin de matérialiser auprès du grand public la réalité de certaines menaces sous le seuil militaire.

Ces idées sont celles qui animent le débat public. Vous trouverez la recommandation de Montaigne en partie 3.

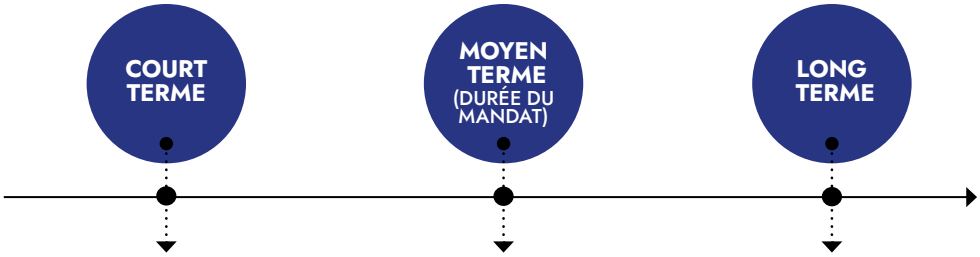
Ce qu'on a déjà su mettre en place, en France ou ailleurs

La sécurité nationale, bras armé de l'exécutif américain

Le modèle de sécurité nationale américain repose sur une architecture institutionnelle centralisée autour du pouvoir exécutif, dont le cœur opérationnel est le *National Security Council Staff (NSC staff)*. Cet organe assure l'intégration interinstitutionnelle de l'ensemble des leviers : diplomatie *(State Department)*, défense *(Pentagon)*, renseignement, économie *(Treasury Department, Commerce Department)*, etc. Cette structure flexible permet de surmonter les rivalités bureaucratiques pour offrir au président une vision globale et réactive ainsi que des options de réponse face aux crises du temps de paix.

Cette gouvernance se matérialise à travers un cycle de planification stratégique formalisé par la publication périodique de documents stratégiques. Au sommet de cette pyramide doctrinale se trouve la *National Security Strategy* (NSS), document public signé par le président et définissant les objectifs prioritaires de la sécurité nationale, les menaces et les moyens de les surmonter. Pour traduire ces orientations politiques globales en directives militaires concrètes, le secrétaire à la Défense publie ensuite la *National Defense Strategy* (NDS). Cette déclinaison propre au Pentagone fixe les priorités budgétaires, technologiques et opérationnelles des forces armées face aux compétiteurs stratégiques. Le rôle de coordination du *NSC staff* et l'articulation de ces stratégies garantissent la cohérence de l'action de sécurité autour d'une vision politique unique.

GOUVERNANCE ET FAISABILITÉ



Publier un décret élargissant les mission de l'EMP.

Initier l'élaboration d'une stratégie de sécurité nationale (SSN).

Décliner la SSN par une loi de programmation de sécurité nationale et l'animation d'un débat parlementaire.

Auditer les mérites et limites des changements effectués.

Créer une filière de formation des personnels dédiés.

Ces idées sont celles qui animent le débat public. Vous trouverez la recommandation de Montaigne en partie 3.

Combien cela coûterait approximativement ?

429 M€/an

UN BUDGET DE RENFORCEMENTS CIBLÉS

Cette stratégie repose essentiellement sur une amélioration de notre organisation et sur une meilleure intégration de nos moyens tels qu'ils existent déjà.

Les moyens supplémentaires concernent essentiellement la création d'une réserve de sécurité nationale (378 M€/an), la protection de nos Outre-mer par des effectifs spécialisés (6 M€), ainsi que le renforcement de notre cybersécurité (45 M€).

Faisabilité et arbitrages

FAISABILITÉ

La réalisation de cette stratégie passe pour l'essentiel par décrets en conseil des ministres et par une réorientation de la pratique institutionnelle.

La faisabilité politique apparaît également forte puisqu'il s'agit de produire une politique publique de la sécurité nationale, associant plus étroitement la représentation nationale et les citoyens dans la protection de nos intérêts vitaux.

ARBITRAGES MAJEURS

Tout en respectant la nécessité du secret sur certains volets sensibles, accepter une communication plus transparente et une responsabilisation accrue des échelons administratifs de la sécurité nationale. Cela permettrait de constituer une véritable politique publique de sécurité nationale, et de mobiliser pleinement les citoyens concernant la protection des intérêts vitaux de la nation.

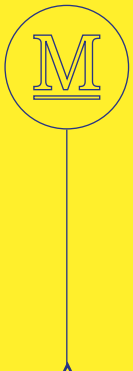
POINTS DE TENSION

La réforme de la gouvernance et l'introduction d'une plus grande responsabilité dans l'action de sécurité nationale est susceptible de rencontrer de réelles résistances administratives. Les avis des hauts fonctionnaires restent assez tranchés sur cet aspect entre ceux qui appellent de leur vœu une concentration des moyens pour décider et ceux qui privilégient l'étalement actuel du système.

Ces idées sont celles qui animent le débat public. Vous trouverez la recommandation de Montaigne en partie 3.

LES REPÈRES DE MONTAIGNE

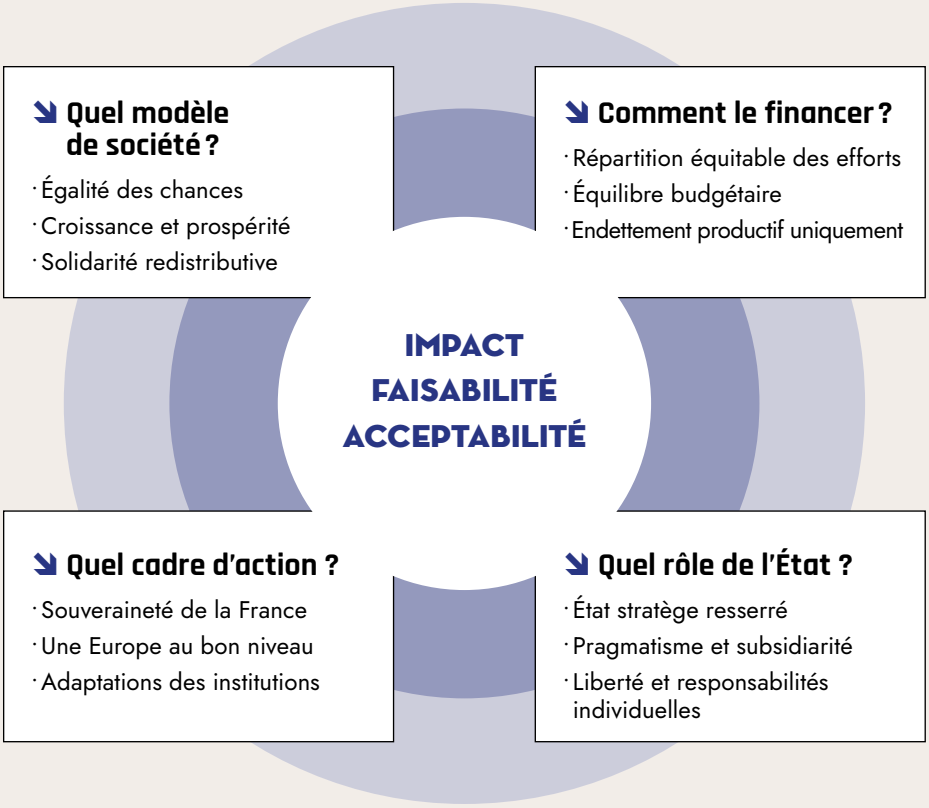
PARTIE 3



LA RECOM-MANDATION DE MONTAIGNE

NOS PRINCIPES D'ARBITRAGES

Pour ses propres recommandations, l'Institut Montaigne a structuré sa grille de réflexion selon les principes suivants :



LA VOIE CHOISIE PAR L'INSTITUT MONTAIGNE

NOTRE RECOMMANDATION

ANTICIPER ET PARER LES MENACES



POURQUOI CETTE VOIE ?

RECHERCHE D'EFFICACITÉ MAXIMALE LE PLUS RAPIDEMENT POSSIBLE

Les menaces sont multiformes et simultanées, la conflictualité déborde le champ militaire, les facteurs d'escalade sont multipliés d'une manière particulièrement véloce. Dans ces conditions, une approche par silos ministériels (Armées/Intérieur/Affaires étrangères/ Numérique/Santé…) et séparation entre menaces extérieures et menaces intérieures apparaît dépassée. L'échelon de coordination administrative par le biais d'un secrétariat général dédié ne tient plus le rythme de l'anticipation et de la gestion des attaques en temps réel et ne tient que par la qualité des personnels mobilisés avec les effets limitants que cela entraîne (mode de gestion urgent constant, fatigue, biais de gestion…).

Dans cette lecture, nous favorisons une approche intégrée (plus proche de l'idée n° 2 du débat) qui semble correspondre plus pragmatiquement à la nécessaire protection de l'ensemble de nos intérêts. Sans cette vigilance d'un temps de paix mis à l'épreuve, il ne saurait y avoir un déploiement militaire capable de tenir la haute intensité : résilience de l'arrière, force morale, logistique solide, capacités financières, crédibilité auprès de nos alliés, etc. Tout est lié et la solidité tant des forces citoyennes que des forces économiques est un prérequis à toute efficacité militaire durable.

L'urgence à nous organiser face à l'évolution des menaces, l'existence de moyens très dispersés au sein de l'État et la nécessité de recouvrer une pensée stratégique dans la durée ont donc guidé le choix d'une reconfiguration de nos outils et du pilotage de notre politique de sécurité nationale afin de combiner le plus efficacement possible les principes stratégiques que nous voulons suivre et l'exécution opérationnelle qu'ils imposent.

Une telle reconfiguration est facilement implémentable par décret. Elle devra être complétée par une refonte majeure de notre organisation et de notre stratégie globale de cybersécurité, talon d'achille de notre sécurité nationale.

AXE 1

AMÉLIORER LA GOUVERNANCE DE NOTRE SÉCURITÉ NATIONALE

Créer un organe permanent de sécurité nationale auprès du président de la République

Reconfigurer l'état-major particulier du président de la République pour en faire un état-major dédié à la sécurité nationale, comprenant les ressources civiles et militaires nécessaires et fédérant les compétences aujourd'hui dispersées au sein des différentes instances étatiques (cellule diplomatique, CNRLT, SGDSN, etc).

Il aura pour mission de :

- définir l'état de la menace contre nos intérêts vitaux (sécuritaires, économiques, technologiques…) et proposer les orientations et les priorités d'action permettant d'y répondre ;
- **élaborer la stratégie de sécurité nationale** intégrant les différentes dimensions : sécurité physique, sanitaire, économique, etc. déclinée par une **loi de programmation sécuritaire** qui sanctuarise les missions et les moyens (incluant les aspects spatiaux et numériques); dans cette optique, la RNS n'a plus lieu d'être et le Livre Blanc de la défense qu'elle remplaçait est réinstitué

comme prévu par la loi *(Cf. Note Défense nationale)* ;
- fournir en permanence au président de la République les éléments d'analyse et d'aide à la décision.

Recentrer le SGDSN sur la gestion des crises rattachée à Matignon au titre de la coordination interministérielle

Le SGDSN aura la responsabilité première de :

- Anticiper les crises et planifier leur gestion au niveau interministériel.

À ce titre, **la direction générale de la sécurité civile,** chargée de l'anticipation, de la coordination et de la gestion des crises au niveau national et international **lui est rattachée,** en liaison avec les zones de défense et de sécurité et leur états-majors interministériels. Devant la récurrence des crises, en particulier liées au changement climatique (incendies, sécheresses, innovations, ouragans…), il conviendra de planifier les besoins en moyens. Le modèle a fait ses preuves au cours du temps et fait partie des meilleurs au monde, il s'agira donc de **poser les arbitrages de priorité sur les investissements en équipements et ressources** nécessaires.

- Pour mettre fin à la faiblesse de notre cybersécurité (10 fuites massives de nos fichiers souverains au cours des 12 derniers mois), avec le risque démultiplicateur désormais de l'IA agentique, il est nécessaire de **construire un dispositif gouvernemental plus clair, plus opérationnel et plus pilotable.** Notre posture doit évoluer d'une simple doctrine de conformité à une approche stratégique critique appelant un effort prioritaire et soutenu dans le temps.
  - Dans le cadre des engagements de la loi de résilience, auditer avec l'ANSSI et le Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI), la vulnérabilité des 15 000 entités identifiées comme essentielles. Coordonner avec l'ANSSI les **missions d'estimation des vulnérabilités numériques de l'architecture nationale et établir les catégories de profils de sécurité**
  - Accélérer les plans de sécurisation des infrastructures de commandement, de contrôle et de communications afin d'achever leur transition vers des normes cryptographiques hybrides d'ici fin 2027 et mettre fin à la capacité d'adversaires de « collecter maintenant et déchiffrer plus tard » nos données sensibles. D'une manière générale, anticiper et planifier les besoins des menaces issues de cryptographie post-quantique et celles conduites par des agents étrangers et des agents non-humains. Le plan PIRANET doit être adapté et prendre en compte l'IA, les API, les modèles de langage et les identités non humaines. Les fuites de secret ont cru de + 80 % en un an à cause de l'IA.
- **Définir un plan de centralisation et de gestion des stocks stratégiques :** la Stratégie Nationale de Résilience (SNR) doit être actualisée pour tenir compte du besoin de diversification et de sécurisation des approvisionnements stratégiques de notre base industrielle et technologique de défense (BITD) en prévision d'un déclenchement d'un conflit majeur ou d'attaques de prédation économique. Cette politique de stocks stratégiques (équipements essentiels notamment dans le domaine NRBC, mais aussi composants et matières premières) devra également intégrer les nouvelles obligations faites aux industriels (par la loi d'actualisation de la loi de programmation militaire votée en 2026) de constituer des stocks stratégiques à leur niveau. Des stress test réguliers seront effectués.

AXE 2

AGIR SUR NOS VULNÉRABILITÉS SYSTÉMIQUES

Augmenter la protection de nos 2 000 OIV (Opérateurs d'Intérêts Vitaux) et SIV (Systèmes d'Importance Vitale)

Renforcer la gouvernance et le pilotage de la résilience des infrastructures essentielles :

- Associer systématiquement aux travaux du comité interministériel de résilience nationale (CIRN) les opérateurs d'infrastructures et les acteurs économiques avec lesquels ils présentent des situations d'interdépendance. Cette intégration permettra de mieux coordonner et suivre les avancées des filières en matière de résilience, et de les accompagner par un budget dédié.
- Généraliser l'attribution de la compétence de la résilience à un élu, *a minima* dans les plus grandes collectivités, en charge du suivi transversal de la résilience sur les différents OIV/SIV.
- Généraliser l'introduction de clauses visant à renforcer la résilience des services dans les contrats de commandes publiques, dans une logique capacitaire (moyens devant être disponibles et mobilisables en cas de crise).

Mettre en place une culture de la résilience, mieux partager les informations et les compétences :

- Systématiser, *via* l'outil du CIRN, le partage d'expérience et de responsabilités entre public et privé: scénarios de projections entre les administrations et les entreprises, méthodologie commune d'identification des vulnérabilités croisées entre les acteurs économiques, retours d'expérience sur les exercices et la gestion de crises.
- Intégrer, dès les exercices préparatoires à la gestion de crises, l'ensemble des acteurs et personnes qui seront impliqués dans une crise d'envergure, pour diffuser les bonnes pratiques et réactions et favoriser un esprit de résilience partagé et éprouvé.
- **Planifier les passations intergénérationnelles des savoirs** indispensables à l'entretien et les opérations d'infrastructures anciennes (pérennité des compétences dans le long ou très long terme, structuration de filières de formation dédiées qui s'appuient sur des nouvelles technologies et mobilisation des anciens des secteurs stratégiques).

Renforcer notre cybersécurité, sur tous les fronts

Nous consacrons 0,15% du PIB à la cybersécurité civile, soit deux fois moins que ce que recommande la cour des comptes 16 juin 2025). L'approche officielle s'est focalisée sur des aspects de nationalité (hébergement national, modèles français) sans suffisamment prendre en compte les aspects de sécurité, en particulier dans le domaine des identités humaines et machines, qui abîment directement notre souveraineté.

Au niveau national

Consolider l'ANSSI comme acteur central d'exécution de notre cybersécurité afin de garantir une gouvernance plus opérationnelle et des résultats probants :

- Élargir les compétences et les responsabilités de l'ANSSI **pour en faire une agence nationale placée directement sous les ordres du Premier ministre et responsable de l'ensemble des capacités cyber interministérielles (à l'exception de la défense).** Ce format permettra de sanctuariser ses effectifs et sa trajectoire budgétaire et de la doter d'une stratégie de développement commun pour l'État selon les recommandations de la Cour des Comptes.
- Donner à l'ANSSI les moyens d'agir et la doter d'une programmation budgétaire pluriannuelle cohérente avec la stratégie nationale actualisée : *a minima*, dès 2027, un budget d'au moins 35 M€ et 60 postes supplémentaires (soit +20% tel que demandé par l'ANSSI en 2025) et une coordination avec les politiques de mise à niveau des infrastructures numériques *(Cf Note Innovation et Technologie)*.
- Sécuriser le vote de la loi de résilience prévue en septembre 2026, reportée depuis 2 ans, et porter de 6 mois à 30 jours les délais de remédiation post-incidents

- Signer des conventions ANSSI-ministères – prestataires d'appui **fixant objectifs, échéancier et moyens cyber, ministère par ministère,** avec une attention particulière concernant l'évolution des plateformes IA agentique et des identités non humaines (NHI).
- Certifier un plus grand nombre de prestataires de cybersécurité et favoriser la création et la solidité de ces entreprises et métiers par de la commande publique (les besoins étant 30 fois supérieurs aux moyens actuels)
- Sortir d'une logique de pompiers qui se mobilisent une fois l'intrusion malveillante identifiée (Unité Cyber voulue par le gouvernement) pour passer à une logique stratégique de renforcement, d'anticipation, d'identification des acteurs malveillants et de contre-attaque préventive.

Mieux protéger les identités numériques humaines et non humaines

Les attaques récentes de ces deux dernières années mettent en avant la facilité déconcertante avec laquelle des attaquants récupèrent des identifiants de personnels autorisés et pénètrent sans force dans nos systèmes numériques.

- **Réinsister sur les bonnes pratiques sécuritaires au sein de l'administration** (mise à jour des logiciels, multi-facteurs d'identification) qui ne sont pas aujourd'hui assurée. Donner un objectif chiffré et un calendrier aux administrations et des pénalités en cas de défaut. Garantir que les budgets de sécurité informatique ne sont pas détournés.
- **Conditionner le plan de déploiement massif de l'IA dans l'administration** (SIAAG – Socle Interministériel d'IA Générative – launched ~March 2026) et visant 1 million de fonctionnaires à un traitement robuste de cybersécurité et interdire les IA clandestines (outils non validés).
- **Mettre en place un plan massif de protection et de détection avancée dans les domaines « identités » (humaines et machines) et « chaînes d'approvisionnement »** qui sont les plus compromis aujourd'hui).

Au niveau local

Étendre le filet de sécurité aux 13000 territoires et les PME qui font partie du nouveau périmètre de la loi de Résilience et qui sont souvent le maillon faible.

- Étendre les outils de cybersécurité du secteur public vers le secteur privé en demande : adapter ***MonServiceSécurisé*** pour le décliner aux acteurs économiques privés : ***MonEntrepriseSécurisée***. Cette plateforme gratuite et collaborative permettra aux dirigeants de PME, cibles privilégiées des rançongiciels, d'obtenir un diagnostic cyber rapide, de piloter collaborativement leur démarche d'homologation, d'accéder automatiquement à un catalogue d'aides et de subventions étatiques directes pour financer l'acquisition de solutions logicielles de confiance qualifiées.
- Conditionner l'obtention de subventions d'équipements de l'État (la DETR pour le monde rural et la DSIL pour l'investissement local) à la réalisation d'un **audit de sécurité initial de conformité au ReCyF** (le Référentiel Cyber France) et à la mise en œuvre d'un plan correctif. Pour le secteur privé (PME/ETI), conditionner le versement des aides de Bpifrance à l'investissement et les subventions du plan France 2030 à la réalisation du **diagnostic obligatoire Cyber PME** (audit de 8 jours pris en charge à 50% par l'État).

AXE 3

DÉVELOPPER UNE CULTURE DE SÉCURITÉ NATIONALE

Actualiser la Défense Opérationnelle du Territoire et renforcer les moyens sécurisant nos Outre-mer

- **Repenser une nouvelle DOT** qui prenne en compte les nouvelles frontières du territoires, physiques autant que numériques. Reconsidérer la protection physique de nos infrastructures critiques, l'entrave des actes de subversion étrangers sur le territoire, mais également la neutralisation des actions de déstabilisation numérique. La répartition des forces sur le territoire doit être rééquilibrée pour englober tous les potentiels d'attaque : spatial, terrestre, maritime et numérique *(Cf. note Sécurité Intérieure et note Défense nationale)*.
- **Intégrer à la DOT un grand plan de cybersécurité** pour adapter notre défense des opérateurs d'importance vitale (OIV) en cas de guerre, en mettant l'accent sur leur interdépendance, et la lutte contre les attaques générées par les agents IA.
- **Anticiper les risques de subversion** actionnée par l'étranger pour entraver nos forces et renverser nos institutions en renforçant l'expertise et les moyens de la gendarmerie mobile.
- Repenser le **système de casernement** dans l'hexagone et nos Outre-mer afin de dessiner un maillage militaire prêt pour une montée en puissance des forces à engager en cas de guerre.
- **Déploiement de moyens supplémentaires de la DGSI,** à hauteur d'une trentaine d'équivalents temps plein (ETP), dotés des moyens techniques nécessaires. Loin de se substituer au renseignement territorial obtenu par la gendarmerie et la police, ce renforcement agira en parfaite complémentarité pour remonter les filières d'agents d'influence, offrant à l'État un véritable levier pour anticiper les crises et faciliter les mesures d'entrave administrative.
- **Déploiement de moyens supplémentaires de la DNRED,** à hauteur d'une dizaine d'équivalents temps plein (ETP), afin de démanteler les filières logistiques et financières visant nos territoires ultramarins, ces filières profitant à la criminalité organisée et pouvant être instrumentalisées dans une logique de subversion.

Créer une réserve de sécurité nationale

Mettre en place une **réserve de sécurité nationale,** fonctionnant comme une réserve civile compétente dans les sujets technologiques pour venir, si besoin, en appui des unités militaires. Les différents dispositifs existants (réserve civile, réserve civique, réserve communale de sécurité civile) devraient être fusionnés, autour de 3 piliers :
- un pilier sécurité intérieure (hors DOT) avec les forces de police déjà en place ;
- un pilier résilience traitant les fonctions de sécurité civile, de réserve sanitaire et de réserve logistique ;
- un pilier cybersécurité avec les experts technologiques compétents.

Un discours annuel du PR sur l'état de notre sécurité nationale

Le président prononcera un discours annuel (sur le modèle du discours sur l'état de l'Union du président américain) devant la représentation nationale réunie en Congrès, consacré à exposer les enjeux de notre sécurité nationale. Ce discours pourrait être suivi (au titre de l'article 18) d'un débat parlementaire permettant à la représentation nationale de s'approprier cette dimension et de s'exprimer chaque année sur ces enjeux.

Développer une communication de prévention envers les citoyens

- Partager avec les médias l'état d'information des menaces afin d'en faire des acteurs responsables auprès du grand public.
- Déclassifier une partie des informations de renseignement afin de matérialiser auprès du grand public la réalité de certaines menaces sous le seuil militaire.

FEUILLE DE ROUTE

DANS LES 100 PREMIERS JOURS

UNE GOUVERNANCE AMÉLIORÉE, DES OBJECTIFS CLAIRS

L'objectif est de poser rapidement les moyens d'une gouvernance rationalisée et d'une approche globale et cohérente fixant les priorités :

- doter le président d'un outil permanent de conception intégrée et de pilotage de la sécurité nationale (reconfiguration de l'état-major particulier par décret) ;
- prioriser le vote de la loi de Résilience si elle n'a pas été votée en septembre 2026 ;
- élaborer une stratégie de sécurité nationale fixant les objectifs prioritaires et la posture stratégique globale, cadre de l'action nationale et de nos partenariats ;
- recentrer le SGDSN sur la préparation et la gestion des crises au niveau interministériel ;
- lancer l'audit sécurité de nos systèmes numériques.

DURANT LE MANDAT

LA MISE EN PLACE D'UNE POLITIQUE PUBLIQUE DE SÉCURITÉ NATIONALE

Le cours du mandat s'attachera à mettre en œuvre une politique publique de sécurité nationale, protégeant nos vulnérabilités systémiques et associant les citoyens et leurs représentants autour de la défense de nos intérêts vitaux.

Cela passe par plusieurs grands chantiers :

- protection accrue pour nos OIV/SIV ;
- renforcement de notre cybersécurité par les déploiements requis ;
- actualisation de la DOT et sécurisation de nos outremers ;
- création d'une réserve de sécurité nationale ;
- discours annuel du Président sur la sécurité nationale devant le Parlement ;
- communication et prévention en direction de nos concitoyens.

À PLUS LONG TERME

ANTICIPER LES MENACES PAR DES STRATÉGIES GLOBALES

Au-delà du mandat présidentiel, la protection de nos intérêts vitaux passera par une action efficace en amont des crises, avant que les menaces ne se concrétisent contre nos intérêts vitaux.

Une culture stratégique de l'anticipation

Cette démarche impose un renforcement de notre capacité d'anticipation, et une révolution dans la manière de concevoir nos stratégies de réponse. Il faudra dépasser une approche en silos pour mobiliser systématiquement l'ensemble des moyens de l'Etat au service d'un objectif stratégique clair et mesurable.

COÛT ET RESSOURCES

Coût

511 M€/an

les 2 premières années

Puis **384 M€/an**

AMÉLIORER LA GOUVERNANCE DE NOTRE SÉCURITÉ NATIONALE : COÛTS CONSTANTS

AGIR SUR NOS VULNÉRABILITÉS SYSTÉMIQUES : 127 M€ PAR AN SUR LES 2 PREMIÈRES ANNÉES

- **Évaluation de la Posture Cyber** des 15 000 Entités de la Loi Résilience (NIS2) : 50 M€/ an sur 2 ans
- **Sécuriser le passage de l'évaluation de la posture (audit) à l'outillage opérationnel effectif** (EDR, SOC/MSSP, durcissement des accès, sauvegardes immuables) pour l'ensemble des 15 000 entités régulées : 140 M€ par an sur 2 ans
- **Supervision - surcouche IA défensive** : 65 M€ par an sur 2 ans

L'enveloppe d'urgence de 200 M€ débloqués par le premier ministre Lecornu suite au breach d'ANTS (30 Avril 2026) et les 50 M€ toujours en réserve dans le plan cyber de France 2030 **couvrent 50 % de ces coûts**.

DÉVELOPPER UNE CULTURE DE SÉCURITÉ NATIONALE : 384 M€/ AN

- **Actualiser la Défense Opérationnelle du Territoire et renforcer les moyens sécurisant nos Outre-mer** : 6 M€ par an
- **Créer une réserve de sécurité nationale** : 378 M€ par an

INDICE D'ACCEPTABILITÉ CITOYENNE

Afin de mesurer l'acceptabilité des réformes proposées, **l'Institut Montaigne et Verian** ont développé un Indice d'Acceptabilité Citoyenne, noté de 0 à 10.

Cet indice synthétise trois dimensions essentielles de l'acceptabilité d'une réforme : son impact perçu pour la société, sa légitimité et son acceptabilité morale, ainsi que l'adhésion personnelle qu'elle suscite.

SÉCURITÉ NATIONALE :
ANTICIPER ET PARER LES MENACES



Il est calculé à partir des réponses des Français à trois questions posées après présentation de chaque projet de réforme. **Plus le score est élevé, plus la réforme est jugée acceptable par les citoyens.**

Les résultats sont issus d'une enquête en ligne réalisée en août et septembre 2026 auprès d'un échantillon de 1500 personnes représentatif de la population française âgée de 18 ans et plus..

MIEUX COMPRENDRE

Budget de la DGSE · Avis de la commission de la défense et des affaires étrangère du Sénat sur le PLF 2025, p. 3.

274 victimes du terrorisme · Compte rendu du conseil des ministres du 12 mars 2025, « Le bilan de la politique de lutte contre le terrorisme ».

800 alertes de sécurité économique · Rapport d'information de l'Assemblée Nationale n° 1757 sur la guerre économique du député Christophe Plassard, juillet 2025, p. 7.

Depuis 2014, les effectifs de la DGSI ont augmenté de 66,1% · Rapport de la Délégation parlementaire pour le renseignement 2018 (p. 94) et Compte rendu du conseil des ministres du 12 mars 2025, « Le bilan de la politique de lutte contre le terrorisme ».

4000 incidents de sécurité sur des entités stratégiques · Rapport d'information de l'Assemblée Nationale n° 1757 sur la guerre économique du député Christophe Plassard, juillet 2025, p. 90.

2 milliards (coût des cyberattaques pour l'économie française en 2022) · Étude économique du cabinet ASTERES « Les cyberattaques réussies en France : un coût de 2 Mds€ en 2022 », juin 2023.

Hausse des effectifs du SGDSN depuis 2019 · Rapport n° 4524 de la commission des finances de l'Assemblée Nationale sur le PLF 2022, annexe 14, p. 12, et Avis de la commission des forces armées et des affaires étrangères du Sénat sur le PLF 2026, Tome IX, « Direction de l'action du gouvernement », p. 5.

Coût de la cybercriminalité. Statista Technology Market Insights.

Délégation parlementaire au renseignement : rapport public pour l'année 2020-2021.

Assemblée nationale: commission de la défense nationale et des forces armées, audition à huis clos, compte rendu n° 54 (avril 2024).

Assemblée nationale : commission d'enquête sur les liens existants entre les représentants de mouvements politiques et des organisations et réseaux soutenant l'action terroriste ou propageant l'idéologie islamiste, audition à huis clos, compte rendu n° 5 (décembre 2025).

Sénat : Rapport n° 379 de la commission d'enquête sur les politiques publiques face au opérations d'influence (juillet 2024).

LE CHAMPS DES CONTRAINTES

Décret n° 2022-665 du 25 avril 2022 portant organisation du secrétariat général de la défense et de la sécurité nationale.

Décret n° 2019-206 du 20 mars 2019 relatif à la gouvernance de la politique de sécurité économique.

Décret n° 2017-1095 du 14 juin 2017 relatif au coordinateur national du renseignement et de la lutte contre le terrorisme, à la coordination nationale du renseignement et de la lutte contre le terrorisme et au centre national de contre-terrorisme.

Arrêté du 19 septembre 2022 fixant l'organisation du secrétariat général de la défense et de la sécurité nationale.

QUELS SONT NOS ATOUTS ?

Hausse du budget du programme 144 depuis 2015 : avis de la commission des forces armées et des affaires étrangères du Sénat sur le PLF 2015, Tome V, « Défense : Environnement et prospective de la politique de défense », p. 5., et Avis de la commission des forces armées et des affaires étrangères du Sénat sur le PLF 2026, Tome V, « Défense », p. 6.

Rapport d'enquête Verian, « Les Français et la désinformation provenant de pays étrangers » (septembre 2025).

DANS LE DÉBAT

Idée du débat n° 1

Revue Nationale Stratégique, juillet 2025.

Avis de la commission des finances du Sénat sur le PLF 2026, Tome IX « Sécurités », Gendarmerie Nationale (programme 152).

DIEFENBACHER, Jean-Wilfried et ISRAEL, Nicolas, *Réarmement français et métaux critiques : l'angle mort stratégique*, Revue de Défense Nationale n° 892, été 2026.

Idée du débat n° 2

Institut Montaigne, *Du risque à la résilience : s'adapter collectivement* (octobre 2022).

Projet annuel de performance, annexe au Projet de loi de finances pour 2026, programme 163.

Projet de loi actualisant la loi de programmation militaire 2024-2030.

Rapport de la Cour des Comptes : « La réponse de l'État aux cybermenaces sur les SI civils », 2025.

Rapport général de la commission des finances du Sénat sur le PLF 2026.

LA RECOMMANDATION DE MONTAIGNE

BAVEREZ, Nicolas, *Sécurité nationale, quels moyens pour quelles priorités*, Institut Montaigne, avril 2017.

BUFFOTOT, Patrice, « Les Livres blancs sur la défense sous la Ve République », *Paix et sécurité européenne et internationale*, n° 2, 2015.

BUFFOTOT, Patrice, « La Revue stratégique de défense et de sécurité nationale 2017 et le projet de Loi de programmation militaire 2019-2025 », *Paix et sécurité européenne et internationale*, n° 9, 2018.

COSTE, Frédéric, *L'adoption du concept de sécurité nationale : une révolution conceptuelle qui peine à s'exprimer*, Recherches & Documents n° 03/2011, Fondation pour la Recherche Stratégique (FRS), 2011.

GUIFFARD, Jonathan, *Pour une administration stratégique de notre sécurité nationale*, Institut Montaigne, Janvier 2025.

INSTITUT MONTAIGNE, *Refonder la sécurité nationale*, septembre 2016.

KREPINEVICH, Andrew F. et WATTS, Barry D., *Regaining Strategic Competence*, Center for Strategic and Budgetary Assessments (CSBA), 2009.

les REPÈRES de MONTAIGNE

Cette note, publiée par l'Institut Montaigne, fait partie de la collection :
Les repères de Montaigne, 25 recommandations pour la France
Dépôt légal : Octobre 2026
Sous la direction générale de Marie-Pierre de Bailliencourt
Enquête territoriale : Institut Enterritoires
Enquête d'acceptabilité : Verian

Design graphique : Élodie Ruiz ; Studio Nathalie Bastide
Mise en page : Matthieu Mercier



Imprimé en France par Maqprint
ISSN : 1771-6756

Institut Montaigne
59 rue La Boétie, 75008 Paris
Tel. +33 (0)1 53 89 05 60
institutmontaigne.org

INSTITUT Montaigne

MÉTHODOLOGIE

Chaque note est le produit d'une réflexion collégiale. Celle-ci mobilise **25 années d'expertise en politiques publiques, plusieurs mois de revue de littérature scientifique et d'analyses de données officielles sourcées.** Elle s'appuie sur des auditions de chercheurs, d'économistes et d'experts indépendants, ainsi que sur des échanges réguliers avec les entreprises adhérentes de l'Institut Montaigne, des élus et des personnalités œuvrant au quotidien dans les territoires.

Nous avons tenu compte des idées présentes dans le débat politique et des attentes exprimées par les Français, telles qu'elles ressortent des enquêtes et sondages de ces derniers mois. Les mesures que nous proposons découlent ainsi d'arbitrages pris dans l'intérêt de la France en conciliant efficacité, faisabilité opérationnelle et acceptabilité citoyenne.

MERCI !

L'Institut Montaigne remercie chaleureusement son comité directeur, ses équipes internes, les experts permanents et associés, les entreprises adhérentes ainsi que l'ensemble de ses partenaires, qui ont contribué pendant 18 mois à l'élaboration de ces notes.

INSTITUT Montaigne

REPÈRES POUR LA FRANCE

L'Institut Montaigne, espace de réflexion indépendant et apartisan, au service de l'intérêt général, s'engage dans la préparation de l'élection présidentielle 2027.

Parce que nous pensons qu'il est indispensable de favoriser un débat démocratique sur le fond, réaliste et nuancé, **nous publions 25 notes thématiques pour informer les citoyens et inspirer les candidats.**
En diffusant un contenu accessible à tous, nous souhaitons **donner des repères sur l'état réel de la France, poser un diagnostic et encourager les arbitrages nécessaires** au service de 4 ambitions : créer de la richesse, vivre ensemble, se protéger et mettre en œuvre nos politiques publiques.

Cette initiative vise à restaurer la confiance politique et à dessiner pour la France un futur désirable.