ASSEMBLÉE NATIONALE

XVIIe LÉGISLATURE

Rapport d'information n° 1757

La guerre économique

COMMISSION DES FINANCES

JUILLET 2025

Christophe Plassard
Rapporteur spécial

DOCUMENTS D'INFORMATION

www.assemblee-nationale.fr

ASSEMBLÉE NATIONALE

N° 1757

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 16 juillet 2025.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 146 du Règlement

PAR LA COMMISSION DES FINANCES, DE L'ÉCONOMIE GÉNÉRALE ET DU CONTRÔLE BUDGÉTAIRE

sur la **guerre économique**

ET PRÉSENTÉ PAR

M. CHRISTOPHE PLASSARD,
rapporteur spécial

SOMMAIRE

—

Pages

SYNTHÈSE

● La base industrielle et technologique de défense (BITD) est confrontée à un niveau de menace élevé.

La menace s'intensifie. Le nombre d'atteintes caractérisées contre des entités de la BITD ou des organismes de recherche de défense se situe entre 500 et 550 par an. On compte par ailleurs 750 à 800 alertes de sécurité économique chaque année contre des entreprises ou des actifs stratégiques, soit plus du double de 2020 (1).

80 % des atteintes visent les PME. Nos compétiteurs stratégiques tentent d'attaquer les grands groupes et de paralyser nos chaînes de valeur en visant les sous-traitants qui ont de moindres capacités à se défendre.

Les menaces sont de plus en plus protéiformes. Si les atteintes physiques (vols, intrusions non autorisées, sabotages) et les atteintes humaines (espionnage stratégique, économique et technologique) restent importantes, elles s'accompagnent de menaces informatiques, juridiques (*lawfare*), capitalistiques et informationnelles.

Les menaces viennent de tous nos compétiteurs stratégiques. Les ingérences étrangères les plus graves proviennent naturellement de la Russie et de la Chine ainsi que d'autres pays dont l'industrie de défense est concurrente de la nôtre, mais certaines proviennent aussi de pays qui sont nos alliés sur le plan géostratégique, en tête desquels les États-Unis.

● Les services de l'État ont renforcé les moyens qu'ils consacrent à l'intelligence économique et se sont réorganisés afin de mieux assurer leurs missions de sécurité et de promotion économiques.

La **direction générale de l'armement** (DGA) exerce depuis longtemps une compétence en matière d'intelligence économique et de protection des entreprises de la BITD. La création d'une direction de l'industrie de défense, actée en 2024, a renforcé la concentration des moyens alloués par le ministère des armées à ces sujets, avec une trentaine de créations de postes et de nouveaux leviers d'action (bureau cyber, campus OSINT, posture plus offensive).

Le **service de l'information stratégique et de la sécurité économiques** (SISSÉ), qui pilote et coordonne au niveau interministériel la protection des entreprises, technologies et organismes de recherche stratégiques, est monté en puissance depuis 2020 et a pris une ampleur à la mesure des enjeux de sécurité économique. Ses effectifs ont augmenté de 24 ETP en 2016 à 32 ETP en 2025, auxquels s'ajoutent 24 délégués régionaux.

---

(1) Les alertes de sécurité économique incluent une partie des atteintes enregistrées contre des entités de la BITD ou de la recherche de défense ; les deux chiffres ne peuvent donc pas s'additionner.

Les **services de renseignement**, en particulier la direction du renseignement et de la sécurité de la défense (**DRSD**) et la direction générale de la sécurité extérieure (**DGSE**) pour ce qui concerne la BITD, sont aussi plus actifs. La stratégie nationale du renseignement de 2019 compte la défense et la promotion de nos intérêts économiques et industriels parmi les enjeux prioritaires. Les moyens alloués à la contre-ingérence économique tendent à rattraper ceux prévus pour la lutte contre le terrorisme.

● Plusieurs dispositifs de sécurité économique ont été renforcés pour accroître les moyens d'action de l'État.

Le **contrôle des investissements étrangers en France** (IEF) a été **modernisé**, avec un élargissement de la liste des investissements soumis à autorisation, une extension des secteurs et des technologies considérés comme stratégiques et un durcissement des sanctions. S'il est essentiel de maintenir l'attractivité économique de la France, les flux de capitaux étrangers au sein de la BITD doivent rester maîtrisés. Lorsque des intérêts nationaux sont en jeu, la DGA négocie avec les investisseurs étrangers une lettre d'engagement destinée à éviter le pillage, la vente à la découpe, la sortie des centres de R&D du territoire national voire à mettre sous cloche les activités stratégiques. Pas moins de **deux cents lettres d'engagement** sont actives, dont la DGA assure un suivi strict, assorti de pénalités si elles ne sont pas respectées. Seules deux marges de progression ont pu être identifiées par le rapporteur spécial : mieux anticiper la sortie des fonds d'investissement et développer la pratique des *proxy boards* pour renforcer le suivi des engagements imposés aux investisseurs étrangers.

Recommandation n° 1 : Dans le cadre du contrôle des investissements étrangers en France, mieux anticiper la sortie des fonds d'investissement.

Recommandation n° 2 : Dans le cadre du contrôle des investissements étrangers en France, généraliser la pratique du conseil d'administration alternatif (*proxy board*) pour renforcer le suivi des engagements imposés aux investisseurs étrangers.

La **loi de blocage du 26 juillet 1968** a été **réactivée**. Elle interdit à toute personne physique de nationalité française de communiquer à des autorités publiques étrangères des renseignements de nature à porter atteinte à la souveraineté de la France. Elle interdit aussi à toute personne de demander de tels renseignements dans le cadre de procédures judiciaires ou administratives étrangères. Les modalités d'application du dispositif ont été précisées au niveau réglementaire, avec le SISSÉ désigné en tant que guichet unique. Longtemps inappliquée, la loi est devenue crédible et confère désormais une réelle protection aux entreprises et personnes subissant des demandes d'information abusives de la part d'autorités étrangères. Le **nombre de saisines** a été **multiplié par cinq** par rapport à la période antérieure. Le rapporteur spécial salue l'action des services de l'État, qui sont parvenus à redonner à un outil ancien une utilité réelle. Il relève toutefois la faiblesse des sanctions encourues et recommande d'alourdir le montant des amendes.

Recommandation n° 3 : Alourdir le montant des amendes pouvant être prononcées en cas de méconnaissance de la loi de blocage.

Les moyens consacrés à la **cybersécurité** des entreprises ont également été renforcés, à la fois au niveau de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour les groupes les plus stratégiques et de la DRSD pour les PME de la BITD. La DGA a mis place un référentiel de maturité cyber, afin d'aider les entreprises à élever leur niveau de protection, ainsi qu'une prise en charge partielle des frais de cybersécurisation.

● **Un cadre juridique national complet et efficace, qui appelle peu d'évolutions législatives ou réglementaires, mais des moyens budgétaires et humains supplémentaires**.

Augmenter les moyens des services de l'État chargés de protéger et de soutenir les actifs stratégiques permettrait de renforcer leurs moyens d'action et d'améliorer encore leur coordination.

Recommandation n° 4 : Augmenter les moyens humains et budgétaires alloués aux services de l'État chargés de la protection des actifs stratégiques.

En outre, le rapporteur spécial estime nécessaire d'ouvrir une réflexion sur la possibilité de réaliser des enquêtes administratives et de délivrer des avis de sécurité pour des personnes souhaitant travailler dans la BITD préalablement à leur recrutement. Une telle possibilité permettrait de constituer un vivier de personnes autorisées ou habilitées dans lequel les entreprises de l'industrie de défense pourraient rapidement trouver la main-d'œuvre dont elles ont besoin, pour couvrir des besoins de recrutement urgents ou temporaires. Cela supposerait d'accélérer la hausse des moyens de la DRSD.

Recommandation n° 5 : Renforcer les moyens budgétaires et humains alloués aux services d'enquête de la DRSD, et envisager un nouveau cadre juridique autorisant la constitution d'un vivier de travailleurs autorisés ou habilités à la disposition des entreprises de la BITD en cas de recrutements urgents ou temporaires.

Les actions de sensibilisation aux risques et aux bonnes pratiques doivent se poursuivre et s'amplifier. Les organismes de recherche, en particulier, présentent des vulnérabilités qui peuvent en faire des cibles pour nos compétiteurs. Les étudiants des écoles d'ingénieurs sous la tutelle du ministère des armées gagneraient aussi à être davantage sensibilisés aux enjeux de la guerre économique.

Recommandation n° 6 : Renforcer la sensibilisation des étudiants des écoles d'ingénieurs sous la tutelle du ministère des armées aux enjeux de la guerre économique.

Afin de renforcer la protection des connaissances et savoir-faire stratégiques dans les entreprises et les organismes de recherche, le rapporteur propose de rendre le cadre réglementaire relatif à la protection du potentiel scientifique et technique (PPST) plus contraignant, en imposant aux entreprises et organismes de recherche les plus critiques de recourir au dispositif, aujourd'hui facultatif.

Recommandation n° 7 : Rendre le cadre relatif à la protection du potentiel scientifique et technique de la nation plus contraignant, notamment pour les entreprises et les organismes de recherche les plus critiques, en renforçant les dispositifs d'accompagnement.

Une évolution progressive de nos outils de télécommunications et messagerie ainsi que de nos moyens de stockage numérique vers des solutions souveraines et sécurisées est possible. Les acteurs français, qui existent et qui constituent une alternative crédible, ne pourront se développer et acquérir une taille critique que s'ils reçoivent des commandes. Un certain degré de contrainte paraît nécessaire, pour imposer aux entreprises, y compris celle de la BITD, d'utiliser des solutions françaises ou européennes, et d'éviter de recourir à certains prestataires lorsqu'il existe une incertitude sur le stockage des données. Au delà de la seule question de la BITD, le rapporteur spécial estime en outre que les élus de la Nation ont un devoir d'exemplarité dans l'utilisation d'outils numériques sécurisés.

Recommandation n° 8 : Imposer progressivement aux entreprises de la BITD un très haut niveau de protection des données, impliquant le stockage de données sensibles sur des serveurs situés en France ou sur le territoire de l'Union européenne.

Longtemps naïve, l'Union européenne semble progressivement prendre conscience de la nécessité de se défendre elle-même. Sous l'impulsion de la France, l'Union européenne s'est dotée d'outils destinés à renforcer et harmoniser le contrôle des investissements des étrangers. Ce système comporte encore des lacunes, mais la Commission européenne a initié une révision du règlement en vigueur.

La meilleure manière de contrer certaines normes étrangères à portée extraterritoriale dont se servent certains de nos compétiteurs pour atteindre nos entreprises est d'adopter des réglementations équivalentes pour pouvoir les opposer aux autorités étrangères. À cet égard, le rapporteur spécial estime que la loi de blocage du 26 juillet 1968 a fait ses preuves au niveau national et gagnerait à trouver une équivalence au niveau européen.

Recommandation n° 9 : Sur le modèle de la loi de blocage du 26 juillet 1968, adopter un règlement de blocage au niveau de l'Union européenne.

Dans la même perspective, la création d'un label de type « Itar » au niveau européen permettrait aux États membres de l'Union européenne – qui constitueraient collectivement une masse critique suffisante – de s'opposer à certaines demandes abusives des autorités américaines vis-à-vis de leurs entreprises stratégiques, voire de réaliser des contrôles similaires auprès d'entreprises ou d'investisseurs étrangers.

Recommandation n° 10 : Mettre en place un label de type « Itar » au niveau de l'Union européenne.

● **Face aux difficultés de financement des PME de la BITD, qui perdurent, la nécessité de trouver de nouvelles sources financement innovantes**.

Malgré un contexte de plus en plus favorable au financement de l'industrie de défense, au niveau national, dans la continuité de la conférence du 20 mars 2025, comme au niveau européen, un certain nombre de PME auditionnées par le rapporteur spécial ont encore récemment rencontré des refus de financement en raison de leur appartenance au secteur de la défense.

Il est tout d'abord nécessaire de réserver les financements européens, en particulier ceux du programme EDIP, aux matériels européens, développés et produits par des entreprises européennes sur le sol européen, afin qu'ils puissent être utilisés, maintenus en condition opérationnelle et modifiées par les armées sans restriction de la part d'un pays tiers.

Recommandation n° 11 : Dans le cadre du programme européen d'investissement dans la défense (EDIP), réserver les financements européens aux matériels européens – composés d'au moins 65 % de pièces développées et produites par des entreprises européennes sur le sol européen – et dont l'autorité de conception est européenne, en limitant les exceptions.

Par ailleurs, les fonds publics visant à protéger les entreprises et les technologies stratégiques ou innovantes demeurent insuffisants : leur dotation est limitée, le nombre d'opérations réalisées chaque année est faible et ils sont difficilement mobilisables pour des levées de fonds de plus de 20 millions d'euros. Le rapporteur spécial appelle donc une nouvelle fois à augmenter les moyens budgétaires alloués par l'État à la protection des entreprises stratégiques et des technologies sensibles, de façon à maximiser les effets de levier qu'il est possible d'obtenir en associant des fonds publics et des fonds d'investissement privés.

Recommandation n° 12 : Renforcer les moyens budgétaires alloués aux fonds publics destinés à la protection des entreprises stratégiques et des technologies sensibles (notamment Definvest et le fonds pour l'innovation de défense).

Les moyens d'action de l'Agence des participations de l'État (APE) pour la protection des entreprises et des technologies stratégiques pourraient être renforcés. Le produit des dividendes perçus par l'État pourrait ainsi être affecté au compte d'affectation spéciale *Participations financières de l'État*, afin de conférer à l'APE une possibilité d'intervention contra-cyclique.

Recommandation n° 13 : Pour accroître le rôle de l'Agence des participations de l'État dans la protection des entreprises stratégiques, affecter le produit des dividendes perçus par l'État au compte d'affectation spéciale *Participations financières de l'État*.

Il n'en demeure pas moins que remédier aux difficultés de financement des entreprises de la BITD passe avant tout par une meilleure mobilisation des fonds privés. Le rapporteur spécial salue les récentes annonces relatives à la création de fonds de *private equity* ouverts aux particuliers souhaitant investir dans la BITD. Toutefois, compte tenu du volume d'épargne disponible, il réitère sa proposition de créer un livret défense et souveraineté ou de flécher une partie des encours des livrets réglementés vers les PME de la BITD. En s'adressant à un public plus large, un tel fléchage aurait une portée symbolique plus forte. Il monterait la détermination

de l'État à protéger ses intérêts nationaux. Il permettrait également de mobiliser non seulement l'épargne des Français, mais aussi les Français eux-mêmes, autour de la protection des entreprises stratégiques.

Recommandation n° 14 : Créer un livret défense et souveraineté ou flécher une partie des encours du livret A et du livret de développement durable et solidaire vers les PME de l'industrie de défense.

Enfin, le rapporteur spécial appelle à plus de cohérence fiscale pour contrer les menaces capitalistiques et soutenir les entreprises stratégiques. À l'heure actuelle, une large partie de l'épargne part à l'étranger, notamment aux États-Unis, à la recherche de rendements plus élevés. Afin d'inciter les épargnants à investir dans l'économie française, ou européenne, il pourrait être envisagé de créer un crédit d'impôt spécifique qui permettrait de réduire le montant de l'imposition due au titre des produits des investissements dans des entreprises établies en France ou au sein de l'Union européenne.

Recommandation n° 15 : Créer un crédit d'impôt permettant de réduire l'imposition due au titre des produits des investissements dans les entreprises françaises et européennes.

Enfin, bien que la France dispose d'un cadre juridique solide, éprouvé et exemplaire en matière de vente d'armes et de biens à double usage, certaines banques se permettent de refuser de financer des opérations qui ont pourtant été autorisées par l'État. En conséquence, le rapporteur spécial estime nécessaire d'envisager la possibilité de conférer aux licences d'exportation délivrées par l'État un caractère plus contraignant, qui s'impose d'une manière ou d'une autre aux établissements bancaires.

Recommandation n° 16 : Envisager une évolution du cadre législatif permettant de conférer aux licences d'exportation délivrées par l'État un caractère contraignant pour les établissements bancaires.

LISTE DES RECOMMANDATIONS

Recommandation n° 1 : Dans le cadre du contrôle des investissements étrangers en France, mieux anticiper la sortie des fonds d'investissement.

Recommandation n° 2 : Dans le cadre du contrôle des investissements étrangers en France, généraliser la pratique du conseil d'administration alternatif (*proxy board*) pour renforcer le suivi des engagements imposés aux investisseurs étrangers.

Recommandation n° 3 : Alourdir le montant des amendes pouvant être prononcées en cas de méconnaissance de la loi de blocage.

Recommandation n° 4 : Augmenter les moyens humains et budgétaires alloués aux services de l'État chargés de la protection des actifs stratégiques.

Recommandation n° 5 : Renforcer les moyens budgétaires et humains alloués aux services d'enquête de la DRSD, et envisager un nouveau cadre juridique autorisant la constitution d'un vivier de travailleurs autorisés ou habilités à la disposition des entreprises de la BITD en cas de recrutements urgents ou temporaires.

Recommandation n° 6 : Renforcer la sensibilisation des étudiants des écoles d'ingénieurs sous la tutelle du ministère des armées aux enjeux de la guerre économique.

Recommandation n° 7 : Rendre le cadre relatif à la protection du potentiel scientifique et technique de la nation plus contraignant, notamment pour les entreprises et les organismes de recherche les plus critiques, en renforçant les dispositifs d'accompagnement.

Recommandation n° 8 : Imposer progressivement aux entreprises de la BITD un très haut niveau de protection des données, impliquant le stockage de données sensibles sur des serveurs situés en France ou sur le territoire de l'Union européenne.

Recommandation n° 9 : Sur le modèle de la loi de blocage du 26 juillet 1968, adopter un règlement de blocage au niveau de l'Union européenne.

Recommandation n° 10 : Mettre en place un label de type « Itar » au niveau de l'Union européenne.

Recommandation n° 11 : Dans le cadre du programme européen d'investissement dans la défense (EDIP), réserver les financements européens aux matériels européens – composés d'au moins 65 % de pièces développées et produites par des

entreprises européennes sur le sol européen – et dont l'autorité de conception est européenne, en limitant les exceptions.

Recommandation n° 12 : Renforcer les moyens budgétaires alloués aux fonds publics destinés à la protection des entreprises stratégiques et des technologies sensibles (notamment Definvest et le fonds pour l'innovation de défense).

Recommandation n° 13 : Pour accroître le rôle de l'Agence des participations de l'État dans la protection des entreprises stratégiques, affecter le produit des dividendes perçus par l'État au compte d'affectation spéciale *Participations financières de l'État.*

Recommandation n° 14 : Créer un livret défense et souveraineté ou flécher une partie des encours du livret A et du livret de développement durable et solidaire vers les PME de l'industrie de défense.

Recommandation n° 15 : Créer un crédit d'impôt permettant de réduire l'imposition due au titre des produits des investissements dans les entreprises françaises et européennes.

Recommandation n° 16 : Envisager une évolution du cadre législatif permettant de conférer aux licences d'exportation délivrées par l'État un caractère contraignant pour les établissements bancaires.

INTRODUCTION

Le présent rapport, initialement prévu pour être présenté en 2024, n'avait pu être publié en raison de la dissolution de l'Assemblée nationale. L'arrivée de M. Donald Trump à la présidence des États-Unis, la menace d'une remontée brutale des droits de douane et la bascule stratégique globale initiée par l'allié historique de l'Europe n'ont fait que confirmer les constats posés par le rapporteur spécial il y a un an. **La guerre est bien de retour**, sous toutes ses formes : la **guerre traditionnelle**, celle que l'on observe en Ukraine, dans certains pays d'Afrique et au Moyen-Orient ; la **guerre hybride**, qui se déploie à coups d'ingérences étrangères, de cyberattaques ou encore de manipulations de l'information ; et la **guerre économique**, qui oppose nos entreprises à celles de nos compétiteurs stratégiques.

Sans traiter en intégralité la question, dont tous les aspects ne relèvent pas du domaine de compétences de la commission des finances, le rapport se concentre sur les **menaces qui pèsent sur la base industrielle et technologique de défense** (BITD), dans un contexte de durcissement des rapports de forces économiques internationaux, ainsi qu'aux moyens mobilisés par l'État, en particulier ceux de la mission *Défense*, pour protéger et soutenir les actifs stratégiques de la France.

La notion de **guerre économique** est proche de celle d'intelligence économique sans se confondre totalement avec elle. La guerre économique peut être définie comme une confrontation entre différentes parties qui cherchent à capter, contrôler et accaparer des richesses afin d'accroître leur puissance par l'économie [(1)]. La notion d'**intelligence économique** renvoie quant à elle, selon la définition qui s'est imposée depuis le rapport Martre de 1994 [(2)], aux actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques (État, entreprises, organismes de recherche).

Au cours des **vingt-neuf auditions** qu'il a menées, en 2024 puis en 2025, le rapporteur spécial a pu constater que la notion de guerre économique ne faisait pas l'unanimité. Pour certains, le mot **guerre** serait inutilement belliqueux et donnerait l'impression que l'ensemble des rapports de forces économiques se réduisent à une logique de combat. D'autres, préférant le concept d'**ingérence**, soulignent que la guerre est supposée opposer uniquement des ennemis en conflit armé, tandis que la compétition économique internationale met aussi en concurrence, y compris en temps de paix, des pays qui sont alliés sur un plan militaire ou géostratégique.

Les termes de guerre économique n'en sont pas moins assumés par un courant de l'intelligence économique. La guerre économique y est analysée comme

(1) Définition du centre de recherche CR451 rattaché à l'École de guerre économique.

(2) Commissariat général du plan, « Intelligence économique et stratégie des entreprises », travaux du groupe présidé par M. Henri Martre, février 1994.

« *la poursuite de la guerre par d'autres moyens* » et « *un mode de domination qui évite de recourir à l'usage de la puissance militaire pour imposer une suprématie durable. Il ne s'agit plus de soumettre l'autre par la force, mais de le rendre dépendant par la technologie. À la volonté guerrière des anciens empires se substitue désormais une forme de duplicité des nouveaux conquérants qui instrumentalisent la morale afin de masquer la finalité de leur stratégie* » (1).

Ces termes étaient d'ailleurs repris en première page du rapport Carayon de 2003 (2), qui constatait que « *la compétition s'est exacerbée entre États, entre entreprises. Prix et spécificités des produits ou services ne constituent plus exclusivement les facteurs déterminants de conquête des marchés* » et qui évoquait un « *climat de guerre économique où tous les coups sont permis* ».

La théorisation de la guerre économique s'étend même au delà de nos frontières. Ainsi, deux anciens hauts gradés de l'armée de l'air chinoise, prenant acte du différentiel de puissance entre la Chine et les États-Unis et de l'impossibilité pour leur pays de défaire militairement son adversaire, ont-ils théorisé **la guerre hors limites**, c'est-à-dire la poursuite de la guerre dans tous les autres espaces possibles : économique, technologique, juridique, social (3).

Dans cette perspective, le rapporteur spécial est allé à la rencontre des militaires, des services de renseignement et d'un certain nombre d'entreprises, petites et grandes, dont l'identité est volontairement gardée confidentielle, afin de ne pas les exposer et de conserver la plus grande liberté de parole possible. Le présent rapport dresse **un état des lieux des menaces pesant sur la BITD en matière de guerre économique** et des **moyens mobilisés par l'État** pour assurer la protection et la promotion de nos intérêts économiques. Dans la continuité de ses travaux sur l'économie de guerre (4) et sur l'orientation de l'épargne réglementée vers l'industrie de défense (5), le rapporteur spécial analyse aussi plus particulièrement les **difficultés d'accès aux financements des PME de l'industrie de défense** ainsi que les solutions qui pourraient permettre d'y remédier.

Les constats et les propositions du rapporteur spécial rejoignent en partie ceux du rapport sur la sécurité économique des entreprises remis par M. Geoffroy Roux de Bézieux au Président de la République en octobre 2024, et dont le contenu

---

(1) Christian Harbulot, « Trente ans de travaux sur la guerre économique », Cahiers de la guerre économique, n° 1, mars 2020, page 29.

(2) M. Bernard Carayon, « Intelligence économique, compétitivité et cohésion sociale », rapport remis au Premier ministre le 1er juillet 2003.

(3) Qiao Liang et Wang Xiangsui, « La guerre hors limites. Réflexion sur l'art de la guerre à l'époque de la mondialisation », 1999.

(4) Assemblée nationale, rapport d'information n° 1023 (XVIe législature) de M. Christophe Plassard sur l'économie de guerre, déposé en application de l'article 146 du règlement par la commission des finances, de l'économie générale et du contrôle budgétaire, enregistré à la présidence le 29 mars 2023.

(5) Assemblée nationale, rapport n° 224 (XVIe législature) de M. Christophe Plassard, fait au nom de la commission des finances, de l'économie générale et du contrôle budgétaire, sur la proposition de loi visant à flécher l'épargne non centralisée des livrets réglementés vers les entreprises du secteur de la défense nationale (n° 2094), enregistré à la présidence le 28 février 2024.

est classifié. On peut notamment noter que la BITD y est considérée comme un secteur particulièrement bien organisé et protégé, dont l'ensemble des domaines d'activité ont vocation à s'inspirer.

I. LA BASE INDUSTRIELLE ET TECHNOLOGIQUE DE DÉFENSE MENACÉE DANS UN CONTEXTE DE GUERRE ÉCONOMIQUE ACCRU

Les menaces qui pèsent sur la BITD en matière de guerre économique sont non seulement en hausse mais aussi de plus en plus protéiformes. Elles concernent à la fois les entreprises, en particulier les PME, et les laboratoires, les organismes de recherche ou encore les écoles d'ingénieur sous tutelle du ministère des armées, avec des moyens toujours plus intrusifs et agressifs.

A. UN NIVEAU DE MENACE ÉLEVÉ

Les menaces qui pèsent sur la BITD en matière de guerre économique tendent à s'amplifier. La résurgence des **tensions géopolitiques** s'accompagne d'une intensification de la **compétition économique internationale**. L'accélération du rythme de l'innovation et le caractère systémique des technologies contribuent à durcir les **rapports de forces entre les grandes zones économiques mondiales**. Depuis 2020, les perturbations liées à la pandémie de covid ont accéléré la montée des préoccupations souveraines, notamment sur l'accès aux matières premières, aux composants et aux ressources stratégiques. De même, le conflit militaire qui oppose l'Ukraine à l'agresseur russe, et qui possède une dimension économique prégnante, a relancé la production d'armement à l'échelle mondiale.

En 2024, M. Sébastien Lecornu, ministre des armées avait indiqué que **le nombre d'atteintes physiques contre des entités de la BITD tend à augmenter** – d'une quarantaine de cas relevés en 2021 à une cinquantaine en 2022 et 2024 – précisant qu'il parlait là non pas de « *petites cyberattaques* » mais « *d'opérations beaucoup plus structurées et documentées menées par des individus qui, au gré d'une visite, au gré d'un cambriolage qui apparaît comme anodin, tentent de s'introduire au sein de notre industrie de défense pour le compte d'un acteur étranger* » (1).

Ses propos ont été confirmés par M. Emmanuel Chiva, délégué général pour l'armement, qui évoquait « ***une augmentation significative des attaques****, qu'il s'agisse de délits de droit commun, de rackets, ou d'actions liées au conflit en Ukraine* » visant à « *neutraliser* » ou à « *voler des données* ». Il ajoutait qu'« *[a]u-delà de la cyberprotection, la sécurité physique des entreprises est également préoccupante. Nous constatons une multiplication d'incidents comme des incendies ou des dégradations, potentiellement intentionnels. Je rappelle l'incendie d'une usine en Allemagne fabriquant des missiles utilisés en Ukraine, probablement d'origine criminelle* ». Il soulignait en outre que toutes les atteintes n'étaient pas détectées, et que « *[l]a découverte tardive de vols de données soulève la question de leur durée et de l'ampleur réelle du problème* » (2).

---

(1) Sénat, audition de M. Sébastien Lecornu, ministre des armées, par la commission d'enquête sur les politiques publiques face aux opérations d'influences étrangères, 25 juin 2024.

(2) Assemblée nationale, audition de M. Emmanuel Chiva, délégué général pour l'armement, par la commission de la défense nationale et des forces armées, sur le projet de loi de finances pour 2025, 23 octobre 2024.

La direction du renseignement et de la sécurité de la défense (DRSD), chargée de la protection de la BITD, relève également **un niveau de menace élevé** et qui tend à augmenter. Depuis 2022, on dénombre, chaque année, **entre 500 et 550 atteintes contre des entités de la BITD ou de la recherche de défense**. La tendance se poursuit en 2025, avec près de 300 atteintes recensées à la fin du mois de juin. **Ces chiffres doivent** toutefois **être nuancés**. Les atteintes ainsi dénombrées représentent les actes qui font l'objet d'un signalement et que l'on parvient à caractériser. N'y sont donc pas inclus les incidents qui ne remontent pas auprès des services de l'État, ni ceux pour lesquels il n'existe pas la preuve d'une intention malveillante liée à une action de guerre économique ou à une ingérence de la part d'un État étranger. Il n'en demeure pas moins, comme l'ensemble des personnes entendues par le rapporteur spécial le lui ont indiqué, que **la menace s'intensifie**. Le **nombre réel d'atteintes** est **probablement très supérieur** à celui relevé, même s'il est impossible de le mesurer de manière précise et exhaustive.

B. LES SOUS-TRAITANTS SONT PLUS PARTICULIÈREMENT VISÉS

Plus que d'autres pays européens, **la France est une cible privilégiée**, parce qu'elle est l'un des plus grands États membres de l'Union européenne, qu'elle organise des événements internationaux majeurs – comme les jeux olympiques et paralympiques ainsi que les salons de l'armement tels que le Bourget, Eurosatory et Euronaval –, qu'elle ambitionne de jouer un rôle de puissance d'équilibre sur la scène internationale et que son attitude et sa parole ne laissent pas indifférent.

En particulier, **la base industrielle et technologique de défense** (**BITD**) – ses 4 000 entreprises, et notamment ses 1 200 entités les plus critiques – est l'objet de convoitises. Sa capacité à produire des équipements performants et innovants suscite l'intérêt de nos compétiteurs, soucieux de saper notre outil de défense, de réduire notre autonomie stratégique et / ou de favoriser leur propre industrie. Les menaces se concentrent singulièrement sur des **domaines stratégiques** dans lesquels la France a acquis une certaine expertise. Environ un tiers des attaques concernent ainsi les secteurs de l'**aéronautique** et du **spatial**. Sont aussi visés les technologies de l'information et de la communication, l'armement et les véhicules terrestres, la construction navale, les matériaux, la métallurgie, la chimie, et toutes les technologies innovantes dans lesquelles la France dispose de savoir-faire d'excellence.

Si les grands donneurs d'ordre, qui ont acquis une position dominante au niveau européen ou mondial, sont naturellement des cibles, **80 % des atteintes visent** néanmoins **les sous-traitants**. Tandis que les grands groupes ont les moyens financiers et humains de déployer des capacités de protection importantes, les petites et moyennes entreprises, plus isolées, sont naturellement moins bien préparées et donc plus exposées aux risques d'atteinte ou d'ingérence étrangère. Les *start-ups* développant des innovations de rupture liées aux enjeux de souveraineté du futur, notamment, sont à la fois des cibles particulièrement menacées et vulnérables.

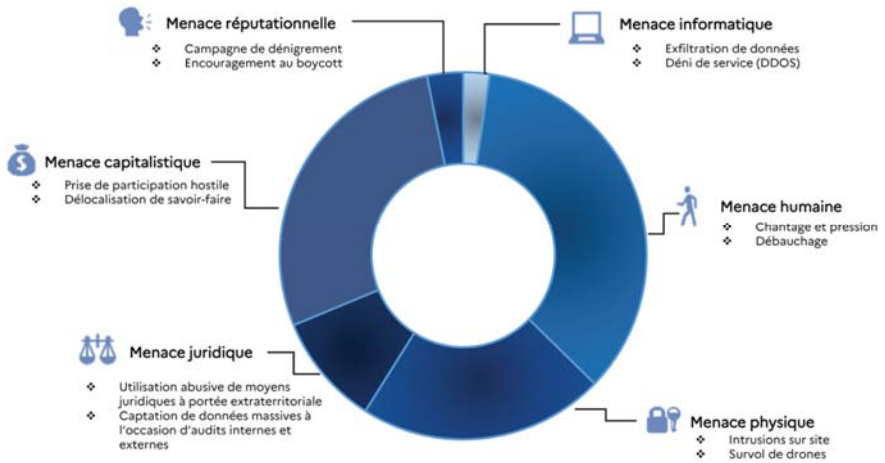
Or, comme le dit l'adage : **la force d'une chaîne dépend de son maillon le plus faible**. Les difficultés d'un sous-traitant critique peuvent avoir des conséquences graves sur l'ensemble de la chaîne de valeur d'une entreprise et de ses productions. La paralysie, la disparition ou le rachat d'une seule entreprise peut ainsi entraîner une perte de compétences ou un manque de maîtrise sur des composants essentiels et non substituables susceptibles d'entraîner des blocages ou une perte d'autonomie stratégique.

Par ailleurs, les entreprises de la BITD ne sont pas les seules victimes de la guerre économique. Les **organismes de recherche** – universités, écoles, laboratoires, instituts de recherche, dans le secteur public comme dans le secteur privé – font eux aussi l'objet d'atteintes. Là encore, leur excellence dans de nombreux secteurs d'avenir fait d'eux des objets de convoitise.

C. DES MENACES PROTÉIFORMES

De plus en plus, **nos compétiteurs stratégiques sont prêts à utiliser tous les moyens à leur disposition pour défendre et promouvoir leurs intérêts**, y compris des moyens intrusifs, agressifs et violents. Si les actes d'espionnage stratégique ou économique – qu'ils se matérialisent par des atteintes humaines ou physiques – sont loin d'avoir disparu, ils s'accompagnent de menaces informatiques, capitalistiques, juridiques ou encore réputationnelles. Ces menaces sont d'autant plus dangereuses qu'elles peuvent se combiner entre elles.

LES PRINCIPALES MENACES PESANT SUR LA BITD



Source : DRSD, « Panorama des ingérences contre la sphère de défense », Lettre d'information économique, n° 13, juin 2023.

● Les **atteintes humaines**, basées sur l'homme et ses vulnérabilités, représentent **plus d'un tiers des menaces**, et leur nombre est en hausse depuis 2020 [(1)]. Elles demeurent pour nos compétiteurs stratégiques l'**un des moyens les plus efficaces** d'obtenir des informations sur une entreprise, une technologie ou un savoir-faire. Elles peuvent se produire sous des formes très diverses : indiscrétions de salariés détenant un savoir spécifique, actes d'espionnage de la part de visiteurs extérieurs, chantages, démarchages de collaborateurs au mépris des clauses de confidentialité ou de non-concurrence, démarchage d'anciens salariés à la retraite, recrutement d'anciens hauts gradés à la retraite susceptibles de servir de caution à des entreprises peu recommandables, etc. Certaines atteintes peuvent aussi prendre des formes plus insidieuses, cachées derrière de fausses relations professionnelles ou privées (approche par un consultant ou par un baby-sitter, organisation d'un faux entretien d'embauche). Les déplacements professionnels et les salons du secteur de l'armement, notamment, sont des moments pouvant susciter des vulnérabilités particulières.

L'exemple du salon du Bourget

Les salons de l'armement sont, chaque année, l'occasion pour certains États et concurrents étrangers de mener des actions d'approche à des fins d'espionnage ou de déstabilisation. L'édition 2025 du salon de l'aéronautique et de l'espace du Bourget n'y a pas fait exception.

Les modes d'actions de nos compétiteurs stratégiques se renouvellent en permanence : vol d'ordinateur, détournement d'un réseau wifi, distribution de clés USB publicitaires contenant des logiciels malveillants, espion se faisant passer pour un membre d'une délégation, un acheteur potentiel ou un agent d'entretien…

La direction du renseignement et de la sécurité de la défense (DRSD) alerte régulièrement sur les dangers de ces salons et organise des sessions d'informations pour sensibiliser les participants français aux mesures de sécurité de base.

● Les **atteintes physiques**, qui se concentrent sur des lieux ou sur du matériel (repérages, intrusions non autorisées, cambriolages, dégradation d'enceinte, sabotages), représentent près d'**une attaque sur cinq**. Le nombre d'atteintes enregistrées a presque doublé en 2024 par rapport aux années antérieures, et leur **niveau élevé** semble se confirmer en 2025.

Parmi les exemples emblématiques, plusieurs cas de coupure de câbles ont été enregistrés, notamment sur des navires en construction, ainsi que des incendies volontaires sur des installations d'importance vitale pour certaines entreprises. La DRSD relève aussi de plus en plus fréquemment des survols de sites sensibles par des drones, lesquels sont d'ailleurs difficiles à détecter et à caractériser, peu de télépilotes étant appréhendés. Certaines atteintes peuvent prendre des formes très élaborées ; par exemple, une entreprise a identifié une faille de sécurité liée à

(1) DRSD, « Panorama des ingérences contre la sphère de défense », Lettre d'information économique, n° 13, juin 2023.

l'utilisation dans ses locaux de distributeurs automatiques dotés de terminaux de paiement produits par un groupe étranger [1].

● Outre les menaces traditionnelles, la BITD est aussi la cible d'**attaques informatiques**. Si ces dernières représentent, selon les années, 10 % à 15 % des cas recensés, leur nombre réel est probablement beaucoup plus élevé. Compte tenu du volume de cyberattaques, toutes ne sont pas signalées. La plupart des entreprises en expérimentent chaque jour, les grands groupes parfois des dizaines voire des centaines tous les jours. Certaines sont d'ailleurs bloquées par les systèmes de sécurité mis en place, sans qu'il soit besoin de les faire remonter.

Il ne fait aucun doute que la **menace informatique continue d'augmenter**, portée par les tensions géopolitiques, notamment par la guerre en Ukraine. En 2024, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a traité 4 386 « événements de sécurité », soit une augmentation de 15 % par rapport à 2023, liée notamment au contexte des jeux olympiques et paralympiques. L'agence note aussi « *une augmentation significative du ciblage d'entités travaillant dans des domaines stratégiques – groupes de réflexion, instituts de recherche et base industrielle et technologique de défense – ou qui assurent la transmission de données sensibles, comme les entreprises de télécommunications et de fourniture de services numériques* » [2].

La **numérisation de l'économie**, qui augmente la surface des attaques, induit ainsi de **nouvelles vulnérabilités**. Elles peuvent naturellement être liées à l'utilisation de services de messagerie ou de visioconférence non sécurisés issus de pays compétiteurs. L'accès illégal à un système d'information peut aussi donner lieu à l'utilisation de logiciels espions et à des exfiltrations de données non maîtrisées, soit à des fins pécuniaires, notamment via l'utilisation de rançongiciels, soit à des fins d'espionnage stratégique, économique ou technologique. Les attaques par déni de service distribué [3] visant à saturer un système d'information, bien qu'elles puissent être déjouées, ont connu une recrudescence qui tend à se résorber.

Comme les atteintes humaines et physiques, les cyberattaques peuvent se révéler particulièrement pénalisantes pour l'entreprise qui subit un vol de savoir-faire, d'une liste de clients ou d'une liste de fournisseurs. Dans les cas les plus critiques, **elles peuvent paralyser l'activité** de l'entreprise, mettre à l'arrêt une ligne de production ou entraver le développement d'un programme en cours. Le rapporteur spécial a notamment eu connaissance d'une PME dont les systèmes d'information ont été bloqués pendant un mois, ce qui est très long à l'échelle d'une petite structure. Certaines études montrent aussi que 50 % des PME victimes d'une cyberattaque réussie disparaissent dans les dix-huit mois qui suivent [4].

---

(1) DGSI, « Flash ingérence économique », n° 100, février 2024.

(2) ANSSI, « Panorama de la cybermenace 2023 », février 2024.

(3) Une attaque par déni de service distribué (DDOS) vise à saturer un système d'information en le soumettant à un très grand nombre de demandes de façon coordonnée.

(4) Statistique rapportée par M. Jean-Noël Barrot, ministre délégué chargé de l'Europe, lors de l'annonce d'un « bouclier cyber » pour les PME et ETI en novembre 2022.

● Les entités de la BITD sont aussi soumises à des **atteintes capitalistiques**. Elles représentent, selon les années, 15 % à 30 % des menaces enregistrées. Certains de nos compétiteurs stratégiques n'hésitent plus à exploiter la fragilité financière de nos entreprises et les faiblesses de l'écosystème financier européen pour cibler nos entreprises stratégiques ainsi que nos technologies critiques.

Les entreprises de l'industrie de défense sont ainsi sous la menace d'une **prise de participation** ou d'une **prise de contrôle** par une entité étrangère, avec le risque de devoir se soumettre à des orientations stratégiques différentes ou de voir leur échapper une partie de leur activité, de leurs savoir-faire ou de leurs travaux de recherche. Ces investissements orchestrés indirectement par l'intermédiaire d'entreprises concurrentes ou directement par des États étrangers peuvent non seulement entraîner la **délocalisation** d'activités de production et des **transferts de technologies**, mais aussi déstabiliser des chaînes d'approvisionnement critiques, créer des dépendances fortes pour l'industrie et de défense et *in fine* aboutir à des **pertes de souveraineté**.

Les atteintes capitalistiques représentent un danger d'autant plus grand que les PME de la BITD font face à des **difficultés d'accès aux financements privés** *(voir le IV du présent rapport)*.

● La BITD est également confrontée à des **menaces de nature juridique**. Le droit est de plus en plus instrumentalisé par certains États pour protéger leurs entreprises et favoriser leurs intérêts économiques. Cette **instrumentalisation du droit** (***lawfare***) peut consister en une utilisation abusive de moyens juridiques à portée extraterritoriale à l'encontre d'entreprises concurrentes. La réalisation de contrôles administratifs ou d'audits voire l'engagement de poursuites judiciaires, y compris pénales, peuvent permettre à des compétiteurs de mettre des entreprises en difficulté pour capter des données stratégiques ou entraver leur développement. En outre, le recours à des prestataires de service soumis à un droit étranger (banques, assurances, experts-comptables, courtiers, avocats, consultants) peut induire de fortes vulnérabilités, avec un risque de fuite de données, en particulier lorsque ces dernières sont stockées à l'étranger.

Les atteintes juridiques passent également par l'utilisation ou le détournement de la **norme internationale**. Dans les organisations internationales se joue ainsi une véritable bataille de la norme visant, pour chaque État, à imposer une réglementation favorable à ses intérêts. À cet égard, le rapporteur spécial a déjà eu l'occasion de souligner combien certains textes portés au niveau européen s'étaient révélés contraires aux intérêts de la défense européenne. De la même manière, une bataille d'influence a lieu au sein des groupes de travail de l'OTAN chargés de définir les caractéristiques techniques des équipements militaires utilisés au sein de l'alliance.

La **menace** juridique peut consister en l'**exploitation de vulnérabilités juridiques** résultant de notre droit interne ou de nos engagements européens. Il en va ainsi de la réglementation relative aux actions de groupe, qui peut permettre de

noyer une petite entreprise sous des milliers de plaintes pour la contraindre à la faillite ou à un rachat forcé en toute légalité.

● Les entités de la BITD sont également confrontées de façon croissante à des **menaces informationnelles et réputationnelles** derrière lesquelles se cachent des opérations d'ingérence étrangère visant à les déstabiliser. Ces atteintes peuvent prendre des formes diverses : campagne d'appel au boycott, dénigrement de la performance d'un produit, désinformation sur des éléments de conformité aux normes environnementales ou sanitaires, exploitation de problématiques sociales, révélation publique d'informations confidentielles sur des difficultés financières ou juridiques, attaques contre le cours de bourse d'une entreprise sur laquelle on parie à la baisse…

Relayées par voie de presse mais aussi sur internet et sur les réseaux sociaux, ces campagnes de désinformation, de propagande ou de subversion peuvent être organisées à distance sans nécessiter la moindre présence physique. Elles sont susceptibles de mettre à mal la réputation positive acquise par une entreprise, d'entacher durablement sa notoriété et de détériorer la relation de confiance qu'elle entretenait avec ses clients et fournisseurs.

Ces atteintes peuvent se révéler difficiles à contrer, notamment lorsqu'elles visent la France dans son ensemble ou qu'elles sont organisées par des organisations non gouvernementales aux financements opaques qui, bien que soutenues directement ou indirectement par des États ou des concurrents étrangers, mettent en avant des raisons éthiques, sociales ou environnementales. Ainsi, certaines entreprises françaises sont parfois faussement accusées de livrer des armes dans des pays instables, alors même que la France est exemplaire dans la façon dont elle gère la production et l'exportation de matériels *(voir le 3 du C du IV du présent rapport)*.

Les attaques informationnelles surviennent aussi régulièrement à l'encontre d'entreprises sur le point de se positionner sur ou de remporter un marché à l'export. Il ne fait alors guère de doute qu'elles sont organisées directement ou indirectement par des entreprises étrangères concurrentes, parfois avec le soutien de leur État.

● Depuis la crise du covid-19, et encore plus depuis le début de l'agression de l'Ukraine par la Russie, les entreprises de la BITD doivent également traiter des vulnérabilités liées à leur **dépendance à des matériaux ou des composants stratégiques**. Ainsi l'Europe dépend à plus de 90 % d'approvisionnements extérieurs pour certaines matières premières considérées comme critiques [(1)]. C'est le cas pour la plupart des **matières premières** utilisées dans la fabrication d'équipements militaires, par exemple le titane, l'acier, l'aluminium, les terres rares, le cobalt, le tungstène ou le nickel. C'est également le cas de certaines **pièces détachées** essentielles dans la production de matériels de guerre, notamment les composants électroniques. Toute rupture d'approvisionnement, même temporaire, peut conduire à un arrêt de production et entraîner des difficultés en cascade.

(1) Raphaël Danino-Perraud, « La criticité des matières premières stratégiques pour l'industrie de défense », IRSEM, étude n° 72, novembre 2019.

D. LES MENACES VIENNENT DE TOUS NOS COMPÉTITEURS STRATÉGIQUES

Dans un contexte de remontée des tensions géopolitiques et d'exacerbation des rivalités entre puissances, les atteintes à la sécurité économique, notamment en ce qui concerne la BITD, se renforcent. Leur origine n'est pas toujours facile à identifier, du fait de stratégies souvent opaques et hybrides, avec des acteurs étatiques n'agissant pas toujours de manière directe et transparente.

Les principales menaces proviennent, logiquement, **de compétiteurs qui ne sont pas nos alliés sur un plan militaire ou géostratégique**. Ainsi que l'ont établi, en 2023, la délégation parlementaire au renseignement (1) et la commission d'enquête sur les ingérences étrangères (2), la Russie comme la Chine constituent les deux menaces principales.

Avec la guerre en Ukraine, la **menace russe a évolué mais demeure élevée**. Les actions d'infiltration russes ont diminué, notamment du fait des expulsions et interdictions d'entrée sur le territoire prononcées à l'encontre d'un certain nombre d'officiers de renseignement qui opéraient sous couverture diplomatique. Toutefois, les Russes continuent d'œuvrer contre la BITD, à la fois *via* des menaces humaines ou physiques (vols d'ordinateur, actes de sabotage) ou à distance (piratage d'emails, achats clandestins de matériels sous embargo). La Russie demeure très active en matière de cyberattaques, à l'instar du groupe de hackers « APT28 », lié au GRU, le service de renseignement militaire du Kremlin. Un certain nombre d'entreprises de la BITD mobilisées dans le cadre du soutien à l'Ukraine ont ainsi été la cible d'attaques. En outre, la Russie est la principale source de désinformation et d'attaques réputationnelles. Malgré la fermeture des médias russes en Europe (*Russia Today* et *Sputnik*), elle déploie de nombreux moyens sur les réseaux sociaux pour alimenter, en France, un climat de désordre et de division et, à l'étranger, un discours anti-français.

La menace chinoise tend aussi à se durcir, avec une stratégie assumée de pillage technologique destinée à combler des retards à moindre coût. Outre les moyens considérables alloués aux services de renseignement – le *Guoanbu*, l'équivalent de la DGSE chinoise, est doté d'environ 250 000 agents –, elle s'appuie aussi sur une forte diaspora (600 000 personnes en France) et sur une loi de 2017 qui, en imposant à tous les citoyens d'assister le renseignement national, fait de tout ressortissant chinois un espion potentiel, susceptible de collecter des informations sensibles ou de relayer de fausses informations. Une grande partie des menaces humaines identifiées proviennent ainsi de la Chine. Les organismes de recherche sont tout particulièrement les cibles de tentatives d'espionnage. La Chine est également très active en termes de menace cyber et de menace informationnelle. Ces dernières semaines, la Chine a notamment été à la manœuvre d'une campagne de dénigrement du Rafale menée sur les réseaux sociaux. Le rapporteur relève

---

(1) Délégation parlementaire au renseignement, rapport public de M. Sacha Houlié, président, et M. Christian Cambon, vice-président, relatif à l'activité pour l'année 2022-2030, enregistré à la présidence le 29 juin 2023.

(2) Assemblée nationale, rapport n° 1311 (XVIe législature) de Mme Constance Le Grip, fait au nom de la commission d'enquête relative aux ingérences politiques, économiques et financières de puissances étrangères, enregistré à la présidence de l'Assemblée nationale le 1er juin 2023.

également la campagne de dénigrement de l'industrie française du luxe organisée par la Chine, en avril 2025, qui, si elle ne concerne pas la BITD, n'en concerne pas moins l'un de nos fleurons stratégiques, par son importante contribution à notre balance commerciale. S'agissant des menaces capitalistiques, les investissements chinois sont souvent habilement calibrés pour rester sous les seuils au delà desquels des contrôles ou des mesures d'entrave peuvent intervenir.

De la même manière, tous les États dotés d'une industrie de défense concurrente de la nôtre (Iran, Turquie, Israël, Corée…) constituent une menace potentielle. À cet égard, il convient de souligner qu'**en matière de guerre économique, les menaces peuvent venir de tous les pays**. Les scandales médiatiques liés à l'utilisation de systèmes de surveillance électronique pour espionner des dirigeants européens ou encore l'annulation par l'Australie du contrat de vente de sous-marins qu'elle avait signé avec Naval Group au profit d'un partenariat américano-britannique ne sont que la face émergée de l'*iceberg*.

Les **États-Unis**, cela n'a rien d'une révélation, mènent une véritable guerre économique contre l'Europe, visible depuis l'accession au pouvoir de M. Donald Trump, mais en réalité plus ancienne. Le ***lawfare*** est devenue une véritable arme pour favoriser les entreprises américaines au détriment de leurs concurrents. La réglementation « Itar » [(1)], tout comme la réglementation américaine en matière de lutte contre la corruption et le blanchiment de capitaux ou de protection cyber sont ainsi utilisées par l'administration américaine pour contrôler des entreprises étrangères, y compris au travers de visites sur le territoire français, avec un risque fort que les enquêtes débordent au delà de la simple question du respect des règles. De même, le *Patriot Act* et le *Cloud Act* autorisent le FBI à obliger des entreprises, notamment des fournisseurs d'un accès à internet ou d'un service de stockage de données de lui communiquer toutes les données qu'ils ont pu collecter, y compris sur des entreprises situées en dehors du territoire américain. Auditionnés par le Sénat [(2)], les représentants de Microsoft ont ainsi indiqué que, bien qu'un tel cas ne s'était encore jamais présenté, la possibilité que l'entreprise soit juridiquement tenue de communiquer aux autorités américaines des données confidentielles de leurs clients ne pouvait être exclue.

En parallèle, les agences de **renseignement** se sont mises au service des grands groupes américains, y compris en espionnant les entreprises européennes, notamment sur les marchés export. Les États-Unis n'hésitent pas non plus à faire usage des liquidités financières abondantes dont ils disposent pour **racheter des entreprises stratégiques et des technologies sensibles** lorsqu'elles ne trouvent pas

---

*(1) L'*international traffic in arms regulations *(ITAR) est une réglementation américaine qui contrôle la fabrication, la vente et la distribution d'objets et de services liés à la défense et à l'espace. Elle prévoit que l'accès aux matériaux physiques ou aux données techniques liés à la défense et aux technologies militaires est réservé aux citoyens des États-Unis. Les États-Unis s'en servent comme d'un outil protectionniste pour protéger leurs champions nationaux au détriment des autres industriels y compris européens.*

(2) Sénat, audition de M. Anton Carniaux, directeur des affaires publiques et juridiques de Microsoft France, et de M. Pierre Lagarde, directeur technique du secteur public de Microsoft France, par la commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française, 10 juin 2025.

de fonds pour se développer. Les personnes auditionnées par le rapporteur lui ont confirmé que les tentatives de prédation capitalistique sont régulièrement combinées à des attaques juridiques, selon un schéma d'une efficacité redoutable, qui vise à noyer une entreprise concurrente sous des procédures lourdes et très coûteuses jusqu'à ce qu'elle cède à un rachat. L'agressivité des prétentions américaines s'étend d'ailleurs bien au delà du secteur de la défense. Ainsi, dans le domaine de l'énergie, la guerre en Ukraine tend à remplacer la dépendance de l'Europe au gaz russe par une dépendance au gaz naturel liquéfié américain dont le coût est encore plus élevé.

D'autres de nos concurrents cherchent également à **imposer des rapports de forces économiques plus favorables à leurs entreprises**. Le Comité d'intelligence stratégique pour la souveraineté [(1)] et l'École de guerre économique [(2)] ont de longue date mis en évidence les opérations d'influence financées par des fondations allemandes contre la filière nucléaire française, tant pour des raisons idéologiques qu'économiques. D'autres exemples existent dans le domaine de la pêche ou de la filière de la viande [(3)]. S'agissant plus spécifiquement des questions de défense, on peut noter que certains sous-traitants du secteur aéronautique ont été gênés par les décisions de l'Allemagne de bloquer la vente d'avions Eurofighter à l'Arabie Saoudite et à la Turquie.

Il ne s'agit pas ici de porter grief à nos compétiteurs stratégiques, qui ne font que défendre leurs intérêts. Comme le dit une citation attribuée au général de Gaulle, récemment reprise par Geoffroy Roux de Bézieux : « *les pays n'ont pas d'amis, ils n'ont que des intérêts* ». C'est donc plutôt à une prise de conscience qu'il faut appeler, afin de **cesser d'être naïfs** et de **mieux défendre nos propres intérêts**.

(1) Comité d'intelligence stratégique pour la souveraineté, « Rapport d'investigation : Comment l'Allemagne finance l'affaiblissement du secteur nucléaire français », avril 2023.

(2) École de guerre économique, « Rapport d'alerte : Ingérence des fondations politiques allemandes et sabotage de la filière nucléaire française », juin 2023.

(3) Observatoire de l'intelligence économique français, « L'arme écologique-activiste comme facteur de déstabilisation d'entreprises françaises », 6 septembre 2021.

II. UN RENFORCEMENT DES MOYENS ET DES OUTILS MOBILISÉS PAR L'ÉTAT POUR PROTÉGER ET SOUTENIR LES ACTIFS STRATÉGIQUES

En 1994, le **rapport Martre** énumérait les retards accumulés par la France en matière d'intelligence économique, non seulement par rapport aux États-Unis, champions de l'accroissement de puissance par l'économie, mais aussi par rapport à d'autres pays tels que le Japon, l'Allemagne ou la Suède. Il l'expliquait par un cloisonnement des administrations et des entreprises ainsi que par un manque de circulation de l'information, notamment au niveau des PME.

En 2003, le **rapport Carayon** confirmait que « *l'intelligence économique n'occupe pas la place qu'elle mérite, c'est-à-dire celle qu'elle occupe en réalité dans les grands pays occidentaux* », le rapport Martre n'ayant été suivi que « *d'efforts disparates et désordonnés* », sans véritable « *impulsion politique* ». Il regrettait l'absence de doctrine permettant d'identifier les intérêts économiques et scientifiques majeurs du pays devant être protégés. Il déplorait également que les administrations publiques ne soient pas conduites à collaborer entre elles et qu'elles fonctionnent de façon cloisonnée voire concurrente. Il soulignait enfin l'absence de convergence entre le secteur public et le secteur privé et leur méfiance réciproque.

Si certains de ces constats restent en partie d'actualité, il convient de reconnaître que **les choses ont évolué dans le bon sens** au fil des années. La France a ainsi mis en place un système défensif qui identifie mieux les actifs stratégiques et renforce la surveillance. Ce système ne fait pas disparaître toutes les vulnérabilités, mais il permet de mieux appréhender les risques qui pèsent sur nos entreprises, notamment celles de la BITD, de détecter les menaces le plus tôt possible et d'agir en conséquence pour les désamorcer, les neutraliser ou les entraver.

Si la BITD est traditionnellement mieux protégée que les autres secteurs, la **crise du covid** et la **guerre en Ukraine** ont **accéléré la prise de conscience** de l'intérêt vital de renforcer la souveraineté économique de la France. Dans la période récente, les services de l'État ont ainsi renforcé les moyens qu'ils consacrent à l'intelligence économique et se sont réorganisés afin de mieux assurer leurs missions de sécurité et de promotion économiques.

A. LA CONSOLIDATION DES MOYENS BUDGÉTAIRES ET HUMAINS ALLOUÉS À LA POLITIQUE D'INTELLIGENCE ÉCONOMIQUE

La politique de sécurité économique et de soutien aux entreprises stratégiques met en jeu des acteurs du secteur de la défense, à commencer par la direction générale de l'armement (DGA) et les services de renseignement financés par la mission *Défense*, la direction du renseignement et de la sécurité de la défense (DRSD) ainsi que la direction générale de la sécurité extérieure (DGSE). Elle implique aussi d'autres acteurs de la sphère étatique, notamment le secrétariat général de la défense et de la sécurité nationale (SGDSN), chargé de piloter l'effort de défense et de sécurité nationale au niveau interministériel, le service de l'information stratégique et de la sécurité économiques (SISSÉ), chargé de piloter

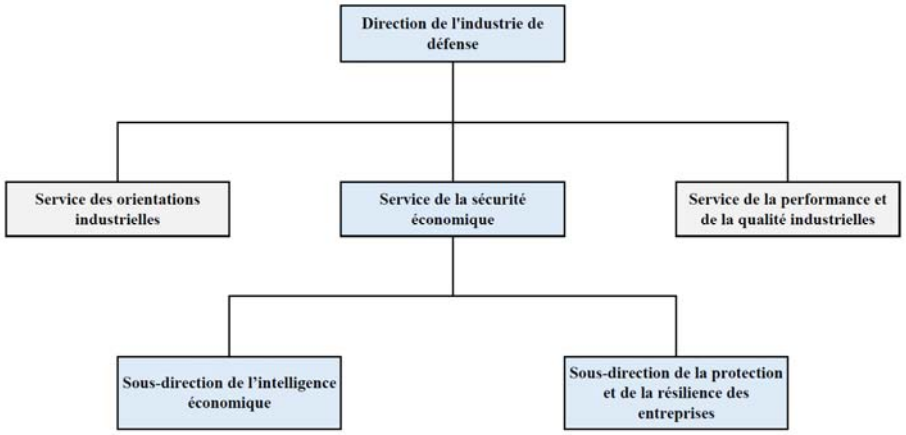
la politique de sécurité économique, et l'agence nationale de la sécurité des systèmes d'information (ANSSI), qui est l'autorité nationale en matière de cybersécurité et de cyberdéfense.

Les moyens budgétaires et humains alloués par l'État à la protection des actifs stratégiques se sont renforcés, notamment depuis le milieu des années 2010, en particulier au sein de la DGA, du SISSÉ et des services de renseignement.

1. Une concentration des moyens renforcée au sein de la direction générale de l'armement

La question de la guerre économique n'est pas nouvelle au sein du ministère des armées. La **DGA**, dans le cadre de sa mission d'organisation de l'autonomie industrielle de l'équipement des forces, **exerce depuis longtemps une compétence en matière d'intelligence économique et de protection des entreprises de la BITD**. Elle dispose d'une connaissance fine du tissu industriel militaire, renforcée à l'occasion de la crise du covid avec la mise en place d'une *task force* pour surveiller, accompagner et soutenir les entreprises en difficulté, et entretenue par des rencontres de terrain régulières – la DGA effectue près de **900 visites par an**.

Outre ses outils budgétaires, avec lesquels elle s'emploie à octroyer aux entreprises de la BITD les plus critiques un niveau de trésorerie adapté à leur plan de charge (paiement accéléré de factures, anticipation de commandes militaires, facilitation de l'obtention d'une licence ou d'un partenariat à l'export), l'action de la DGA en matière de protection de la BITD s'appuie sur la **direction de l'industrie de défense (DID)**, qui a pris la suite du service des affaires industrielles et de l'intelligence économique, et dont la création a renforcé la **concentration des moyens consacrés par le ministère des armées à la sécurité et à l'intelligence économiques** ainsi qu'à ses relais régionaux.



La direction de l'industrie de défense regroupe plus de 600 emplois, et a en outre bénéficié d'une trentaine de créations de postes depuis 2023. Ces moyens renforcés bénéficient en particulier au service de la sécurité économique – lui-même composé d'une sous-direction de l'intelligence économique et d'une sous-direction de la protection et de la résilience des entreprises – et permettent à la DGA de renforcer son action de protection des entreprises de la BITD.

a. La **sous-direction de la protection et de la résilience des entreprises** est chargée de superviser la mise en œuvre de la politique du ministère des armées en faveur des entreprises et de déployer les dispositifs de soutien nécessaires au développement économique des PME.

Dans cette perspective, elle met en œuvre, en lien avec la direction générale du trésor, le **contrôle des investissements étrangers en France**, lorsqu'il concerne une entreprise du secteur de la défense *(voir le 1 du B du présent II)*.

La sous-direction de la protection et de la résilience des entreprises instruit aussi, en lien avec l'Institut national de la propriété industrielle (INPI), les **dépôts de brevet**, **de marque** ou de tout élément relatif à la **propriété intellectuelle**, au regard des intérêts de la défense nationale et de la préservation des droits des inventeurs. Si une information comprend un intérêt essentiel pour la sécurité nationale, la DGA est ainsi en capacité de prendre des mesures d'entrave temporaires ou pérennes, afin d'éviter la diffusion d'informations ayant vocation à rester confidentielles. Cette expertise permet aussi à la sous-direction de sensibiliser les PME aux questions de propriété intellectuelle et de renforcer leur prudence lorsqu'elles communiquent des informations en la matière avec de potentiels investisseurs ou partenaires, notamment étrangers.

Depuis la création de la direction de l'industrie de défense, la sous-direction de la protection et de la résilience des entreprises exerce une compétence nouvelle : elle pilote les **projets d'amélioration du niveau de sécurité numérique et de résilience des entreprises** contribuant aux intérêts essentiels de défense. Cette évolution était nécessaire, dans un contexte de montée des menaces informatiques et cyber. C'est dans ce cadre que sont progressivement mis en place différents dispositifs visant à élever le niveau de cybersécurité des entreprises de la BITD *(voir le 3 du B du présent II)*.

Enfin, dans le prolongement des travaux sur l'économie de guerre réalisés par la DGA, les états-majors et les industriels, qui ont permis d'identifier un certain nombre de risques de rupture d'approvisionnement et de goulets d'étranglement, la direction de l'industrie de défense, en partenariat avec Bpifrance, a mis en place un **programme « Accélérateur défense »** visant à soutenir les PME appelées à faire évoluer leurs moyens de production pour se mettre en capacité de produire de plus gros volumes, plus vite, à coûts maitrisés et dans la durée. Ce programme doit notamment permettre aux entreprises qui ne disposent pas d'un bureau des méthodes de bénéficier de conseils collectifs et individualisés pour optimiser leurs processus de production, pris en charge à 50 % par l'État.

b. La **sous-direction de l'intelligence économique** élabore et coordonne la mise en œuvre de la stratégie de veille d'informations du ministère de la défense. Elle regroupe environ 10 % des effectifs de la direction de l'industrie de défense.

La sous-direction organise la **remontée des informations de terrain**, à partir des échanges qu'elle peut avoir avec les PME avec qui elle est en permanence en contact au travers de ses réseaux déconcentrés. Elle s'appuie aussi sur les réseaux de renseignement économique des grands groupes et sur les informations relayées par les services de renseignement, en particulier la DRSD. Elle joue ainsi un rôle important dans l'orientation des capteurs du renseignement, notamment *via* un plan annuel d'orientation du renseignement, qui est chaque année pris en compte dans l'élaboration du plan de charge des services de renseignement.

Ce travail de veille économique s'appuie aussi sur le **renseignement en sources ouvertes** (*open source intelligence* ou OSINT). À cet égard, la sous-direction de l'intelligence économique dispose de moyens renforcés, avec la mise en place d'un campus OSINT chargé de repérer les solutions de renseignement en source ouverte pouvant être utilisées par le ministère et de former les personnels à leur utilisation. Ce campus doit permettre à la DGA de développer des compétences d'analyse complémentaires de celles des industriels, afin de fédérer un véritable écosystème des acteurs de l'OSINT et de la veille stratégique.

La sous-direction de l'intelligence économique a également autorité sur **DGA Intelligence technique et économique** : cet organisme extérieur est chargé de capter et de produire de l'information stratégique au profit des PME qui ne disposent pas des compétences nécessaires en interne, qui n'ont pas accès aux sources d'information adéquates ou qui souhaitent exercer une veille stratégique tout en se concentrant sur leur cœur de métier.

L'augmentation des moyens alloués à la veille stratégique doit permettre à la fois de mieux protéger et mieux informer les entreprises de la BITD, mais aussi de détecter le plus en amont possible d'éventuels projets de réglementation en cours à l'étranger ou aux niveaux international et européen afin de pouvoir désamorcer autant que possible les évolutions contraires à nos intérêts économiques.

La réorganisation de la DGA a non seulement permis un renforcement des moyens consacrés à la protection et au soutien des entreprises de la BITD, mais aussi un décloisonnement de services autrefois séparés et agissant désormais sous l'autorité d'une hiérarchie unique. Cela facilite les échanges d'informations et la mise en œuvre de nouvelles solutions innovantes.

2. La montée en puissance du service de l'information stratégique et de la sécurité économiques

Si la DGA constitue un point fort de notre système d'intelligence économique, avec une expérience des enjeux de souveraineté plus ancrée, la protection des actifs stratégiques de la France en dehors de la seule sphère défense a été renforcée avec la création, en 2016 [(1)], du **service de l'information stratégique et de la sécurité économiques** (SISSÉ). Ce service, placé sous l'autorité du directeur général des entreprises (DGE), à qui est également attribuée la qualité de commissaire à l'information stratégique et à la sécurité économique, est **chargé d'élaborer, de piloter et de coordonner, au niveau interministériel, la politique de sécurité économique de l'État et la protection des intérêts économiques de la France**.

● Le SISSÉ est le **résultat d'un long processus de mise en œuvre d'une politique d'intelligence économique** engagé à la suite de la publication du rapport Martre. Le Haut responsable à l'intelligence économique créé en 2003, alors rattaché au SGDSN, avait laissé sa place, en 2009, à une délégation interministérielle à l'intelligence économique, rattachée au Premier ministre, et à un service de coordination à l'intelligence économique, rattaché au ministère de l'économie. Ces structures, dispersées et insuffisamment structurées, ont été fusionnées au sein du SISSÉ, ce qui a contribué à clarifier l'organisation de l'État.

En 2018, peu après la création du SISSÉ, la délégation parlementaire au renseignement s'était interrogée sur la cohérence du dispositif mis en place et sur la capacité du SISSÉ à coordonner les différents acteurs et ministères concernés par la mise en œuvre de la politique de sécurité économique [(2)]. Six ans plus tard, le rapporteur spécial constate que **le rôle joué par le SISSÉ a été salué par l'ensemble des personnes qu'il a auditionnées**. Le SISSÉ a non seulement trouvé sa place dans l'environnement interministériel mais il a aussi pris une ampleur à la mesure des enjeux de sécurité économique. Son action s'est révélée complémentaire de celle d'autres directions du ministère de l'économie, concentrées sur la seule politique d'attractivité de la France, et cette action a permis d'acclimater ce ministère à des inclinaisons qui ne sont traditionnellement pas les siennes.

En 2023, un rapport sénatorial proposait la création d'un secrétariat général à l'intelligence économique, soit une structure rattachée directement au Premier ministre, chargée de concevoir et de piloter une stratégie nationale d'intelligence économique [(3)]. L'on comprend le souci de rattacher à Matignon une mission naturellement transversale et interministérielle. Toutefois, les changements récurrents de nom et de tutelle des structures administratives chargées de coordonner la politique

---

(1) Décret n° 2016-66 du 29 janvier 2016 instituant un commissaire à l'information stratégique et à la sécurité économiques et portant création d'un service à compétence nationale dénommé « service de l'information stratégique et de la sécurité économiques ».

(2) Délégation parlementaire au renseignement, rapport de M. Philippe Bas, sénateur, relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2017, enregistré à la présidence le 12 avril 2018.

(3) Sénat, rapport n'information n° 872 (2022-2023) de Mme Marie-Noëlle Lienemann et M. Jean-Baptiste Lemoyne, fait au nom de la commission des affaires économiques, sur l'intelligence économique, enregistré à la présidence le 12 juillet 2023.

d'intelligence économique ont nui à la lisibilité de cette politique sans nécessairement avoir d'effets concrets. Un nouveau changement relancerait des querelles de service et paralyserait l'action de l'État pendant plusieurs mois. Sur ce point, **le rapporteur spécial estime qu'une certaine stabilité est nécessaire et qu'il convient de continuer à renforcer nos actions de protection et de promotion des actifs stratégiques en s'appuyant sur les équilibres existants**.

● Le SISSÉ **a progressivement vu ses moyens augmenter**, de 24 ETP en 2016 à 32 ETP en 2025. S'y ajoute un réseau territorial composé de 24 délégués à l'information stratégique et à la sécurité économiques, placés auprès des préfets de région et des directions régionales de l'économie, de l'emploi, du travail et des solidarités (Dreets). Ces délégués, qui n'existaient pas avant la création du SISSÉ, ont pour mission de conseiller les entreprises face aux risques qu'elles rencontrent en matière de guerre économique. Ils effectuent aussi une veille stratégique.

Le SISSÉ est véritablement monté en puissance depuis 2020, avec la crise du covid puis la guerre en Ukraine, qui ont accéléré la prise de conscience de la nécessité de renforcer la souveraineté économique de la France. Aux fins d'identifier les actifs stratégiques matériels et immatériels devant être protégés, **un répertoire de sécurité économique** a été mis en place, sous l'impulsion du SISSÉ, contenant trois listes : une liste d'**entreprises stratégiques**, une liste de **technologies critiques** ainsi qu'une liste de **laboratoires et organismes de recherche**. Y sont inclus l'ensemble des actifs dont la criticité impose qu'ils soient détenus par des Français et des actifs stratégiques pour notre potentiel d'innovation et de croissance à moyen terme. Tous les actifs identifiés comme étant stratégiques font l'objet d'une surveillance constante, organisée par le SISSÉ, pour détecter les menaces potentielles le plus en amont possible afin de les neutraliser ou les entraver.

La montée en puissance du SISSÉ s'est en outre matérialisée par un décret du 20 mars 2020 [(1)], qui a renforcé ses **missions de coordination**. S'appuyant sur ses délégués en région, le SISSÉ assure ainsi la coordination territoriale d'un réseau opérationnel de surveillance des alertes de sécurité économique. Une fois détectées, les alertes sont traitées par le Comité de liaison en matière de sécurité économique (COLISÉ), présidé par le SGDSN et dont le SISSÉ assure le secrétariat, lequel réunit des représentants des ministères – notamment celui des armées mais aussi ceux de l'économie, de la recherche ou encore de l'agriculture – pour coordonner les actions de sécurité économique.

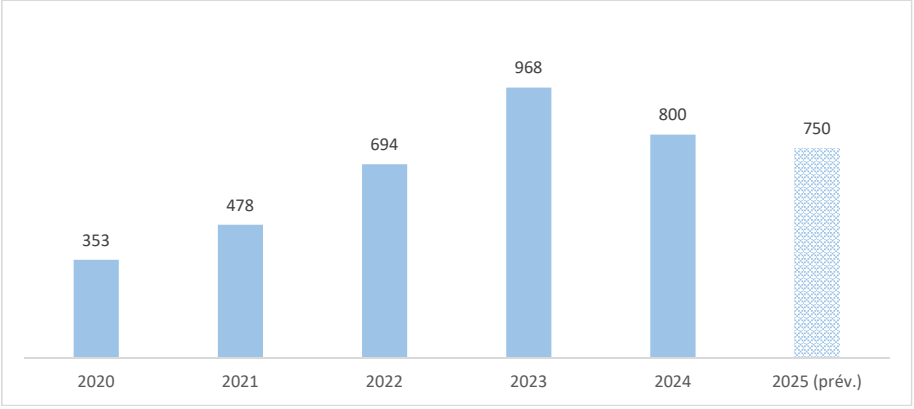
Le SISSÉ est également alimenté par les services de renseignement, et il contribue largement à orienter le travail de ces services en matière de sécurité économique. En lien avec le coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT), il assure la co-présidence du Comité d'orientation pour le renseignement d'intérêt économique (CORIÉ), qui réunit les services de renseignement sur les sujets liés au renseignement économique.

(1) Décret n° 2016-66 du 29 janvier 2016 instituant un commissaire à l'information stratégique et à la sécurité économiques et portant création d'un service à compétence nationale dénommé « service de l'information stratégique et de la sécurité économiques ».

Le SISSÉ est notamment très actif dans la **détection des opérations capitalistiques** susceptibles de menacer l'intégrité des actifs stratégiques nationaux. Il est également impliqué dans les principales procédures mises en œuvre en matière de sécurité économique. En matière de **contrôle des investissements étrangers** en France, il est notamment impliqué dans le suivi des conditions imposées aux investisseurs ayant réalisé une prise de participation dans un secteur stratégique *(voir le 1 du B du présent II)*. Depuis 2022, il est également le guichet unique des entreprises concernées par la loi de blocage de 1968 *(voir le 2 du B du présent II)*.

● **Le nombre d'alertes de sécurité économique reçues par le SISSÉ a triplé entre 2020 et 2023** (1). Après un pic de près de 1 000 affaires traitées en 2023, notamment lié à l'organisation en France des jeux olympiques et paralympiques, il tend toutefois à se stabiliser autour de 750-800 affaires en 2024 et 2025. Plus de 40 % des menaces identifiées sont à finalité capitalistique, et environ autant concernent un risque de captation d'informations sensibles (audit, procédure devant une juridiction étrangère). Les atteintes d'autres types (intrusions dans des locaux, cyber) sont moins volumineuses mais réelles. Les attaques informationnelles demeurent quant à elles encore peu documentées.

ÉVOLUTION DU NOMBRE D'ALERTES TRAITÉES ANNUELLEMENT PAR LE SISSÉ



Source : service de l'information stratégique et de la sécurité économiques.

Ces chiffres traduisent le renforcement des moyens de surveillance avec, d'une part, l'entrée dans le champ des contrôles de nouvelles entreprises, de nouveaux centres de recherche, de nouvelles technologies *(voir le 1 du B du présent II)* et, d'autre part, une meilleure détection des menaces, fondée sur des technologies de traitement de données en masse ainsi que sur des effectifs renforcés.

(1) Les alertes de sécurité économique recensées par le SISSÉ intègrent une partie des atteintes enregistrées contre la BITD ou des organismes de recherche de défense, que la DRSD fait remonter.

3. Des services de renseignement mieux dotés et plus actifs en matière de contre-ingérence économique

Dans leurs missions de protection et de promotion des actifs stratégiques, le SISSÉ comme la DGA, pour ce qui est de la BITD, s'appuient largement sur les **services de renseignement**, qui constituent des **sources d'information essentielles** compte tenu des prérogatives qui leur sont conférées par la loi. Si le renseignement économique avait régressé depuis la fin de la Guerre froide, le rôle joué par les services de renseignement en matière d'intelligence économique, leur coordination avec les directions opérationnelles et les moyens consacrés par ces services aux questions de sécurité économique se sont renforcés depuis le milieu des années 2010.

a. La défense et la promotion des intérêts économiques et industriels

La protection des intérêts économiques et industriels de la France a longtemps été une matière difficile à appréhender publiquement pour les services de renseignement, **traditionnellement centrés sur les questions régaliennes**. Toutefois, deux évolutions du cadre normatif dans lequel évoluent les services de renseignement sont intervenues :

– depuis 2015, les **intérêts économiques, industriels et scientifiques majeurs** de la France figurent parmi les intérêts fondamentaux de la Nation pour lesquels les services de renseignement, dans l'exercice de leurs missions, sont autorisés à recourir à des techniques exorbitantes du droit commun (1) ;

– en outre, depuis 2019, la stratégie nationale du renseignement compte **la défense et la promotion de nos intérêts économiques et industriels** parmi les enjeux prioritaires des services de renseignement. Ces derniers sont appelés à contribuer à la détection des menaces afin de limiter les risques de déstabilisation, d'affaiblissement ou de captation de nos actifs stratégiques dans la compétition internationale, à appuyer les services de l'État chargés de la mise en œuvre des actions de promotion de nos intérêts et à contribuer à la diffusion auprès des acteurs économiques des informations stratégiques utiles à leur développement international.

Ces évolutions ont contribué à faire évoluer les pratiques et à légitimer l'action des services de renseignement en matière de protection et de promotion des intérêts économiques de la France. Les directions opérationnelles, à commencer par le SISSÉ et la DGA, pour ce qui concerne la BITD, sont ainsi davantage alimentées par le renseignement que durant les périodes antérieures.

La DRSD, pour la sphère défense, et la DGSI, pour la sphère civile, mènent, elles aussi, des actions de veille stratégique des entreprises, technologies et organismes de recherche d'importance majeure. Elles bénéficient pour cela du soutien des autres services de la communauté du renseignement, dans leurs domaines de compétences respectifs, notamment la DGSE pour la précision des menaces venant d'acteurs extérieurs, mais aussi la direction nationale du

(1) Article L. 811-3 du code de la sécurité intérieure, dans sa rédaction résultant de l'article 2 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

renseignement et des enquêtes douanières (DNRED) et du service de traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN).

La défense et la promotion de notre économie
Extraits de la stratégie nationale du renseignement de 2019

« Le premier objectif de notre politique de sécurité économique est de détecter et de neutraliser le plus amont possible toute menace sérieuse, potentielle ou avérée, systémique ou ponctuelle, susceptible d'affecter les intérêts économiques, industriels et scientifiques de la Nation, en particulier les actifs stratégiques. Le Renseignement doit ainsi contribuer à la détection de ces menaces afin de limiter les risques de déstabilisation, d'affaiblissement ou de captation de nos actifs stratégiques dans la compétition internationale.

« Le second volet de cette politique est la promotion de nos intérêts économiques. Cela se décline en trois finalités : identifier les actions susceptibles de contribuer à cette promotion ; appuyer les services de l'État chargés de la mise en œuvre de ces actions ; contribuer à la diffusion auprès des acteurs économiques des informations stratégiques utiles à leur développement international. Le Renseignement doit contribuer à l'acquisition des connaissances de nature à répondre à ces trois finalités.

« Dans le même temps, deux questions spécifiques retiennent l'attention des services de Renseignement :

« – la lutte contre les fraudes financières, fiscales, sociales ou à la propriété intellectuelle est un enjeu majeur […] ;

« – l'instrumentalisation des champs normatifs ou contentieux : l'édiction, par des États ou des entités non-étatiques, de normes y compris à portée extraterritoriale, peut s'accompagner d'actions d'influence agressives dans les instances de production des normes. On assiste par ailleurs à un développement des enquêtes d'autorités judiciaires étrangères à l'encontre des entreprises françaises commerçant à l'international sur la base de lois offensives à portée extraterritoriale. Ces procédures contentieuses ont fréquemment pour effet – recherché ou non – de contraindre les entreprises visées à transférer des actifs essentiels à leur prospérité (informations confidentielles relatives aux dirigeants, clients et fournisseurs, informations financières, brevets et savoir-faire technologiques…), ou à se retirer de certains marchés. À ce titre, le Renseignement doit contribuer à identifier, dénoncer, voire entraver les actions malveillantes et les actions d'influence faussant l'environnement juridique et normatif des acteurs économiques. »

La promotion de nos intérêts

« Le Renseignement, outil de défense de nos intérêts et d'acquisition de connaissances dans les domaines stratégiques, est également un outil de promotion de nos intérêts (politiques, économiques, scientifiques, militaires, culturels, etc…).

« Il s'agit ici, non seulement de développer, en appui de notre diplomatie, des actions d'influence en direction des structures d'intérêts pour notre pays, mais de capter et d'analyser les données nécessaires à la réalisation de nos objectifs et à la protection de nos intérêts.

« Cette compétence est prise en compte dans la rédaction de la loi Renseignement de 2015, qui évoque la possibilité pour les services spécialisés de recueillir des renseignements "relatifs à la défense et à la promotion des intérêts fondamentaux", s'agissant notamment "des intérêts économiques, industriels et scientifiques majeurs de la France". »

b. Des moyens renforcés, notamment consacrés à la contre-ingérence économique

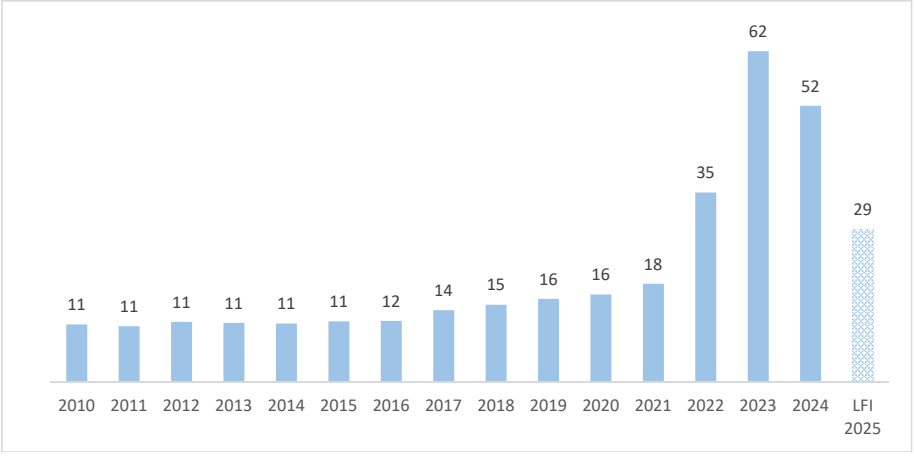
La montée en puissance des services de renseignement en matière d'intelligence économique est également permise par le renforcement de leurs moyens budgétaires et humains. Dans le cadre des lois de programmation militaire pour les périodes 2019-2025 et 2024-2030, la DRSD comme la DGSE – dont les crédits de fonctionnement hors dépenses de personnel sont inscrits sur le programme 144 de la mission *Défense* – bénéficient d'une remontée de leur budget et de leurs effectifs, qui profitent notamment à leurs actions de renseignement et en particulier à leurs missions de contre-ingérence économique.

● Le montant des crédits de paiement de la DRSD est en hausse constante ces dernières années. Il a doublé entre 2018 et 2025, passant de 15 à 29 millions d'euros, avec un objectif de 32 millions d'euros d'ici 2030 inscrit dans l'actuelle loi de programmation militaire (LPM) [(1)]. Hors opérations exceptionnelles, le budget de fonctionnement de la DRSD a lui aussi augmenté de plus de 20 % entre 2018 et 2025. Sur la même période, la direction a bénéficié de **49 créations de postes**, même si, sur les derniers exercices, elle peine à atteindre sa cible en matière de ressources humaines.

Cette hausse du budget doit permettre à la DRSD de faire face à l'évolution des menaces sur la « sphère défense », notamment la BITD. Elle se traduit par des **investissements significatifs** dans le domaine des infrastructures, des systèmes d'information et des équipements.

MONTANT DES CRÉDITS DE PAIEMENT ALLOUÉS À LA DRSD

(en millions d'euros)



Source : commission des finances d'après les annexes budgétaires.

(1) 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.

Depuis 2022, le budget de la direction connaît par ailleurs des niveaux exceptionnellement élevés liés à la construction du nouveau siège de la direction centrale, au Fort de Vanves, qui est en voie d'achèvement et dans lequel les services ont emménagé en 2025. Ce bâtiment doit permettre à la direction de renforcer les standards de protection de ses emprises, de faire face à l'augmentation de ses effectifs et de bénéficier de nouvelles facilités favorisant le travail collaboratif entre les personnels (ateliers techniques, espaces de formation, locaux pour les serveurs). Dans le domaine des systèmes d'information, la DRSD a poursuivi le développement de sa **nouvelle base de données souveraine** qui doit lui permettre de stocker et d'exploiter le renseignement à partir d'une solution logicielle purement nationale.

Ces moyens supplémentaires alloués à la DRSD ont notamment contribué au renforcement de ses missions de contre-ingérence économique et de contre-ingérence cyber. Selon les informations transmises au rapporteur spécial, le niveau d'activité de la contre-ingérence économique a désormais dépassé celui de la contre-ingérence des forces. La DRSD effectue notamment 180 missions de protection par an pour vérifier que les entreprises de la BITD sont suffisamment protégées et qu'elles appliquent bien les réglementations auxquelles elles sont soumises. Elle a également mis en place, en 2023, un centre de réponse aux incidents cyber au profit des PME du secteur de la défense (CERT-ED), qui ne sont pas couvertes par l'action de l'ANSSI *(voir le B du présent II)*.

● **La DGSE a elle aussi vu ses moyens budgétaires et humains augmenter**, notamment depuis l'adoption de la LPM pour 2019-2025 [(1)]. Le montant moyen des crédits de paiement sur la période 2018-2025 a ainsi augmenté de 50 % par rapport aux huit années précédentes. La hausse des crédits accompagne la progression des effectifs, prévue dans le cadre de la LPM, ainsi que l'**augmentation de l'activité opérationnelle**, dans un **contexte de menaces accrues** et multiformes.

Ainsi, la DGSE consacre une grande part de son budget à des **investissements techniques** visant à maintenir en capacité ses matériels opérationnels et à développer des moyens innovants pour recueillir, traiter et exploiter des masses de données de plus en plus volumineuses. Ces investissements sont cruciaux pour permettre à la DGSE et aux autres services de la communauté du renseignement – le service étant chef de file sur un certain nombre de programmes interministériels profitant à l'ensemble de la communauté du renseignement – de garder un temps d'avance sur leurs adversaires.

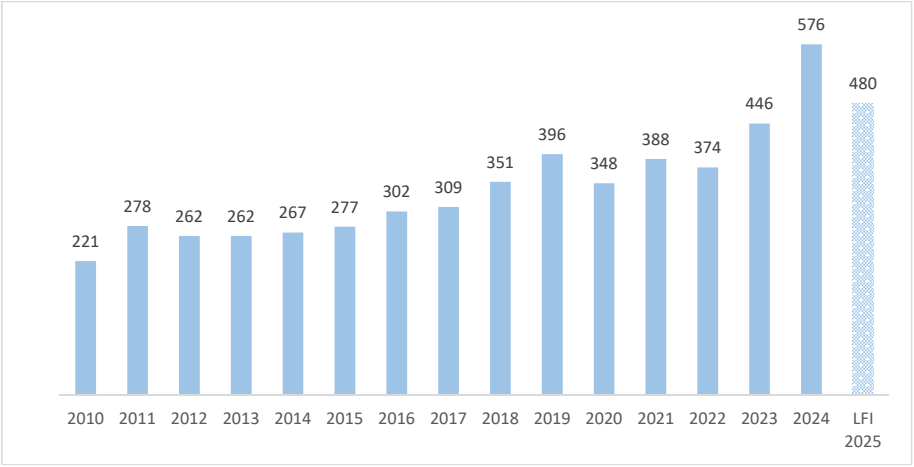
L'accroissement des crédits profite aussi aux investissements immobiliers, notamment au **projet de nouveau siège** de la direction centrale, au Fort neuf de Vincennes, dont le marché principal de travaux a été notifié et engagé en 2024, et dont les travaux ont commencé au premier semestre 2025, pour un emménagement envisagé à l'horizon 2030. Le financement du projet de nouveau siège – dont le coût

(1) Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

total s'élèvera à 1,3 milliard d'euros [1] – est un enjeu majeur pour la DGSE : dans la mesure où il s'agit d'une dépense contrainte, toute remise en cause de la trajectoire budgétaire prévue dans la programmation 2024-2030 aurait un effet d'éviction sur d'autres dépenses, notamment sur les investissements techniques et donc sur les capacités du service.

MONTANT DES CRÉDITS DE PAIEMENT ALLOUÉS À LA DGSE

(en millions d'euros)



Source : commission des finances d'après les annexes budgétaires.

L'augmentation du budget de la DGSE a permis au service de **renforcer ses moyens consacrés à l'intelligence économique**. Depuis sa réorganisation intervenue en 2022, la DGSE est dotée d'un service entièrement consacré à la contre-ingérence économique. Selon les informations communiquées au rapporteur spécial, ce centre de mission est, en termes d'effectifs, d'une taille équivalente à celui chargé de la lutte contre le terrorisme, ce qui témoigne là aussi de la montée en puissance de ces questions au sein du service.

Depuis 2022, la DRSD comme la DGSE tendent à effectuer une bascule d'effort de l'Afrique vers l'Europe de l'est, pour accompagner le redéploiement des forces armées dans le cadre des opérations de réassurance menées pour renforcer la défense du flanc est de l'OTAN. La présence des services de renseignement en Pologne, en Roumanie ou encore en Estonie leur permet notamment de mieux suivre les entreprises françaises qui se mobilisent pour soutenir l'Ukraine dans son effort de résistance contre la Russie, lesquelles sont naturellement des cibles privilégiées.

(1) Une ouverture de 1,1 milliard d'euros est intervenue en 2021, suivie d'un abondement complémentaire de 184 millions d'euros en 2023.

B. LE RENFORCEMENT DES OUTILS À LA DISPOSITION DE L'ÉTAT EN MATIÈRE DE GUERRE ÉCONOMIQUE

L'arsenal des outils à la disposition des services de l'État s'est renforcé au fil du temps. Plusieurs évolutions réglementaires ont permis une mise en œuvre efficace et une capacité d'adaptation rapide des dispositifs à l'évolution des menaces. Les effets de cette politique de sécurité économique renforcée sont souvent discrets mais réels (rachat d'entreprise bloqué ou encadré, propriété intellectuelle protégée, opposition à un partenariat de recherche, mise en évidence d'un vol de technologie ou d'un cas de concurrence déloyale, etc.).

1. La densification du contrôle des investissements étrangers en France

Le **contrôle des investissements étrangers en France (IEF)**, opéré par la direction générale du trésor, et par la DGA pour ce qui concerne les entreprises du secteur de la défense, est l'**outil le plus visible de la politique de sécurité économique**.

Si les relations financières entre la France et l'étranger sont libres, en principe, elles peuvent être limitées, par exception, pour assurer la défense des intérêts nationaux. L'article L. 151-3 du code monétaire et financier **soumet à une autorisation préalable du ministre de l'économie les investissements étrangers dans les activités sensibles**. Les entreprises entrant dans le champ du contrôle sont tenues à une obligation de déclaration préalable auprès de la direction générale du trésor, sous peine de sanction (amende pouvant aller jusqu'à 10 % du chiffre d'affaires, poursuites pénales des dirigeants, annulation de l'opération). L'autorisation de l'État peut être refusée ou assortie de conditions visant à assurer que l'investissement ne portera pas atteinte aux intérêts nationaux.

Depuis plusieurs années, le contrôle des investissements étrangers en France a été modernisé, avec un rôle accru du SISSÉ, afin de mieux préserver les intérêts fondamentaux de la Nation, de soutenir l'autonomie stratégique de la France et de renforcer la résilience des chaînes de valeur.

● La **liste des investissements soumis à une autorisation préalable a été élargie**. N'entrent dans le champ du contrôle que les prises de participation par un investisseur étranger dans une **entité de droit français**. Ce critère a longtemps exclu les opérations de rachat d'une filiale française détenue par une société de droit étranger. Cette lacune a été comblée en 2023, pour viser tout « *établissement immatriculé au registre du commerce et des sociétés en France* » [(1)].

En outre, le **seuil de déclenchement du contrôle**, en termes de détention directe ou indirecte de droits de vote ou de capital, initialement fixé à 33 %, a été abaissé à 25 % et à 10 % pour les sociétés cotées (d'abord en 2020 à titre

(1) Décret n° 2023-1293 du 28 décembre 2023 relatif aux investissements étrangers en France.

temporaire [1] puis, après trois prolongations du dispositif [2] [3] [4], à titre permanent à compter du 1er janvier 2024 [5]), pour les investissements réalisés par une personne n'étant ni ressortissant d'un État membre de l'Union européenne ni ressortissant d'un État partie à l'Espace économique européen.

● Par ailleurs, le contrôle des investissements étrangers en France a été étendu à un nombre croissant d'activités et de secteurs économiques stratégiques. La **liste des activités soumises à autorisation**, fixée par décret en Conseil d'État, a été **continuellement étendue** depuis le milieu des années 2010 :

– en 2014, sous l'impulsion du ministre de l'économie Arnaud Montebourg, la liste est allongée aux activités liées à l'exploitation d'infrastructures critiques (approvisionnement en eau et en énergie, réseaux et services de transport, communications électroniques, protection de la santé publique) [6] ;

– en 2018, la liste est complétée des activités liées aux opérations spatiales, à la captation de données informatiques, aux systèmes d'information liés aux missions de la police et de la gendarmerie nationales ou de la sécurité civile, aux activités de recherche et développement relatives à certaines technologies critiques (cybersécurité, robotique, semi-conducteurs, intelligence artificielle, fabrication additive) ainsi qu'à l'hébergement de données stratégiques [7] ;

– en 2020, de nouveaux secteurs sont inclus dans la liste, tels que la sécurité alimentaire et la presse d'information politique et générale [8] ;

– entre 2020 et 2024, à la faveur d'une réécriture du décret relatif aux investissements étrangers soumis à autorisation préalable, la liste des technologies critiques est étendue par voie d'arrêté aux technologies quantiques et au stockage

(1) Décret n° 2020-892 du 22 juillet 2020 relatif à l'abaissement temporaire du seuil de contrôle des investissements étrangers dans les sociétés françaises dont les actions sont admises aux négociations sur un marché réglementé.

(2) Décret n° 2020-1729 du 28 décembre 2020 modifiant le décret n° 2020-892 du 22 juillet 2020 relatif à l'abaissement temporaire du seuil de contrôle des investissements étrangers dans les sociétés françaises dont les actions sont admises aux négociations sur un marché réglementé.

(3) Décret n° 2021-1758 du 22 décembre 2021 prorogeant l'abaissement temporaire du seuil de contrôle des investissements étrangers dans les sociétés françaises dont les actions sont admises aux négociations sur un marché réglementé.

(4) Décret n° 2022-1622 du 23 décembre 2022 relatif à l'abaissement temporaire du seuil de contrôle des investissements étrangers dans les sociétés françaises dont les actions sont admises aux négociations sur un marché réglementé.

(5) Article R. 151-2 du code monétaire et financier, dans sa rédaction résultant du décret n° 2023-1293 du 28 décembre 2023 relatif aux investissements étrangers en France.

(6) Décret n° 2014-479 du 14 mai 2014 relatif aux investissements étrangers soumis à autorisation préalable.

(7) Décret n° 2018-1057 du 29 novembre 2018 relatif aux investissements étrangers soumis à autorisation préalable.

(8) Décret n° 2019-1590 du 31 décembre 2019 relatif aux investissements étrangers en France.

d'énergie [1], aux biotechnologies [2], aux technologies intervenant dans la production d'énergie renouvelable [3] et à la photonique [4].

● La modernisation du contrôle des investissements étrangers en France a aussi consisté, notamment dans le cadre de la loi PACTE [5], en un **durcissement des sanctions** en cas de non-respect par un investisseur de ses obligations.

Si **un investissement étranger** a été **réalisé sans autorisation préalable**, le ministre chargé de l'économie peut désormais enjoindre à l'investisseur de déposer une demande d'autorisation, de rétablir à ses frais la situation antérieure et de modifier l'investissement (I de l'article L. 151-3-1 du code monétaire et financier), ces injonctions pouvant être assorties d'une astreinte. Si la protection des intérêts nationaux est compromise ou susceptible de l'être, le ministre chargé de l'économie peut également suspendre les droits de vote attachés à la fraction des parts dont la détention par l'investisseur aurait dû faire l'objet d'une autorisation préalable, interdire ou limiter la distribution des dividendes ou des rémunérations attachés à ces parts, suspendre, restreindre ou interdire la libre disposition des actifs concernés, et désigner un mandataire chargé de veiller, au sein de l'entreprise, à la protection des intérêts nationaux.

Par ailleurs, si les **conditions** dont est assorti un investissement étranger ayant fait l'objet d'une autorisation ont été **méconnues**, le ministre chargé de l'économie peut retirer l'autorisation, enjoindre à l'investisseur de se mettre en conformité dans un certain délai ou lui enjoindre de respecter des prescriptions alternatives, ces injonctions pouvant être assorties d'une astreinte (II du même article L. 151-3-1).

En outre, en cas de réalisation d'un investissement sans autorisation préalable, d'obtention par fraude d'une autorisation préalable, de non-respect des conditions dont est assorti un investissement, d'inexécution des décisions ou injonctions prises par le ministre chargé de l'économie, ce dernier peut infliger à l'investisseur **une sanction pécuniaire pouvant aller jusqu'à 10 % du chiffre d'affaires annuel hors taxes de l'entreprise**, cinq millions d'euros pour les personnes morales et un million d'euros pour les personnes physiques (article L. 151-3-2 du code monétaire et financier).

● Ainsi renforcé et modernisé, le **contrôle** des investissements étrangers en France apparaît comme étant **complet et efficace**, en maintenant un équilibre entre, d'une part, la nécessité de préserver les intérêts nationaux ainsi que nos savoir-faire industriels et technologiques et, d'autre part, le besoin de préserver l'attractivité économique de la France, sans dissuader les investisseurs potentiels. Un récent rapport parlementaire sur le sujet souligne à cet égard que la portée du régime

(1) Arrêté du 31 décembre 2019 relatif aux investissements étrangers en France.

(2) Arrêté du 27 avril 2020 relatif aux investissements étrangers en France.

(3) Arrêté du 10 septembre 2021 relatif aux investissements étrangers en France.

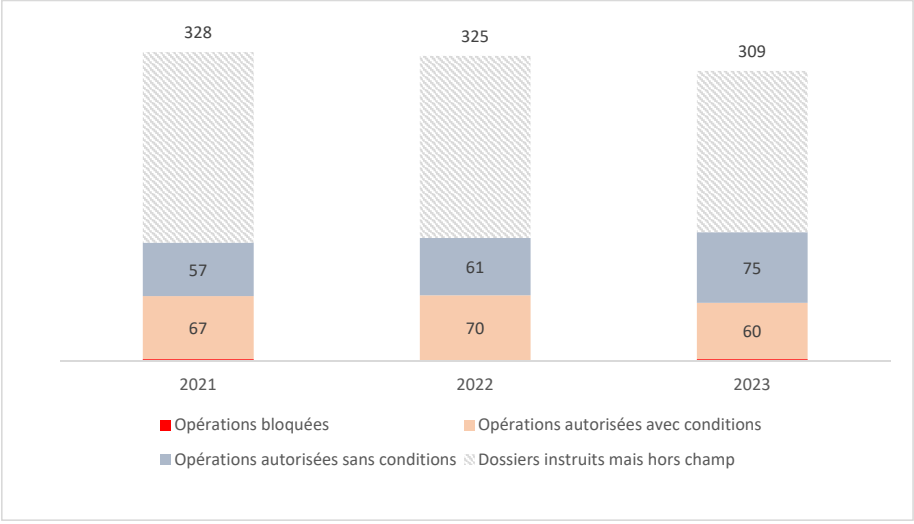
(4) Arrêté du 28 décembre 2023 relatif aux investissements étrangers en France.

(5) Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises.

français est sinon supérieure du moins comparable à celle des régimes équivalents dans d'autres pays européens (1).

Le nombre de dossiers examinés au titre du contrôle des investissements étrangers en France tend à augmenter ces dernières années, passant de moins de 200 par an avant 2020 à plus de 300 par an depuis 2021. Cette hausse s'est poursuivie en 2024, notamment du fait d'une augmentation de l'activité des fusions-acquisitions et de la mise en place d'une plateforme en ligne (« plateforme IEF ») qui facilite le dépôt des demandes. Un peu moins d'un quart des autorisations délivrées au titre du contrôle concernaient des entreprises exerçant une activité dans le secteur de la défense (21,5 % en 2023 et 23,7 % en 2022).

LE CONTRÔLE DES INVESTISSEMENTS ÉTRANGERS EN FRANCE



Source : commission des finances d'après les rapports annuels sur le contrôle des investissements étrangers en France.

Un peu plus de la moitié des dossiers relevant du champ du contrôle n'ont été autorisés qu'assortis de **conditions imposées aux investisseurs**. Il peut s'agir, par exemple, d'imposer le maintien de la propriété intellectuelle ou des centres de R&D d'une entreprise en France. Ces conditions peuvent aller jusqu'à isoler une partie de l'activité de l'entreprise, sous l'autorité d'un mandataire indépendant, désigné par le ministre de l'économie, chargé de veiller à la protection des intérêts nationaux, qui peut faire obstacle à toute décision de nature à porter atteinte à ces intérêts.

Ces conditions sont formalisées sous la forme de lettres d'engagement, négociées par la DGA avec les investisseurs étrangers, destinées à protéger les intérêts français et éviter le pillage ou la vente à la découpe. En 2024, la sous-

(1) Assemblée nationale, rapport d'information n° 1453 (XVII^e législature), de MM. François Jolivet et Hervé de Lépinau, au nom du Comité d'évaluation et de contrôle des politiques publiques, sur l'évaluation du contrôle des investissements étrangers en France, enregistré à la présidence le 22 = mai 2025.

direction de la protection et de la résilience des entreprises a traité près de 120 dossiers liés à des investissements étrangers en France. En outre, **plus de 200 lettres d'engagement sont actuellement actives, dont la DGA assure un suivi strict**, n'hésitant pas, si nécessaire, à imposer des pénalités financières jusqu'à la mise en conformité des investisseurs avec leurs engagements.

Les **opérations bloquées** sont quant à elles rares, avec un seul cas en 2021 (Photonis) et deux en 2023 (Segault et Carrefour [(1)]). Le dispositif n'en reste pas moins dissuasif. La menace d'un blocage ou d'une autorisation sous conditions favorise la mise en place d'un dialogue régulier entre les services de l'État, les entreprises ciblées et les investisseurs, qui permet d'accompagner les opérations lorsqu'elles peuvent se faire sans danger mais aussi d'envoyer des messages lorsque cela s'avère nécessaire.

Il convient d'ajouter que le travail des administrations, et en particulier celui de la DGA, est de protéger les activités souveraines, mais aussi de ne pas se laisser instrumentaliser en donnant de la valeur à des activités qui ne sont pas au cœur de la souveraineté. Ainsi, toutes les activités d'Atos ne participant pas au maintien de la dissuasion, l'État, après un audit approfondi de l'Agence des participations de l'État, ne projette d'en racheter que l'activité « advanced computing » (serveurs de haute performance, supercalculateurs, technologies critiques). S'agissant de Vencorex, sous la menace d'un rachat par le groupe chinois Wanhua, il faut souligner que ce rachat ne concerne pas l'activité de production de sels purifiés qui sont utilisés dans certains matériels stratégiques, qu'il n'induit aucun transfert de technologie, et que la France dispose de stocks suffisants et de sources d'approvisionnement alternatives. Il n'est, de fait, pas souhaitable de mobiliser les moyens publics destinés à protéger la souveraineté du pays pour des entreprises ou des activités qui ne sont pas critiques, ni de prendre le risque de complexifier inutilement les stratégies de sortie des investisseurs au risque de décourager les investissements futurs.

C'est donc bien à **un équilibre entre la protection des actifs stratégiques et l'attractivité économique de la France** qu'il faut trouver, avec des solutions adaptées à chaque dossier. Dans l'ensemble, on peut dire que le contrôle des investissements étrangers en France tel qu'il est organisé aujourd'hui n'est pas loin de l'équilibre idéal.

Seules deux marges de progression ont pu être identifiées par le rapporteur spécial, également portées par le rapport de M. Geoffroy Roux de Bézieux sur la sécurité économique des entreprises. D'une part, les services de l'État gagneraient à mieux anticiper la sortie des fonds d'investissement, de façon à prendre contact avec eux, préalablement à leur sortie, pour leur indiquer le cadre dans lequel la cession de leur part sera possible ou ne le sera pas, sans attendre qu'ils aient conclu avec d'autres investisseurs un accord de rachat qui serait contraire aux intérêts nationaux. Cette clarification des règles, au cas par cas, contribuerait à renforcer la sécurité juridique des fonds, et donc l'attractivité des entreprises concernées.

---

(1) Dans le cas de Carrefour, le blocage n'est pas allé jusqu'à son terme, la menace de blocage ayant conduit l'investisseur à renoncer à son projet d'investissement.

Recommandation n° 1 : Dans le cadre du contrôle des investissements étrangers en France, mieux anticiper la sortie des fonds d'investissement.

D'autre part, l'État ne dispose en réalité que de peu d'outils pour suivre dans le temps les engagements qu'il impose aux entreprises ou aux fonds dans le cadre du contrôle des investissements étrangers. Plus les engagements sont anciens et plus leur respect dépend de la bonne volonté des entreprises et du *turn-over* des services de contrôle. Afin de renforcer les contrôles et de les internaliser au sein des entreprises sensibles, la pratique des *proxy boards*, qui existent aux États-Unis ou en Australie, pourrait être systématisée. Ces conseils d'administration alternatifs, qui coexistent avec les conseils d'administration, et qui sont uniquement composés de ressortissants nationaux, disposent d'un droit de veto sur certaines décisions non économiques de leur entreprise, de façon à bloquer, par exemple, la nomination d'un directeur général ou un déménagement d'infrastructures qui seraient contraires aux intérêts nationaux.

Recommandation n° 2 : Dans le cadre du contrôle des investissements étrangers en France, généraliser la pratique du conseil d'administration alternatif (*proxy board*) pour renforcer le suivi des engagements imposés aux investisseurs étrangers.

2. La modernisation de la loi de blocage du 26 juillet 1968

Le renforcement de la politique de sécurité économique a également été permis par la réactivation de la loi de blocage du 26 juillet 1968 (1), modifiée en 1980 (2). Cette loi, qui **permet aux entreprises françaises confrontées à des demandes intrusives d'informations sensibles de la part d'autorités de poursuite étrangères de se tourner vers l'administration pour un accompagnement**, prévoit une double interdiction :

– il est interdit à toute personne physique de nationalité française ou résidant habituellement sur le territoire français et à tout dirigeant, représentant, agent ou préposé d'une personne morale y ayant son siège ou un établissement de communiquer par écrit, oralement ou sous toute autre forme, en quelque lieu que ce soit, à des autorités publiques étrangères, les documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que de besoin (article 1er) ;

– il est interdit à toute personne de demander, de rechercher ou de communiquer, par écrit, oralement ou sous toute autre forme, des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique

(1) Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.

(2) Loi n° 80-538 du 16 juillet 1980 relative à la communication de documents ou renseignements d'ordre économique, commercial ou technique a des personnes physiques ou morales étrangères.

tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci (article 1er *bis*).

La loi n° 68-678 du 26 juillet 1968 dite de blocage dans sa rédaction résultant de la loi n° 80-538 du 16 juillet 1980

Article 1er. – Sous réserve des traités ou accords internationaux, il est interdit à toute personne physique de nationalité française ou résidant habituellement sur le territoire français et à tout dirigeant, représentant, agent ou préposé d'une personne morale y ayant son siège ou un établissement de communiquer par écrit, oralement ou sous toute autre forme, en quelque lieu que ce soit, à des autorités publiques étrangères, les documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que de besoin.

Article 1er bis. – Sous réserve des traités ou accords internationaux et des lois et règlements en vigueur, il est interdit à toute personne de demander, de rechercher ou de communiquer, par écrit, oralement ou sous toute autre forme, des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci.

Article 2. – Les personnes visées aux articles 1er et 1er *bis* sont tenues d'informer sans délai le ministre compétent lorsqu'elles se trouvent saisies de toute demande concernant de telles communications.

Article 3. – Sans préjudice des peines plus lourdes prévues par la loi, toute infraction aux dispositions des articles 1er et 1er *bis* de la présente loi sera punie d'un emprisonnement de six mois et d'une amende de 18 000 euros ou de l'une de ces deux peines seulement.

Pendant **longtemps**, la loi de blocage est **demeurée largement inappliquée**. Aucune autorité n'était clairement définie pour en assurer l'application et sa méconnaissance ne donnait pas lieu à sanction. Même invoquée devant des autorités étrangères, elle ne conférait pas de protection solide et était le plus souvent écartée.

En 2016, le rapport d'une mission d'information sur l'extraterritorialité de la législation américaine dénonçait l'inefficacité de la loi de blocage en ces termes : « *[l]e principal reproche opposé par les juridictions américaines à la loi française est son manque de caractère contraignant en raison d'une jurisprudence trop peu abondante. Les cours américaines ont toujours écarté la loi de blocage, estimant qu'elle n'impliquait pas de risque réel de poursuites pour les personnes en infraction avec ses dispositions. Il est vrai que des personnalités françaises auditionnées par la mission ont reconnu que, jusqu'à présent, la volonté d'appliquer cette loi avait le plus souvent été faible, que ce soit dans les sphères politiques ou dans les sphères administratives. D'autres ont relevé les imperfections de sa rédaction, très générale, alors qu'une rédaction plus "serrée" pourrait être plus efficace en évitant que le texte ne soit*

invoqué en quelque sorte pour le principe, comme argument de discussion, plus que pour justifier réellement la non-transmission d'informations réellement sensibles » (1).

Un rapport du député Raphaël Gauvain dressait un constat similaire en 2019, estimant que la loi de blocage demeurait « *très limitée à ce jour, pour plusieurs raisons […] : la quasi-absence de décision de justice la mettant en œuvre (une seule en 50 ans) ; […] ; l'absence de mise en œuvre effective de l'obligation de déclaration prévue à l'article 2 ; l'absence de politique pénale ou d'orientations claires du ministère de la justice pour la mise en œuvre de la loi. Ces faiblesses structurelles entament son crédit à l'étranger et en conséquence la loi de 1968 est souvent écartée par les juridictions étrangères* » (2).

Depuis, **la loi de blocage a été modernisée**, sous l'impulsion du SISSÉ, en coopération avec les services de renseignement. Ses modalités d'application ont été précisées, au niveau réglementaire, avec la publication en 2022 d'un nouveau décret (3) et d'un nouvel arrêté (4) redéfinissant le cadre dans lequel les interdictions prévues au niveau législatif sont applicables :

– le ministre chargé de l'économie est désigné comme le ministre chargé de la mise en œuvre de la loi, les ministres des affaires étrangères et de la justice devant être informés des demandes dont il est saisi ;

– les personnes visées par la loi sont tenues, dans les plus brefs délais et avant toute publicité, d'informer le SISSÉ des demandes de communication émises par une autorité publique étrangère ou par toute personne agissant pour son compte ou en vue de répondre à sa demande ;

– le SISSÉ procède à l'instruction des dossiers déposés, en lien avec les ministères de la justice, des affaires étrangères et les autres ministères ou autorités compétentes concernés. Il adresse à la personne désignée par la société, dans un délai d'un mois à compter du dépôt du dossier complet, un avis autorisant ou interdisant la communication des informations demandées.

Cette réforme **a permis de clarifier la procédure pour les entreprises** concernées et de faire du **SISSÉ** un **guichet unique pour centraliser l'ensemble des demandes**. Ces dernières peuvent ainsi s'adresser à un interlocuteur bien identifié et en lien avec les différentes administrations de l'État. La détermination

---

(1) Assemblée nationale, rapport n° 4082 (XIVe législature), déposé en application de l'article 145 du règlement de l'Assemblée nationale par la commission des affaires étrangères et la commission des finances, en conclusion d'une mission d'information sur l'extraterritorialité de la législation américaine, enregistré à la présidence le 5 octobre 2016.

(2) Rapport établi par M. Raphaël Gauvain, député, à la demande de M. Édouard Philippe, Premier ministre, « Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale », 26 juin 2019.

(3) Décret n° 2022-207 du 18 février 2022 relatif à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.

(4) Arrêté du 7 mars 2022 relatif à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.

d'un délai leur permet aussi de disposer d'un avis de l'administration dans un calendrier adapté aux procédures administratives ou judiciaires auxquelles elles peuvent être confrontées.

Surtout, **la loi de blocage est devenue crédible**, parce qu'elle s'inscrit désormais dans un cadre juridique clair, cohérent et donnant lieu à l'application de sanctions dissuasives. Elle confère une réelle protection aux entreprises et personnes subissant des demandes d'information abusives, en leur donnant une « excuse légale » pour ne pas se soumettre à certaines des demandes formulées par des autorités administratives et judiciaires étrangères, et l'avis donné par les services de l'État est admis et respecté par ces dernières.

Selon le SISSÉ, les premiers effets de la réforme ont été supérieurs aux attentes. De plus en plus d'entreprises, y compris des sociétés étrangères, viennent s'adresser au guichet unique. Le SISSÉ rend désormais entre 50 et 60 avis par an. Le nombre de saisines a été multiplié par cinq par rapport à la période antérieure (1), et le réservoir de transactions susceptibles de passer par les voies de la loi de blocage est sans doute encore important.

À cet égard, le SISSÉ souligne la grande diversité des dossiers reçus, à la fois dans leur origine géographique (52 % d'Amérique du Nord, 30 % de l'Union européenne ou du Royaume-Uni, 7 % d'Asie) et dans leur nature (42 % de procédures civiles, 30 % de procédures pénales, 28 % de procédures administratives). Ce succès peut notamment être attribué « *à la notoriété du dispositif, à la confiance qu'il suscite auprès des entreprises, à la crainte de la sanction en cas de non-notification et à l'efficacité de l'administration* » (2).

Le rapporteur spécial salue l'action des services de l'État, qui sont parvenus à redonner à un outil ancien une utilité réelle. Il relève toutefois la faiblesse des sanctions encourues : une sanction de 18 000 euros est considérée comme dérisoire aux États-Unis. Afin de renforcer le caractère dissuasif de la loi de blocage, il pourrait être envisagé d'alourdir les sanctions liées à la méconnaissance de la loi de 26 juillet 1968, par exemple en allant jusqu'à fixer un montant d'amende proportionnel au chiffre d'affaires de l'entreprise concernée.

Recommandation n° 3 : Alourdir le montant des amendes pouvant être prononcées en cas de méconnaissance de la loi de blocage.

(1) Cabinet Skadden, « Loi de blocage : le SISSÉ, le parquet national financer, le département de la justice des États-Unis et le ministère de la justice tirent les premières leçons de la réforme de 2022 », table-ronde de hauts responsables de l'administration française et américaine organisée par le cabinet Skadden, à Paris, le 27 novembre 2023.

(2) Cabinet Skadden, ibid.

3. Le renforcement des moyens de cyberdéfense

La menace cyber impose des protections spécifiques. Face à l'augmentation des attaques informatiques, les moyens consacrés à la cybersécurité et à la cyberdéfense des entreprises ont également été confortés, à la fois pour la BITD et pour l'ensemble des secteurs.

● Dans un cadre juridique défini notamment par les directives NIS (*network and information system security*) [1] [2], le renforcement de la politique de cybersécurité **s'appuie en grande partie sur l'action de l'Agence nationale de la sécurité des systèmes d'information** (ANSSI), qui est chargée de piloter la stratégie nationale pour la sécurité du numérique, présentée en 2015, et renforcée par la revue stratégique de cyberdéfense, présentée en 2018.

L'ANSSI accompagne les entreprises stratégiques, notamment les grands groupes de la BITD, ainsi que les opérateurs de service essentiel [3] et les fournisseurs de service numérique [4] dans l'élévation de leur niveau de maturité cyber, afin de mieux préserver les intérêts économiques et sociaux du pays. Les entités concernées se voient imposer d'appliquer des règles de sécurité d'un niveau minimal et peuvent être sanctionnées si elles ne sont pas en conformité avec leurs obligations.

L'ANSSI a également permis la **mise en place du CERT-FR**, un *computer emergency response team* (centre de réponse aux incidents de sécurité informatique). Ce dispositif, ouvert à l'ensemble des entreprises stratégiques et aux opérateurs d'importance vitale, mais aussi à l'ensemble des administrations et aux collectivités territoriales, leur permet de déclarer à l'ANSSI tout incident de sécurité susceptible d'avoir un impact sur la continuité de leurs services. Il permet ainsi à l'ANSSI d'apporter aux entités concernées un soutien dans la résolution des difficultés qu'elles rencontrent, mais aussi de limiter la propagation des attaques en cours et d'anticiper d'éventuelles attaques futures.

---

(1) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union ; elle a été transposée en 2018.

(2) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148. Elle ne s'adresse plus uniquement aux opérateurs de service essentiel et aux fournisseurs de service numérique, mais accroît considérablement le nombre d'entités et de secteurs soumis à des règles de sécurité informatique harmonisées. Sa transposition devait intervenir avant le 17 octobre 2024. Le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, qui porte cette transposition, est en cours d'examen par le Parlement.

(3) Sont ainsi désignés les opérateurs exerçant des missions dites « essentielles » au sens du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

*(4) Sont ainsi désignés les opérateurs qui fournissent soit des places de marché de ligne, soit des moteurs de recherche en ligne, soit des services d'informatique en nuage (*cloud*), à condition d'avoir un chiffre d'affaires annuel supérieur à 10 millions d'euros ou un nombre d'employés supérieur à cinquante.*

● L'action de l'ANSSI se concentrant nécessairement sur les opérateurs d'importance nationale, elle ne concerne que les grands donneurs d'ordre de la BITD. **Pour les PME de l'industrie de défense, elle est donc prolongée par la DRSD**.

La DRSD accompagne la **montée en maturité cyber des entreprises** exerçant tout ou partie de leur activité dans le secteur de la défense, notamment par la réalisation d'inspections et de contrôles des systèmes d'informations directement liés à des activités de défense. Ces inspections et contrôles servent à vérifier que les niveaux d'exigence cyber précisés dans les contrats de marchés défense sont bien atteints par les entreprises. Le service réalise également des actions de sensibilisation au profit des dirigeants des diverses entités de la BITD.

En outre, en complément du CERT-FR de l'ANSSI, la DRSD a mis en place, en 2023, **un CERT-ED destiné spécifiquement aux PME de la BITD** qui ne dépendent pas du périmètre de l'ANSSI. Comme le CERT-FR, le CERT-ED permet aux entreprises de déclarer leurs incidents de sécurité, d'être assistées dans la gestion de leurs incidents, d'être informées des incidents subis par d'autres entreprises et de mieux anticiper les attaques futures. Ce dispositif est essentiel en ce qu'il assure un meilleur niveau de protection pour des entités qui sont souvent les principales cibles des groupes cybercriminels pour mettre à mal les chaînes d'approvisionnement des grands donneurs d'ordre.

Le CERT-ED traite tous les types d'incidents de cybersécurité qui surviennent ou menacent de survenir au sein de la sphère défense. Le niveau d'assistance fourni varie en fonction du type et de la gravité de l'incident, des systèmes concernés, de l'impact potentiel de l'incident ou encore de la taille de la communauté d'utilisateurs affectée. À titre d'exemple, la DRSD met en garde contre « *[l]a mise en œuvre de nouveaux malwares de la famille des "infostealer" par des acteurs cybercriminels (méthode d'accès initiale concurrente à l'hameçonnage) [qui] offre aux attaquants des points d'entrée facile dans les entreprises. Le CERT [ED] apporte ainsi son expertise dans les recommandations d'emploi des moyens numériques, notamment sur le cloisonnement de l'utilisation des ordinateurs / téléphones professionnels et privés. Enfin, face à des acteurs cybermalveillants, tels que NoName057 apparu au début du conflit russo-ukrainien et spécialisé dans les attaques DDoS ou encore LockBit plus connu pour ses rançongiciels et dont les attaques ont redoublé ces derniers mois, le CERT [ED] accompagne les entreprises dans la réponse à incidents en les conseillant sur les mesures d'urgence et les bonnes pratiques pour limiter les conséquences de l'incident cyber* » [(1)].

Fonctionnant sur le principe de l'abonnement, le CERT-ED a vocation à monter en puissance au fur et à mesure que le nombre de ses utilisateurs augmentera.

(1) DRSD, « Panorama des ingérences contre la sphère de défense », Lettre d'information économique, n° 13, juin 2023.

● Dans le prolongement des actions de l'ANSSI et de la DRSD, la DGA s'emploie également à élever le niveau de cybersécurité et de cyberdéfense des entreprises de la BITD.

La DGA a mis en place un **référentiel de maturité cyber**, qui contient un certain nombre d'exigences en matière de cybersécurité, et qui constitue le niveau minimal de protection attendu des entreprises souhaitant travailler dans le secteur de la défense. Ce référentiel a pour objectif d'**accompagner** les entreprises dans l'élévation de leur niveau de cybersécurité ainsi que de **simplifier** et d'**harmoniser** les exigences qui leur sont imposées par les donneurs d'ordre étatiques et industriels. Il a vocation à être utilisé par les entreprises, soit dans le cadre d'un processus d'auto-évaluation, soit par les grands maîtres d'œuvre dans leurs relations avec leurs sous-traitants. Il ne concerne toutefois pas les contrats traitant d'informations protégées (diffusion restreinte) ou classifiées (secret, très secret), qui sont déjà soumis à des textes réglementaires spécifiques.

Le référentiel de maturité cyber **doit se déployer par paliers**, avec des exigences de plus en plus complètes. Le premier niveau, qui comprend vingt-et-une exigences élémentaires, a été conçu pour proposer des mesures organisationnelles simples et des mesures techniques fondées sur une configuration adaptée des systèmes d'exploitation ou de logiciels très standards. Il ne requiert pas d'investissement lourd en matériel ou de logiciel spécialisé. Ce niveau « *vise à assurer une sécurité minimale des systèmes d'information (SI) utilisés pour la réalisation des contrats identifiés par le donneur d'ordre comme concourant à des activités de défense* » [(1)]. Ce niveau « fondamental » sera par la suite complété par des niveaux supérieurs, qui s'appuieront notamment sur les règles issues de la transposition de la directive européenne « NIS 2 », afin assurer l'équivalence avec le maximum de référentiels existants.

Le référentiel de maturité cyber **va progressivement s'imposer dans les relations entre la DGA et l'industrie de défense**. Le niveau « fondamental » sera ainsi exigible au titre des clauses contractuelles. Les entreprises qui ne disposent pas d'un niveau de protection suffisant ou qui n'ont pas réalisé d'auto-évaluation de leur niveau de protection ne pourront alors plus contracter avec la DGA, ni directement, ni par l'intermédiaire d'un donneur d'ordre.

Le rapporteur spécial a conscience que le renforcement des contraintes cyber est de nature à entraîner des surcoûts pour les PME de l'industrie de défense. Il estime néanmoins qu'un haut niveau de cybersécurité doit prévaloir au sein de la BITD, notamment pour les entreprises les plus critiques, et qu'**un certain degré de contrainte est pour cela indispensable**. Les plans de certains matériels stratégiques, militaires comme commerciaux, dont le rapporteur spécial doit ici taire le nom, sont accessibles sur le *dark web* ; cela n'est pas acceptable. Les entreprises

(1) DRSD, « Le référentiel de maturité cyber (RMC) des entités de la sphère défense », Lettre d'information économique, n° 17, décembre 2024.

de la BITD ayant nécessairement accès à des données confidentielles, il est du devoir de l'État d'assurer leur plus grande protection.

En outre, l'existence du référentiel de maturité cyber est **un atout dans le contexte de guerre économique et de compétition normative**. Il doit ainsi réduire les risques d'ingérence, en permettant aux entreprises d'attester de leur niveau de maturité cyber autrement que via un audit par un tiers étranger. Il peut aussi éviter l'exclusion de certaines entreprises des marchés internationaux, la DGA travaillant à assurer la conformité du référentiel national aux référentiels internationaux.

Afin d'accompagner les petites entreprises à acquérir le niveau fondamental du référentiel de maturité cyber, la DGA, en lien avec Bpifrance, a également mis en place le « Diag Cyber », un **diagnostic de cybersécurité**, qui permet à certaines entreprises de **faire financer une partie des frais de cybersécurisation** qu'elles engagent. Ouvert aux entreprises de moins de 2 000 salariés, ce diagnostic consiste en une prestation d'audit et de conseil (phase A), éventuellement suivie d'un accompagnement à la mise en œuvre des recommandations et à l'acquisition de solutions de cybersécurisation (phase B). Dans ce cadre, la DGA peut prendre en charge 50 % du montant des frais liés à la phase A et 70 % des dépenses liées à la phase 2. Le reste à charge, volontairement laissé aux entreprises, vise à inciter celles-ci à s'impliquer dans la mise en œuvre des mesures de sécurisation. En 2023, 56 diagnostics cyber ont ainsi été réalisés ; ce chiffre apparaît modeste au regard du nombre d'entités concernées, mais il a vocation à augmenter dans les années à venir.

III. UN CADRE JURIDIQUE NATIONAL COMPLET ET EFFICACE, QUI APPELLE PEU D'ÉVOLUTIONS MAIS DES MOYENS SUPPLÉMENTAIRES

Si le système de protection et de soutien de la BITD s'est nettement renforcé depuis le milieu des années 2010, la montée des menaces pesant sur la BITD et le renouvellement des modes d'action de nos compétiteurs appellent à renforcer encore davantage les outils de souveraineté. Cela passe aussi par une évolution des mentalités des dirigeants d'entreprises et d'organismes de recherche, pas toujours au fait des enjeux de la guerre économique.

A. UNE ÉVOLUTION DES MENTALITÉS PROGRESSIVE MAIS INDISPENSABLE

« *Disons-le franchement : les Français ne cultivent pas le réalisme de leurs principaux concurrents pour lesquels il est aussi naturel qu'une respiration de défendre toutes les formes de souveraineté et de progrès de leurs pays* ». Par ces mots, le rapport Carayon relevait le décalage qui existe, en matière d'intelligence économique, entre la France et certains de ses concurrents. L'évolution des mentalités ne se décrète pas. Il est néanmoins nécessaire de renforcer nos actions de sensibilisation aux risques et aux bonnes pratiques, à tous les niveaux, pour cultiver une attitude plus réaliste et cesser d'être naïfs.

1. La poursuite des actions de sensibilisation aux risques et aux bonnes pratiques

Le rapport de M. Geoffroy Roux de Bézieux sur la sécurité économique des entreprises relève **un progrès dans la prise de conscience** des menaces, mais ajoute que les entreprises françaises, notamment les petites et moyennes entreprises ainsi que les entreprises de taille intermédiaire, doivent encore améliorer leur compréhension des enjeux de sécurité économique.

Les **entreprises de la BITD** sont, naturellement, **plus conscientes** des **menaces** qui pèsent sur elles en matière de guerre économique et de leurs **vulnérabilités**. Elles sont souvent davantage sensibilisées aux bonnes pratiques. L'évolution des tensions géopolitiques depuis la **crise du covid** et la **guerre en Ukraine** a contribué à réduire les éléments de naïveté qui pouvaient exister chez les plus habitués à une économie mondiale qu'on pensait encore il y a peu ouverte et régulée. Les grands groupes, mieux protégés, font désormais davantage attention à la manière dont leurs sous-traitants de rang 1 voire 2 se protègent eux-mêmes et protègent les données qu'ils leur partagent.

Toutes les vulnérabilités n'ont néanmoins pas disparu. Certains dirigeants ou collaborateurs continuent d'ignorer les menaces, soit parce qu'ils n'ont pas pris pleinement conscience des conséquences que peuvent entraîner les atteintes dont ils sont la cible, soit parce qu'ils ne se sentent pas concernés par les attaques. C'est notamment le cas de certaines PME dont l'activité est duale, qui n'ont qu'une petite partie de leur activité ou qui ne travaillent qu'occasionnellement dans le secteur la

défense. Certaines de ces entreprises n'en demeurent pas moins stratégiques ; ainsi, il a été présenté au rapporteur le cas d'une PME dont la quasi-totalité de la production est destinée au domaine civil, mais qui fabrique néanmoins des composants indispensables au fonctionnement des sous-marins nucléaires. D'autres entités ont certes intégré les menaces mais pratiquent une politique d'intelligence économique peu diffuse car isolée du reste des activités.

Par ailleurs, les PME, souvent confrontées à des réglementations nombreuses et lourdes, notamment lorsqu'elles intègrent la BITD, peuvent faire face à des **problématiques de ressources humaines**, qui les empêchent de se saisir des sujets de sécurité autant qu'elles le voudraient. Elles peuvent aussi rencontrer des **difficultés financières**, qui leur imposent des arbitrages au détriment de leur propre sécurité.

Le rapporteur spécial tient à saluer la qualité des **dispositifs mis en place par les services de l'État pour sensibiliser les entreprises** aux risques de guerre économique et à leurs vulnérabilités. Les lettres d'information économique publiées par la **DRSD** et les « Flash ingérence » de la **DGSI**, de même que les guides en matière de cybersécurité de l'ANSSI, sont utilement documentés pour expliquer les menaces, et sont de plus en plus utilisées par les services de sécurité des entreprises de la BITD pour développer en leur sein des réflexes de sécurité de base. Le **SISSÉ** a lui aussi produit des documents d'information, notamment s'agissant de la mise en œuvre de la loi de blocage.

Les **séances de sensibilisation aux risques**, aux menaces et aux bonnes pratiques se développent également, notamment de la part des services de renseignement. Elles s'adressent à l'ensemble des salariés des entreprises comme à leurs comités de direction. La DRSD, en particulier, effectue ainsi près de 1 000 missions de sensibilisation tous les ans. Elle a notamment pris l'habitude de proposer systématiquement des séances de sensibilisation en marge des salons du secteur de l'armement. Ses services sont de plus en plus demandés par les entreprises, certaines d'entre elles allant même jusqu'à en solliciter plusieurs au cours d'un même salon. Ces actions de sensibilisation doivent naturellement se poursuivre et se développer de manière à en élargir le nombre de bénéficiaires.

2. Renforcer la protection des organismes de recherche

Le **monde de la recherche** est aujourd'hui un secteur **particulièrement vulnérable**. Moins protégés que les entreprises, les organismes de recherche cultivent traditionnellement une certaine **ouverture à l'international**, qui se matérialise à la fois par la participation à de nombreux travaux menés en coopération européenne ou internationale et par l'accueil de nombreux étudiants étrangers – 40 % des doctorants en France sont de nationalité étrangère. Une telle attitude n'est d'ailleurs pas sans contribuer à l'excellence et à l'attractivité de nos laboratoires, écoles et instituts de recherche. Néanmoins, cette ouverture est susceptible d'être exploitée par des acteurs malveillants ciblant les savoirs et savoir-faire de pointe français, notamment en ce qui concerne la recherche de défense.

En outre, les organismes de recherche, du fait de l'**insuffisance de leurs ressources**, courent également le risque de devenir dépendants financièrement d'acteurs étrangers : « *[c]ertains États, conscients du besoin de financement des universités et des centres de recherche français n'hésitent pas à financer certaines chaires voire à racheter certains instituts pour y accroître leur influence. Il [peut également s'agir] de propositions de bourse dans des domaines ou sur des thématiques convoités par l'État financeur, ou encore de propositions de voyages d'études afin d'établir le contact avec certains chercheurs français. Ces financements poursuivent souvent un objectif double : promouvoir un narratif officiel attractif et faciliter de futures ingérences* » [(1)]. Un rapport d'information du Sénat de 2021 soulignait à cet égard la dépendance de certaines universités et de certains laboratoires universitaires aux étudiants chinois, qui constituent une part de plus en plus importante du nombre de chercheurs [(2)].

Comme le note la DRSD, ce constat est « *structurellement et conjoncturellement renforcé en ce qui concerne la recherche de défense française, pivot de la base industrielle et technologique de défense (BITD). Le lien étroit entre la recherche "de défense" et la souveraineté nationale, qui vise au maintien et au renforcement des capacités de défense françaises, expose davantage les secteurs scientifiques aux applications militaires et duales à ces menaces d'ingérence* » [(3)]. Les risques sont réels, avec des cas avérés de tentative de vol de données d'un prototype de logiciel conçu par un organisme de recherche ou de travaux pillés par des étudiants étrangers mettant en péril la suite de la carrière des chercheurs spoliés. Le monde universitaire aura bien sûr toujours besoin d'échanges, mais ces derniers doivent rester maîtrisés.

Une **sensibilisation répétée et régulière** est évidemment **nécessaire** pour que la contrainte soit non seulement comprise mais intégrée dans les habitudes. Il faut donc continuer de sensibiliser, à tous les niveaux. C'est là une nécessité qu'aucune évolution législative ou réglementaire ne pourra satisfaire. Il s'agit avant tout de cultiver une attitude. La sécurité économique n'est pas uniquement l'affaire de l'État. Nous avons tous collectivement à gagner à ce que chacun soit mieux protégé.

Par ailleurs, les **étudiants des écoles d'ingénieurs** sous la tutelle du ministère des armées, qui ont pourtant vocation, au moins pour certains d'entre eux, à intégrer la DGA ou des entreprises de la BITD, restent **encore peu sensibilisés aux enjeux de la guerre économique**. Ce constat n'est là encore pas nouveau ; le rapport Carayon faisait déjà état de ces « handicaps culturels » : « *nos élites, issues de la fonction publique ou de l'entreprise, n'ont été formées que superficiellement aux transformations de notre environnement économique international. La*

---

(1) DRSD, « La contre-ingérence dans le monde de la recherche de défense », Lettre d'information économique, n° 11, décembre 2022.

(2) Sénat, rapport d'information n° 873 (2020-2021) de M. André Gattolin, fait au nom d'une mission d'information sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences, enregistré à la présidence le 29 septembre 2021.

(3) DRSD, « La contre-ingérence dans le monde de la recherche de défense », Lettre d'information économique, n° 11, décembre 2022.

mondialisation s'inscrit certes dans leurs préoccupations ou parfois dans leurs ambitions personnelles ; l'attractivité des MBA aux États-Unis est croissante pour nos étudiants comme celle de la Silicon Valley pour nos chercheurs, plus nombreux là-bas que tous les personnels du CNRS. Mais l'idée d'enrichir leur pays d'origine de ces formations ou des connaissances acquises outre-Atlantique est restée pour eux en quelque sorte accessoire ».

Il a été indiqué au rapporteur spécial que des cours de sensibilisation aux équilibres mondiaux et aux enjeux de souveraineté dans les domaines de la défense, des nouvelles technologies ou encore de la transition écologique tendaient à se développer ou à devenir obligatoires plutôt qu'optionnels dans les troncs communs. Une telle évolution doit être soutenue et renforcée, pour **donner aux étudiants la vision la plus systémique et la moins naïve possible**.

Le rapporteur spécial note que l'Académie militaire de Saint-Cyr Coëtquidan a récemment ouvert un master spécialisé dans l'analyse de l'information stratégique multi-sources, délivrant un enseignement de troisième cycle pour la maîtrise opérationnelle des enjeux de l'information. Des initiatives similaires à celles qui se développent pour les officiers ont probablement vocation à être transposées pour les ingénieurs.

Recommandation n° 4 : Renforcer la sensibilisation des étudiants des écoles d'ingénieurs sous la tutelle du ministère des armées aux enjeux de la guerre économique.

3. Un cadre plus contraignant en matière de protection du potentiel scientifique et technique de la nation

Le dispositif de **protection du potentiel scientifique et technique de la nation** (PPST) est un autre outil à la disposition des services de l'État en matière de guerre économique. Il vise à **protéger les biens matériels et immatériels propres à l'activité scientifique et au développement technologique du pays**, en particulier les savoirs, expertises et technologies les plus sensibles des entreprises – qu'elles fassent ou ne fassent pas partie de la BITD – et des organismes de recherche publics ou privés localisés sur le territoire national.

Fondée sur l'article 413-7 du code pénal [(1)], la PPST repose sur un décret de 2011 [(2)] qui prévoit que « *la protection du potentiel scientifique et technique de la nation est assurée par concertation entre les pouvoirs publics et les chefs des services, établissements ou entreprises* » concernés. Il est notamment complété par un arrêté du Premier ministre [(3)] qui détermine la liste des éléments essentiels du

(1) Article 413-7 du code pénal : « Est puni de six mois d'emprisonnement et de 7 500 euros d'amende le fait, dans les services, établissements ou entreprises, publics ou privés, intéressant la défense nationale, de s'introduire, sans autorisation, à l'intérieur des locaux et terrains clos dans lesquels la libre circulation est interdite et qui sont délimités pour assurer la protection des installations, du matériel ou du secret des recherches, études ou fabrications. »

(2) Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation.

(3) Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation.

potentiel scientifique ou technique de la nation susceptibles soit de faire l'objet d'une captation de nature à affaiblir ses moyens de défense, à compromettre sa sécurité ou à porter préjudice à ses autres intérêts fondamentaux, soit d'être détournés à des fins de terrorisme, de prolifération d'armes de destruction massive et de leurs vecteurs ou de contribution à l'accroissement d'arsenaux militaires.

La PPST offre aux acteurs qui décident d'y avoir recours **une meilleure protection juridique contre les actes malveillants** pouvant avoir des conséquences sur la compétitivité ou la réputation de l'entité protégée (utilisation frauduleuse d'informations, vol ou captation de données sensibles, pratiques anticoncurrentielles, intrusion dans les systèmes d'information, etc.). Elle donne aussi accès à un soutien administratif de l'État facilitant l'élévation du niveau de sécurité.

Le principal outil concourant à la PPST est la **possibilité de mettre en place une ou plusieurs zones à régime restrictif** (ZRR) [(1)]. Une ZRR permet de circonscrire une zone de travail particulièrement sensible à la captation d'informations (moyens de production, zone de calcul, bureaux d'études) en maîtrisant les entrées et les sorties à l'intérieur de cette dernière. Tout accès y est soumis à autorisation, accordée après une étude par des services spécialisés. La ZRR offre ainsi une protection ciblée, sur mesure et adaptable : les entités qui choisissent d'adhérer au dispositif sont libres de définir leur niveau de protection en fonction de leurs moyens et de leurs besoins. La réglementation impose uniquement qu'une ZRR soit un espace clos, doté d'une signalétique informant du statut de cet espace et des conséquences pénales auxquelles s'expose une personne y entrant sans autorisation. Si les dispositions de travail évoluent, la ZRR peut être révoquée, réduite ou agrandie, mais aussi dupliquée suivant les besoins.

Pilotée par le secrétariat général de la défense et de la sécurité nationale (SGDSN), la PPST est mise en œuvre par chaque ministère, notamment le ministère des armées et le ministère de la recherche. Pour les entités relevant du ministère des armées, c'est la direction de la protection des installations, moyens et activités de la défense (DPID), accompagnée par la DGA et la DRSD, qui assiste la mise en place des dispositifs de la PPST, et notamment des ZRR [(2)].

La PPST est notamment mise en œuvre **au sein des écoles sous tutelle du ministère des armées**. Elle leur permet de mettre en place des ZRR pour limiter l'accès aux espaces de recherche sensibles. Cela est particulièrement utile pour ces établissements d'enseignement et de recherche, traditionnellement ouverts vers l'extérieur, et qui accueillent un grand nombre d'étudiants, de doctorants ou de chercheurs étrangers pas toujours bien intentionnés.

La PPST est **un outil qui fonctionne bien**. Elle a toutefois une limite : il s'agit d'**un dispositif facultatif**. Ce sont les acteurs de terrain, qu'ils soient publics ou privés, qui décident d'y recourir s'ils souhaitent améliorer la protection de leurs

(1) Articles R. 413-1 et suivants du code pénal.

(2) DRSD, « La contre-ingérence dans le monde de la recherche de défense », Lettre d'information économique, n° 11, décembre 2022.

savoirs, savoir-faire et activités sensibles. Or, selon les informations fournies au rapporteur, certaines entreprises et certains laboratoires renoncent à y recourir, notamment en raison des coûts de mise en œuvre.

Compte tenu des menaces qui pèsent sur la BITD, le rapporteur spécial estime qu'**il est nécessaire d'envisager de rendre le cadre de la PPST plus contraignant**, en imposant aux entreprises et organismes de recherche les plus critiques de recourir au dispositif, aujourd'hui facultatif. Il s'agirait, naturellement, de définir un cadre proportionné, tenant compte des risques spécifiques de chaque entité à protéger. En outre, un dispositif d'accompagnement devra être mis en place, avec une prise en charge partielle des coûts incombant à l'entité protégée, sur le modèle du « Diag Cyber ».

Recommandation n° 5 : Rendre le cadre relatif à la protection du potentiel scientifique et technique de la nation plus contraignant, notamment pour les entreprises et les organismes de recherche les plus critiques.

4. Renforcer la coopération entre le secteur public et le secteur privé

Malgré la réorganisation et le renforcement des services de l'État chargés de mettre en œuvre la politique de sécurité économique, la **coopération entre le secteur public et le secteur privé en matière d'intelligence économique demeure perfectible**. En 1994, le rapport Martre regrettait déjà un trop fort cloisonnement des administrations et des entreprises, avec une faible reconnaissance des convergences d'intérêts, des relations souvent teintées de méfiance voire des stratégies non coopératives. Il appelait à développer des agences privées d'intelligence économique, comme il en existe dans d'autres pays, en particulier dans les pays anglo-saxons.

Trente ans plus tard, **une véritable filière de l'intelligence économique privée a émergé** avec, derrière les agences les plus connues – l'ADIT, Avisa Partners (désormais Forward Global), Altum&Co –, une centaine d'acteurs et un chiffre d'affaires global de près de 750 millions d'euros. Ces entreprises privées offrent des prestations de conseil précieuses, notamment en matière de veille stratégique, de développement et d'export ; elles contribuent à la sensibilisation des entreprises aux enjeux de la guerre économique. Le rapporteur spécial se félicite de cette évolution importante pour la défense de nos entreprises et de nos technologies.

Il n'en demeure pas moins que **les synergies entre les services de l'État** chargés de l'intelligence économique **et ces agences privées demeurent faibles** et que la collaboration entre le secteur public et le secteur privé pourrait s'accroître afin de mieux protéger et de mieux soutenir les actifs stratégiques français. Selon le rapport de M. Roux de Bézieux sur la sécurité économique des entreprises, une meilleure collaboration entre les administrations et les acteurs privés pourrait passer par une labélisation de ces derniers.

Le rapporteur spécial note toutefois qu'une telle labélisation, si elle était mise en œuvre par les services de l'État, nécessiterait un cadre juridique, des contrôles, des audits, et donc de mobiliser un certain nombre de moyens, qui ne seraient alors plus affectés à la détection ou l'entrave aux alertes de sécurité économique. Cela n'irait pas non plus dans le sens de la simplification pour les entreprises concernées. Le rapporteur spécial estime que **la structuration de la filière gagnerait à être portée par le secteur privé lui-même**, à l'instar de l'action du Syndicat français de l'intelligence économique (SYNFIE), qui regroupe déjà un certain nombre d'acteurs.

La coopération entre la BITD et le secteur civil pourrait également avoir un intérêt dans le domaine de la lutte anti-drones. En effet, certaines entreprises, notamment les aéroports, disposent de moyens de défense particulièrement avancés, qui gagneraient à être expérimentés et utilisés pour protéger les emprises de l'industrie de défense.

5. Vers une posture plus offensive ?

Au delà du volet défensif de la politique française d'intelligence économique, qui s'est considérablement renforcé, la guerre économique implique également la mise en œuvre de **manœuvres plus offensives**. On ne peut pas se contenter de subir en permanence, il faut dans certains cas être proactifs. En la matière, force est de constater que **nos compétiteurs stratégiques**, ennemis ou alliés, **hésitent moins que nous**. C'est donc **une évolution des mentalités qui doit s'opérer**.

● Si la BITD dispose de groupes industriels solides capables d'exporter des équipements et de remporter des grands contrats internationaux, la France s'est souvent montrée moins organisée que certains de ses concurrents pour réussir dans la compétition internationale. Là où une équipe soudée et coordonnée s'avère nécessaire, nos entreprises et nos administrations ont parfois eu tendance à agir de manière dispersée voire concurrente, fragilisant ainsi le collectif. Nos récents succès internationaux, la France étant désormais le deuxième plus gros exportateur d'armes au monde, semblent indiquer que nous sommes aujourd'hui mieux organisés.

La réorganisation de la DGA va ainsi dans le bon sens. La direction de l'industrie de défense entend renforcer ses actions de promotion à l'étranger des entreprises de la BITD, en lien avec d'autres acteurs ou directions du ministère, notamment la direction internationale de la coopération et de l'export. Cette posture plus offensive, jusqu'à présent faiblement dotée, consisterait notamment à consolider les analyses prospectives portant sur les BITD étrangères ou sur les zones d'intérêt à l'export. La sous-direction de l'intelligence économique pourrait aussi accompagner les entreprises de l'industrie de défense à détecter les technologies critiques à l'étranger et à investir dans des sociétés stratégiques étrangères. Il s'agit ici d'**employer les mêmes moyens que ceux utilisés par nos concurrents étrangers** et de **mieux utiliser l'intelligence économique comme un outil stratégique permettant de saisir des opportunités** et de gagner des parts de marché.

Le rapporteur spécial s'interroge également sur le **rôle de la diplomatie parlementaire**, qui est très **peu valorisée en France**, mais qui l'est beaucoup plus chez certains de nos compétiteurs, avec des actions communes entre les industriels et les élus. Or les parlementaires, qui connaissent les entreprises implantées sur leur territoire, peuvent être des ambassadeurs utiles vis-à-vis d'interlocuteurs étrangers pour soutenir les activités export des petites entreprises de la BITD.

● Par ailleurs, plusieurs des personnes auditionnées par le rapporteur spécial ont souligné **une plus grande participation des services de renseignement étrangers au soutien des intérêts économiques de leur pays**. Le rapport Carayon en faisait lui aussi état : « *on soulignera l'importance – c'est un euphémisme – des services de renseignement dans les pays anglo-saxons et aux États-Unis […]. Des services de renseignement étroitement imbriqués, et sans pudeur aucune, avec les autres administrations publiques et les entreprises, en particulier celles qui ont pour métier de conseiller, d'auditer, d'assurer, d'investir et d'innover…* ».

La stratégie nationale du renseignement intègre certes dans les missions des services de renseignement la promotion des intérêts économiques, industriels et scientifiques du pays : « *[l]e Renseignement, outil de défense de nos intérêts et d'acquisition de connaissances dans les domaines stratégiques, est également un outil de promotion de nos intérêts (politiques, économiques, scientifiques, militaires, culturels, etc…). Il s'agit ici, non seulement de développer, en appui de notre diplomatie, des actions d'influence en direction des structures d'intérêts pour notre pays, mais de capter et d'analyser les données nécessaires à la réalisation de nos objectifs et à la protection de nos intérêts* ».

Toutefois, pour des raisons culturelles, **nous faisons encore preuve d'une retenue que ne connaissent pas tous nos compétiteurs**, et que cela nuit parfois à la circulation de l'information auprès des plus petits acteurs. Nos adversaires n'hésitent pas à en profiter, en attaquant tout en restant sous le seuil au delà duquel les moyens de l'État sont mis en œuvre. Il a par exemple été indiqué au rapporteur spécial qu'aux États-Unis, les entreprises qui candidatent sur des grands appels d'offre obtiennent de droit un accès aux services de l'État, y compris pour les soutenir en matière de renseignement économique et stratégique.

Sans doute le renforcement des moyens budgétaires et humains des services de renseignement contribue-t-il à faire évoluer les choses. Mais il faut aussi, en la matière, moins hésiter à adopter une posture plus offensive. Il conviendrait aussi de renforcer la coordination entre les services de renseignement et les entreprises stratégiques, de façon à mieux cibler les actions de renseignement économique.

● Dans la même perspective, l**a France est encore en retrait dans le domaine de la guerre cognitive**, c'est-à-dire en termes de capacité à produire de la connaissance pour imposer sa propre vision du monde et influencer les modes de pensées de ses alliés comme de ses adversaires. Le rapport Carayon le soulignait en ces termes : « *[l]a défiance – encore si répandue – de nos universités à l'égard du monde de l'entreprise, l'absence jusqu'à présent d'un statut fiscal et administratif*

attractif pour les fondations, ont retardé l'apparition de think-tanks à l'instar de ceux qui, en Allemagne, en Angleterre et surtout aux États-Unis, ont contribué à élaborer la pensée moderne et à enrichir tous les centres de décision publics et privés de leurs travaux. […] Nos faiblesses dans ces domaines sont tragiques : les marchés du conseil, de la certification et de la notation sont totalement dominés par les Américains et les Britanniques, ainsi que toutes les formes et tous les réseaux techniques d'information. Cette hégémonie s'étend aux fonds de pension mais aussi à de nouvelles formes d'influence mises en œuvre par des organisations non gouvernementales (ONG), des sociétés de lobbying, dont l'efficacité dans les instances internationales nous laissent désarmés… Partout où s'élaborent les règles, les normes, voire les modes, nous avons perdu pied. Des sociétés d'intérêt stratégique passent sous le contrôle d'investisseurs avisés ; des technologies étrangères sont retenues pour traiter des informations liées à notre souveraineté ou à la circulation d'informations confidentielles. Sur de nombreux marchés extérieurs, nos entreprises-phares sont soumises à des déstabilisations parfois inimaginables. Ce constat de carence et d'impuissance ou, dans le meilleur des cas, de désordre, est partagé par la quasi-totalité des acteurs publics et privés ».

En la matière, nous agissons de manière encore trop dispersée. Afin d'être plus efficace dans la protection et la promotion de nos intérêts économiques, il conviendrait de mettre en place une stratégie pour coordonner les acteurs publics et privés produisant ou diffusant de la connaissance, y compris de manière indirecte. Par ailleurs, pour contrer l'action d'États étrangers qui se servent de *proxies* pour diffuser en France des informations fausses ou manipulées à des fins de déstabilisation, les obligations sur la transparence des financements étrangers dont bénéficient les organismes dits d'intérêt général, notamment les organisations non gouvernementales, pourraient être renforcées.

C'était là tout le sens du rapport « Comment la France peut-elle rendre plus influent son récit d'elle-même et de ses priorités stratégiques ? » auquel a contribué le rapporteur spécial dans le cadre de son parcours à l'Institut des hautes études de défense nationale (IHEDN), qui soulignait « *la diffusion continue par nos compétiteurs ou adversaires de récits hostiles […] visant à fragiliser notre système politique et notre cohésion nationale* » et la nécessité pour la France d'imposer son récit sur la scène nationale comme à l'extérieur.

Enfin, de façon plus générale, le contexte de guerre économique doit inciter les services de l'État à cartographier non seulement nos actifs stratégiques et nos vulnérabilités, mais aussi les leviers d'action que nous serions en capacité d'actionner en cas de tension avec des États étrangers.

B. LA NÉCESSITÉ DE RENFORCER NOS OUTILS DE SOUVERAINETÉ AUX NIVEAUX NATIONAL ET EUROPÉEN

Outre une augmentation des moyens alloués aux services de l'État chargés de protéger et de soutenir les actifs stratégiques, les enjeux de guerre économiques appellent un renforcement de certains dispositifs au niveau national comme européen.

1. Renforcer les moyens alloués à la politique de sécurité économique

L'ensemble des interlocuteurs auditionnés par le rapporteur spécial se sont accordés pour dire que le **cadre législatif et réglementaire** relatif à la politique de sécurité économique n'appelait **pas de modification** substantielle. Toutefois, compte tenu de l'intensification des menaces, il paraît nécessaire de poursuivre l'**augmentation des moyens humains et budgétaires** alloués aux services chargés de la protection des actifs stratégiques. Le rapporteur note que cela fait partie des propositions mises en avant dans le rapport de M. Geoffroy Roux de Bézieux sur la sécurité économique des entreprises.

Les moyens de la DGA, de la DRSD et de la DGSE ont vocation à augmenter dans le cadre de la **LPM 2024-2030**. Cela **suppose que les crédits de paiement du ministère des armées augmentent conformément à la trajectoire et ne soient pas annulés en fin d'année** pour couvrir des dépenses accidentelles ou imprévisibles. En outre, en cas de révision de la programmation militaire conformément aux annonces du Président de la République dans son discours aux armées du 13 juillet 2025, les services chargés de protéger et de soutenir les entreprises de la BITD devraient également voir leurs moyens augmenter. Par ailleurs, si le SISSÉ ne bénéficie pas de la hausse des crédits prévue dans la LPM, il paraît tout aussi utile de lui affecter **quelques ETP supplémentaires**.

Augmenter les moyens des services de l'État chargés de protéger et de soutenir les actifs stratégiques permettrait à ces services de **renforcer leurs moyens d'action et de s'implanter de façon plus solide dans l'ensemble des territoires**. Ils auraient notamment davantage de marges pour travailler sur certains types de menaces qui, à l'instar des menaces informationnelles, sont encore peu traitées. En outre, une hausse des effectifs à travers la mise à disposition d'agents publics travaillant dans d'autres administrations partenaires pourrait permettre d'**améliorer encore la coordination entre les différents services**. Si les échanges d'informations se sont renforcés en matière d'antiterrorisme, des progrès peuvent encore être faits en matière de sécurité économique.

Recommandation n° 6 : Augmenter les moyens humains et budgétaires alloués aux services de l'État chargés de la protection des actifs stratégiques.

Néanmoins, dans un contexte budgétaire contraint, toute hausse des crédits alloués à la sécurité et à l'intelligence économiques ne pourra se faire dans la durée que si elle est financée. La France étant l'un des pays où le niveau des prélèvements obligatoires est le plus élevé, les marges de manœuvre en recettes sont

nécessairement limitées. Il conviendra donc d'**effectuer des choix courageux en réduisant d'autres pans de la dépense publique**, en privilégiant les missions régaliennes de l'État et **en donnant la priorité aux dépenses d'avenir**. Protéger les actifs stratégiques aujourd'hui, c'est défendre la croissance économique de demain.

2. Mieux contrôler les ressources humaines

Les enjeux de la guerre économique et le maintien à un niveau élevé des menaces d'origine humaine imposent aussi un meilleur contrôle des ressources humaines employées au sein de la BITD.

L'actualité montre combien l'emploi de salariés ou de collaborateurs peu scrupuleux peut conduire à des **fuites de données** à des fins d'espionnage stratégique ou économique. En 2023, un grand groupe français a ainsi détecté un comportement inhabituel de la part d'une personne employée depuis une dizaine d'années. Après une enquête de la direction générale de la sécurité intérieure (DGSI), ce ressortissant étranger, naturalisé français, a été arrêté pour extraction frauduleuse de données sensibles au profit de son pays d'origine. Il est donc nécessaire de **mieux contrôler les ressources humaines** à la fois **à l'entrée**, lors de leur recrutement, et **à la sortie**, au moment où les personnes quittent une entreprise ou un organisme de recherche.

La **DRSD** est l'autorité **chargée de contrôler** si les personnes qui souhaitent travailler dans une entreprise de la BITD n'ont pas un comportement ou des agissements incompatibles avec l'exercice des fonctions ou des missions qu'elles sont appelées à exercer ou qu'elles occupent déjà. La direction n'intervient toutefois que dans un **cadre juridique précis** : soit dans le cadre d'une procédure d'habilitation au secret défense, si l'emploi concerné rentre dans la catégorie des emplois sensibles fixée par la DGA, soit pour une autorisation d'accès à une zone protégée.

Comme il l'avait fait dans son rapport sur l'économie de guerre, **le rapporteur spécial s'interroge sur la compatibilité de ce cadre juridique** dans lequel intervient la DRSD **et la nécessité d'accélérer les cadences de production** et de recruter davantage, plus rapidement et à moindre coût. Si les entreprises de la BITD venaient soudainement à accroître leurs recrutements pour répondre à des demandes urgentes, les nouvelles embauches ne seraient valides qu'après la réalisation des enquêtes administratives, avec un risque d'engorgement des services d'enquête et, par voie de conséquence, d'allongement des délais.

À l'heure actuelle, la DRSD est en mesure de répondre dans un délai d'un à deux mois pour les contrôles primaires et dans un délai de trois à six mois pour les enquêtes relatives à une habilitation « secret » ou « très secret ». Pour faire face à l'augmentation des demandes, le service s'est doté d'outils numériques permettant de **réorganiser**, de **rationaliser** et d'**accélérer le traitement des dossiers**. Ces efforts ont permis d'**accroître le nombre d'enquêtes réalisées chaque année**, avec 436 000 avis de sécurité émis en 2024, dont 45 000 pour l'habilitation de personnes travaillant en entreprise. Néanmoins, les services d'enquête de la DRSD doivent

aussi faire face à une baisse de leurs effectifs (– 10 % entre 2023 et 2024), qui entraîne des retards récurrents dans la délivrance de certains avis.

Il est vital que la DRSD puisse parvenir à maintenir des délais de délivrance des avis de sécurité raisonnables et compatibles avec les enjeux de l'économie de guerre. L'augmentation des menaces appelle nécessairement une augmentation des moyens alloués aux services d'enquête. Il y a donc un réel enjeu d'ajustement des moyens budgétaires et humains de la direction.

En outre, le rapporteur spécial estime nécessaire d'**ouvrir une réflexion** sur la possibilité de réaliser des **enquêtes administratives** et de délivrer des avis de sécurité pour des personnes souhaitant travailler dans la BITD **préalablement à leur recrutement**. Une telle possibilité permettrait de **constituer un vivier** de personnes autorisées ou habilitées dans lequel les entreprises de l'industrie de défense pourraient rapidement trouver la main-d'œuvre dont elles ont besoin, notamment sous forme d'intérim, pour couvrir des besoins de recrutement urgents ou temporaires. Elle permettrait aussi à la réserve industrielle d'accélérer sa montée en puissance. Elle pourrait enfin faciliter les recrutements dans certaines entreprises duales, parfois moins habituées à la nécessité de « cribler » les personnes qu'elles recrutent. Cela supposerait toutefois une hausse des moyens du service à la hauteur de ses nouvelles missions.

Recommandation n° 7 : Renforcer les moyens budgétaires et humains alloués aux services d'enquête de la DRSD, et envisager un nouveau cadre juridique autorisant la constitution d'un vivier de travailleurs autorisés ou habilités à la disposition des entreprises de la BITD en cas de recrutements urgents ou temporaires.

3. Imposer l'utilisation de moyens souverains pour le stockage numérique de données et les outils de messagerie

La question de la cybersécurité se pose de manière encore plus aigüe s'agissant du **stockage numérique de données** et de l'utilisation des **outils de messagerie**. En la matière, la domination sans partage des grandes plateformes numériques génère de fortes externalités négatives et jette un voile d'opacité sur l'utilisation des données sensibles des entreprises de la BITD, soit qu'elles-mêmes les stockent sur des **serveurs situés à l'étranger**, soit qu'elles les confient à des sous-traitants ou des prestataires (banques, fonds d'investissement, cabinets de conseil, cabinets d'audit, cabinets d'avocats, comptables, commissaires aux comptes, etc.) qui les stockent au moyen de solutions étrangères.

Il est du devoir de l'État de protéger les données confidentielles qu'il partage avec les entreprises qui travaillent pour lui, et il est aussi de la responsabilité de ces entreprises de protéger les données dont elles se voient confier la charge. Cela suppose que les données sensibles soient identifiées au sein de chaque entreprise ou organisme de recherche, qu'elles transitent par des outils de télécommunications ou de messagerie sécurisés, qu'elles ne soient plus stockées sur des serveurs situés à l'étranger, sans cloisonnement et sans chiffrage, et qu'elles le

soient sur des serveurs situés en France ou en Europe, soumis à la réglementation européenne et à l'abri d'atteintes étrangères, légales ou illégales.

Le rapporteur spécial tient ici à **faire preuve d'optimisme**. Ceux qui veulent nous faire croire qu'un *cloud* souverain est impossible contribuent, volontairement ou involontairement, à nous laisser dépendants de solutions étrangères. **Nous disposons des ressources technologiques et des compétences humaines nécessaires pour rehausser notre niveau de sécurité**. Une évolution progressive de nos moyens de stockage vers des solutions souveraines et sécurisées est possible. À nous d'en avoir la volonté. Comme pour le renforcement de notre niveau de cybersécurité, cela supposera d'accepter un certain niveau de surcoût. Mais il s'agit bien là d'une condition indispensable à notre pleine souveraineté.

À cet égard, il faut saluer les dispositifs mis en place par l'État, notamment via Bpifrance, pour favoriser le développement d'une filière de stockage des données, qui ont permis à un certain nombre d'hébergeurs français d'émerger. Néanmoins, il convient de souligner que **les acteurs français, qui existent et qui constituent une alternative crédible, ne pourront se développer et acquérir une taille critique que s'ils reçoivent des commandes**. Il est donc de la responsabilité des décideurs publics – y compris les administrations et les décideurs politiques – comme privés de protéger leurs données sensibles en faisant appel à des hébergeurs sécurisés ou à des prestataires de confiance.

Là encore, **un certain degré de contrainte paraît nécessaire**. C'est la réglementation qui imposera aux entreprises, y compris celle de la BITD, d'utiliser des solutions françaises, ou européennes si elles apportent un niveau de sécurité équivalent, et d'éviter de recourir à certains prestataires lorsqu'il existe une incertitude sur la confidentialité des données envoyées ou stockées. Cela contribuera à renforcer notre niveau de protection des données, mais favorisera aussi le développement d'entreprises capables de concurrencer les grandes plateformes étrangères. Sur un marché de plusieurs centaines de milliards d'euros, gagner ne serait-ce que 10 points de parts de marché ferait déjà une différence non négligeable.

Recommandation n° 8 : Imposer progressivement aux entreprises de la BITD un très haut niveau de protection des données, impliquant le stockage de données sensibles sur des serveurs situés en France ou sur le territoire de l'Union européenne.

Sur ce sujet, le rapporteur spécial, estime que, au delà de la seule BITD, l'ensemble des administrations publiques ne peuvent s'affranchir de sécuriser le stockage de leurs données sensibles. À cet égard, il s'interroge que, dans un contexte de guerre économique, le Gouvernement ait, en juin 2025, choisi de retirer la mission de veille stratégique des réseaux sociaux au bénéfice de l'État à l'entreprise française Visibrain – dont la compétence technique et l'expertise étaient saluées par les services utilisateurs – pour la confier à une société canadienne, Talkwalker, soumise au *Cloud Act* et aux lois extraterritoriales des États-Unis.

Il s'étonne, en outre, de l'utilisation d'outils de télécommunication et de messagerie étrangers au plus haut niveau de l'État. Citons, à titre d'exemples, les « boucles » des parlementaires sur Whatsapp ou Telegram – applications interdites dans l'administration américaine –, plutôt que sur Olvid, application 100 % française et sécurité recommandée par les services chargés de la sécurité intérieure. Il s'inquiète aussi du fait que l'Assemblée nationale proposait, sous les XV^{e} et XVI^{e} législatures, des routeurs de la marque Huawei pour fournir l'accès à internet des permanences parlementaires. Si les députés sont rarement détenteurs d'informations classifiées, les informations qu'ils détiennent et échangent n'en sont pas moins valorisables par nos compétiteurs stratégiques. Le rapporteur spécial mesure l'effort que demande un changement d'habitudes logicielles qui sont puissamment ancrées, mais il estime que les élus de la Nation ont un devoir d'exemplarité en la matière.

4. Vers une Europe moins naïve en matière de guerre économique ?

Dans le contexte de résurgence des tensions géopolitiques et d'accentuation de la compétition entre les grandes zones économiques mondiales, la politique de sécurité économique doit être renforcée au niveau national comme au niveau européen. **Longtemps naïve, l'Union européenne semble progressivement prendre conscience de la nécessité de se défendre elle-même**, même si ce virage idéologique et politique, qui ne correspond pas à son ADN, est lent. Elle épouse progressivement la notion de souveraineté économique et technologique, et plusieurs réglementations ou projets de réglementation récents vont ainsi dans le bon sens.

● Sous l'impulsion de la France, l'Union européenne s'est dotée d'outils destinés à **renforcer et harmoniser le contrôle des investissements des étrangers**. Un règlement européen [(1)], entré en vigueur le 11 octobre 2020, a mis en place, pour les opérations d'investissements réalisées par des acteurs extra-européens dans un ou plusieurs États membres de l'Union européenne, un mécanisme d'échange d'informations entre les États et la Commission. Ce dispositif permet aux États de partager leurs analyses des enjeux et des risques que peuvent présenter certains projets d'investissement devant avoir lieu sur le territoire européen.

Ce système comporte **encore des lacunes**, mises en évidence par un rapport de la Cour des comptes européennes de 2023 [(2)]. Les règles mises en place n'imposent pas aux États membres d'instaurer un mécanisme de filtrage et leur laisse toute discrétion pour déterminer l'étendue de leurs règles nationales en la matière. En outre, les États ne sont pas tenus de communiquer à la Commission européenne leurs décisions en matière de filtrage, même si celle-ci a émis un avis ou que d'autres États membres ont fait part de leurs inquiétudes. Ainsi, la Cour relève que, entre 2020 et 2022, seuls six États membres ont notifié 92 % de l'ensemble des dossiers instruits, les 8 % restants l'ayant été par neuf autres. En

(1) Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union.

(2) Cour des comptes européenne, « Filtrage des investissements directs étrangers dans l'UE – Le cadre est en place, mais des limites importantes empêchent une gestion efficace des risques pour la sécurité et l'ordre public », rapport spécial, décembre 2023.

d'autres termes, douze États soit n'ont pas réalisé de filtrage, soit n'ont pas notifié un seul dossier. Or les informations non partagées par un État membre peuvent empêcher d'autres États ou la Commission de repérer les éventuels risques liés à certains investissements étrangers.

Encore récemment, le **double rachat de la *start-up* française Vade** a montré combien la coordination européenne en matière de souveraineté technologique était insuffisante. La société Vade, après des années de bataille judiciaire intentées par le groupe américain Proofpoint pour tenter de freiner son développement aux États-Unis, avait été racheté par l'entreprise allemande Hornetsecurity. Un an plus tard, Hornetsecurity est elle-même rachetée par Proofpoint, emportant Vade avec elle. De fait, les activités de Vade seront désormais soumises au droit américain, avec un risque de perte de contrôle sur les données des clients européens.

Le **contrôle** des investissements étrangers en Europe **doit donc être renforcé**. En 2024, la Commission européenne a initié une révision du règlement européen sur le filtrage des investissements directs étrangers [(1)], afin d'imposer à tous les États de se doter d'un mécanisme de filtrage des investissements étrangers, d'harmoniser les règles nationales pour permettre une coopération avec les autres États et avec la Commission plus efficace, ainsi que d'étendre le champ des contrôles aux opérations initiées par un investisseur établi au sein de l'Union mais contrôlé en dernier ressort par des personnes ou entités d'un pays tiers. Il s'agit là d'un signal positif, pour **renforcer la coordination entre pays** et bâtir une véritable **doctrine commune en matière de souveraineté économique et technologique**.

Néanmoins, selon le rapporteur spécial, l'Union européenne n'est, aujourd'hui, pas prête à de réels transferts de souveraineté en matière de contrôle des investissements étrangers. Aucun transfert de compétences ne doit avoir lieu s'il s'agit uniquement de déconstruire les systèmes souverains dont certains États ont décidé de se doter sans les remplacer par un système souverain européen.

● Par ailleurs, la meilleure manière de contrer certaines normes étrangères à portée extraterritoriale dont se servent certains de nos compétiteurs pour atteindre nos entreprises est d'adopter des réglementations équivalentes pour pouvoir les opposer aux autorités étrangères. À cet égard, le rapporteur spécial estime que la loi de blocage du 26 juillet 1968 précitée a fait ses preuves au niveau national et gagnerait à trouver un cadre équivalent au niveau européen.

Recommandation n° 9 : Sur le modèle de la loi de blocage du 26 juillet 1968, adopter un règlement de blocage au niveau de l'Union européenne.

Dans la même perspective, l'Union européenne pourrait se doter d'une réglementation de type « Itar ». L'*international traffic in arms regulations* (ITAR) est une réglementation américaine qui contrôle la fabrication, la vente et la distribution d'objets et de services liés à la défense et à l'espace. Elle prévoit que

(1) Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union.

l'accès aux matériaux physiques ou aux données techniques liés à la défense et aux technologies militaires est réservé aux citoyens des États-Unis. Les États-Unis s'en servent comme d'un outil protectionniste pour protéger leurs champions nationaux au détriment des autres industriels y compris européens. La création d'un label de type « Itar » au niveau européen permettrait aux États membres de l'Union européenne – qui constitueraient collectivement une masse critique suffisante – de s'opposer à certaines demandes abusives des autorités américaines vis-à-vis de leurs entreprises stratégiques, voire de réaliser des contrôles similaires auprès d'entreprises ou d'investisseurs étrangers.

Recommandation n° 10 : Mettre en place un label de type « Itar » au niveau de l'Union européenne.

Un tel dispositif ne devrait toutefois en aucun cas transférer au niveau européen le contrôle des exportations d'armes et de biens à double usage réalisées par les États membres au profit d'États tiers. Un tel transfert de souveraineté est exclu, tant les divergences d'intérêt entre États membres et les dangers pour la compétitivité de la BITD française sont prégnants.

IV. LES DIFFICULTÉS DE FINANCEMENT DES PETITES ENTREPRISES DE LA BASE INDUSTRIELLE ET TECHNOLOGIE DE DÉFENSE

Les **atteintes capitalistiques** comptent parmi les principales menaces qui pèsent sur les PME de la BITD, qui sont susceptibles de faire l'objet de prédation de la part de concurrents étrangers, avec un risque de **perte de souveraineté sur certaines technologies** et de **déstabilisation des chaînes de valeur** des grands donneurs d'ordre. Leur fragilité structurelle a été confirmée par une étude de l'Observatoire économique de la défense et de la direction générale du Trésor, qui indique qu'elles présentent « *une structure financière et économique plus fragile dans la BITD que dans le reste de l'économie, avec des marges plus faibles, une capacité moindre à créer de la valeur, un endettement plus élevé et une potentielle sous-capitalisation* » (1).

Les **vulnérabilités des entreprises de l'industrie de défense** procèdent de spécificités propres au secteur : cycles industriels longs, dépendance vis-à-vis de la commande publique, contrôle par l'État des investissements à l'entrée et à la sortie, position dans la chaîne de sous-traitance. Elles sont accentuées par les **montées en cadence liées à l'économie de guerre**, qui exigent la constitution de stocks de matières premières et de composants en avance de phase, d'investir dans du nouveau matériel ou des lignes de production supplémentaires et de recruter, avant même que des commandes fermes n'aient été confirmées par les donneurs d'ordre, ce qui met à mal le besoin en fonds de roulement (BFR) des PME dont la trésorerie est la plus fragile. Les commandes engagées par l'État dans le cadre de la LPM peinent encore à « ruisseler » jusqu'aux PME, et certains sous-traitants **manquent** encore **de visibilité** sur leurs commandes au delà de six mois alors que les commandes de l'État aux grands donneurs d'ordre leur assurent plus de visibilité.

Surtout, les PME de la BITD rencontrent des difficultés pour accéder aux financements privés en raison d'une **tendance des établissements bancaires et des fonds d'investissement à tenir compte de critères éthiques** – souvent rassemblés sous le vocable générique de critères environnementaux, sociaux et de gouvernance (ESG) – dans leurs décisions d'investissement, avec une tendance à sur-interpréter les règles pour éviter tout risque réputationnel. La **tentation d'exclure le secteur de la défense des investissements considérés comme durables et légitimes** a en particulier été portée par l'Union européenne. En effet, les institutions européennes, perméables aux *lobbys* extra-européens, ont longtemps fait preuve de **naïveté** sur ces sujets, en refusant de voir, derrière les discours bienpensants contre la guerre et la vente d'armes, les stratégies d'influence menées par nos compétiteurs stratégiques pour favoriser leurs industries de défense au détriment des nôtres.

Depuis 2021, de nombreux rapports parlementaires, à l'Assemblée nationale comme au Sénat, n'ont cessé d'alerter sur ces sujets. Si l'on observe une évolution, très lente, depuis le début de l'agression de l'Ukraine par la Russie, celle-ci tend à s'accélérer depuis l'arrivée de M. Donald Trump à la présidence des États-Unis.

---

(1) Direction générale du Trésor, « Quelle était la situation financière des entreprises de la BITD avant la guerre en Ukraine ? », Trésor-Éco, n° 360, mars 2025.

A. UN DISCOURS DE PLUS EN PLUS FAVORABLE AU FINANCEMENT DU SECTEUR DE LA DÉFENSE

Les discours sur le financement de l'industrie de défense évoluent dans le bon sens. Cela ne résout pas tout, mais il s'agit bel et bien d'une condition préalable à l'amélioration des conditions de financement de la BITD.

1. Un discours réaffirmé au plus haut niveau de l'État

Malgré la mise en place de référents défense au sein des principaux établissements bancaires, d'un médiateur placé auprès de la DGA ou encore de formations organisées par l'Institut des hautes études de défense nationale (IHEDN), la Fédération bancaire française (FBF) et les groupements industriels à l'attention des institutions bancaires et des industriels, les alertes des PME de la BITD ont continué. En réaction, la LPM pour 2024-2030 a fixé un nouveau cap, son rapport annexé prévoyant que « *l'État favorisera la mise en place de mesures visant à orienter l'épargne et les investissements privés vers les entreprises de la BITD, en particulier les petites et moyennes entreprises (PME) et les entreprises de taille intermédiaire (ETI)* » [(1)]. Depuis, **le ministère des armées et le ministère de l'économie et des finances**, sous l'impulsion du ministre des armées, M. Sébastien Lecornu, **ont travaillé conjointement** sur des solutions permettant d'accélérer le développement de la BITD et de faciliter l'accès des PME aux financements privés.

La **conférence sur le financement de l'industrie de la défense**, organisée le **20 mars 2025** à Bercy, a été l'occasion de rapprocher les représentants de la BITD et ceux des établissements bancaires et institutions financières et de réitérer au plus haut niveau un certain nombre de messages forts.

Dès le début de son discours d'ouverture, M. Éric Lombard, ministre de l'économie, des finances et de la souveraineté industrielle et numérique, a rappelé que le contexte géopolitique avait changé et qu'il n'était plus possible de diminuer les financements alloués à notre défense : « *le monde que nous avons connu depuis la chute du mur de Berlin, en 1989, n'est plus. À l'est, la guerre en Ukraine. À l'ouest, le pivot de notre allié américain. C'est toute la géopolitique et toute notre économie qui se trouvent redessinées. […]* ***Les dividendes de la paix sont épuisés*** ».

Surtout, le ministre a tenu à clarifier un malentendu concernant les critères ESG : « *[c]ertains considèrent que le financement de notre défense ne serait pas compatible avec une politique environnementale, sociale et de gouvernance ambitieuse. Cette vision est fausse. […]* ***L'investissement dans le secteur de la défense est un investissement responsable****. Il l'est d'autant plus qu'il protège notre souveraineté et les principes que nous portons : la démocratie, la liberté et le développement durable. […] L'investissement dans la défense est compatible avec l'investissement responsable. Je dirai même : il en est le protecteur* ».

---

(1) 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.

Dans cet esprit, il a appelé à faire évoluer les pratiques, dans le secteur public comme dans le secteur privé : « *[n]ous avons modifié le label ISR (investissement socialement responsable) en ce sens. Et nous sommes aussi intervenus auprès de l'Autorité européenne des marchés financiers, qui a utilement clarifié sa doctrine dans le domaine. J'invite donc l'ensemble des investisseurs privés à faire de même. Je sais qu'ils l'ont déjà fait ou qu'ils sont en train de le faire, pour* ***s'affranchir d'une frilosité qui, en réalité, est dangereuse pour notre démocratie*** ».

Le ministre des armées, M. Sébastien Lecornu, a quant à lui souligné que « ***[p]roduire des armes, ce n'est pas sale***. *Ce n'est pas l'arme le problème, c'est ce qu'on en fait. Il n'y a pas d'armes controversées. Il n'y a que des armes interdites ou des armes autorisées. D'ailleurs, notre modèle est un des plus vertueux au monde. L'exportation d'armes est interdite, par principe. L'exportation d'armes est l'exception. Elle est donc soumise à des régimes d'autorisation très complexes. Les éléments diplomatiques et la question des droits de l'Homme sont déjà intégrés nativement dans le modèle français. […] Que certains établissements bancaires soient conduits à refuser d'accompagner une PME parce qu'elle concourrait de manière directe ou indirecte à l'arme controversée que serait la dissuasion nucléaire française, c'est un non-sens historique. […] Notre dissuasion nucléaire a la doctrine probablement la plus vertueuse de tous les pays dotés : strictement suffisante, défensive. […] Ce n'est ni un problème de directive, ni de loi, c'est un problème culturel* ».

Le rapporteur spécial ne peut que saluer l'engagement du ministre des armées ainsi que du ministre de l'économie et des finances qui, comme leurs prédécesseurs s'étaient élevés contre les projets européens d'exclusion du secteur de la défense de la « taxonomie verte », de la « taxonomie sociale » et de l'« écolabel européen », réaffirment au plus haut niveau la volonté de l'État que la BITD puisse trouver les financements dont elle a besoin pour monter en cadence.

Il tient à préciser que **ces discours ne marquent pas la fin des critères ESG**, qui sont utiles et doivent perdurer, mais au contraire la fin d'une confusion entre, d'une part, les engagements environnementaux, sociaux ou de gouvernance et, d'autre part, l'exclusion du secteur de la défense des investissements considérés comme légitimes, exclusion qui n'est pas inévitable. **La défense est une condition de la durabilité de nos sociétés : il ne peut y avoir de transition écologique ou de garantie des droits et libertés si notre sécurité n'est pas garantie**. Nous avons besoin de sociétés pacifiques pour préserver l'environnement, lutter contre le réchauffement climatique et avoir un développement social harmonieux. Investir dans la défense c'est préserver la paix. Nous ne construisons pas des armes pour nous en servir, mais pour dissuader nos adversaires de nous attaquer. Cela justifie pleinement que les investissements dans la BITD cessent d'être dénigrés.

2. Un changement de paradigme de la part des institutions européennes

Le rapporteur spécial note, avec satisfaction, que les choses évoluent aussi dans le bon sens au niveau européen. De fait, l'Union européenne a été contrainte de réagir depuis le début de l'agression de l'Ukraine par la Russie, en mettant en place des dispositifs de financement de projets de défense et en abandonnant progressivement ses tentatives d'exclusion du secteur de la défense des investissements légitimes.

L'**Union européenne** a **longtemps** été **réticente à financer des projets de défense**, notamment du fait de l'absence de compétence directe de la Commission européenne en la matière, mais aussi d'un contexte géopolitique qui inclinait vers les dividendes de la paix et le parapluie défensif américain. La remontée des tensions au niveau international puis la situation en Ukraine l'ont conduite à évoluer. Depuis 2017, elle subventionne, via le **fonds européen de défense** (FEDEF), des projets de recherche et **développement** dans le domaine de la défense. En 2022, elle a lancé le dispositif EDIRPA pour financer des acquisitions conjointes d'équipements militaires et le mécanisme **ASAP** destiné à soutenir l'augmentation de la production de munitions. Depuis, elle s'emploie à prolonger ces dispositifs en développant des programmes de financement pérennes, notamment avec les programmes **EDIP** et **SAFE**. Si ces dispositifs souffrent encore de nombreux défauts, ils envoient néanmoins **un signal positif pour le financement de la BITD**.

La **doctrine de la Banque européenne d'investissement** (BEI) tend également à évoluer. Le rapporteur spécial avait maintes fois dénoncé l'impossibilité pour la BEI et son bras armé auprès des PME, le Fonds européen d'investissement (FEI), de financer des projets de défense, y compris des projets à double usage à la fois civil et militaire. Invitée par ses actionnaires, les États membres de l'Union européenne, à adapter sa politique de prêt à l'industrie de la défense, la BEI a été autorisée, en 2024, à investir dans des produits à usage principalement militaire, à condition qu'ils n'entraînent pas de risque mortel et qu'ils conservent un certain degré d'application civile. En décembre 2024, le conseil d'administration de la BEI a également approuvé un projet de financement des PME du secteur de la défense en manque de BFR, portant à la fois sur des prêts aux institutions financières soutenant ces entreprises et sur des mécanismes de garantie en cas de défaillance. Le FEI travaille également sur un projet de soutien aux fonds propres des PME de l'industrie de défense. Ces assouplissements doivent ainsi permettre à la BEI de porter ses investissements dans le secteur de la défense à **2 milliards d'euros en 2025**. Les critères de financement de la BITD pourraient en outre être encore élargis à des projets purement militaires, ce qui suppose une majorité qualifiée d'États membres, mais le **changement des pratiques de la BEI et du FEI**, **qui orientent une partie des stratégies d'investissement privées** en Europe, doit être salué.

L'arrivée de M. Donald Trump à la présidence des États-Unis a eu un effet d'accélérateur sur certaines de ces évolutions. En juin 2025, M. Andrius Kubilius, commissaire européen à la défense, a ainsi annoncé la présentation d'un projet de règlement de simplification en matière de défense (« omnibus défense »), pour alléger et clarifier les règles afin de favoriser le développement de la production d'armements. Ce projet de règlement vise notamment à limiter les délais de délivrance d'un permis de construire une usine de défense. Il assouplit aussi les règles de marchés publics, en limitant les procédures les plus lourdes aux plus gros contrats. Enfin, en matière de financement de la BITD, la Commission européenne clarifie enfin le fait que **les investissements dans le secteur de la défense sont compatibles avec les critères ESG**, et que seules les armes interdites par des conventions internationales ratifiées par une majorité d'États membres peuvent être exclues des indices d'investissement durable.

Le rapporteur spécial salue ces avancées, même s'il convient de rester attentif à ce que ces dernières demeurent pérennes : les tendances de fond, aujourd'hui écartées, sont toujours susceptibles de refaire surface. En outre, il estime que la position de la BEI sur la question du financement des entreprises de la BITD est encore largement déconnectée des réalités du terrain et que l'institution dispose d'une marge de progression certaine.

En outre, il estime indispensable de **réserver les financements européens aux matériels européens**, **développés et produits par des entreprises européennes sur le sol européen**. Les équipements financés doivent contenir des composants majoritairement européens – au moins 65 % – et l'autorité de conception doit être européenne, afin qu'ils puissent être utilisés, maintenus en condition opérationnelle et modifiées par les armées sans restriction de la part d'un pays tiers.

Le programme SAFE (*security action for Europe*) de prêts communs semble devoir déroger à la règle, pour permettre des achats rapides destinés à combler des besoins urgents à court terme. Il ne doit toutefois pas en être le cas du programme EDIP (programme européen d'investissement dans la défense), dont l'enveloppe financière, actuellement modeste (1,5 milliard d'euros sur la période 2025-2027), devrait augmenter rapidement pour soutenir l'industrie de défense à long terme. Or, malgré la position ambitieuse adoptée par le Parlement européen en première lecture, le Conseil a introduit des exceptions regrettables, notamment pour les munitions, y compris les munitions complexes et à haute valeur technologique que sont les missiles.

Le rapporteur spécial estime, en vue de la suite des négociations, que les dérogations doivent être limitées au strict nécessaire. Les exemples de matériels sur lesquels les Européens sont soumis à des dépendances ne manquent pas. Pas plus tard qu'en 2022, Israël avait bloqué temporairement la livraison par l'Estonie à l'Ukraine de missiles antichar Spike, produits par le groupe allemand Diehl, et qui contiennent des composants israéliens. Comment les armées européennes peuvent-elles espérer se défendre si les armements qu'elles utilisent peuvent être bloqués ou soumis à l'autorisation de pays tiers ? Comment la BITD européenne pourrait-elle

se développer, si même les financements européens dont elle devrait bénéficier vont à ses concurrents étrangers ?

Recommandation n° 11 : Dans le cadre du programme européen d'investissement dans la défense (EDIP), réserver les financements européens aux matériels européens – composés d'au moins 65 % de pièces développées et produites par des entreprises européennes sur le sol européen – et dont l'autorité de conception est européenne, en limitant les exceptions.

B. DES ENGAGEMENTS QUI PEINENT ENCORE À SE MATÉRIALISER POUR LES PETITES ET LES MOYENNES ENTREPRISES

Si le 20 mars 2025 était une étape importante, il ne constitue toutefois que le début d'un chantier de long terme. En effet, les discours peinent parfois à se matérialiser par des actes, notamment pour les PME. La plupart des dirigeants d'entreprise auditionnés par le rapporteur spécial lui ont confirmé rencontrer des difficultés à financer leur BFR à court terme, à renforcer leurs fonds propres pour se développer et à se faire accompagner sur les marchés export.

1. Le secteur bancaire tend à clarifier ses engagements en faveur de l'industrie de défense

Le discours politique semble de plus en plus entendu et compris par les établissements bancaires et les institutions financières, même si toutes les difficultés ne sont pas réglées.

Le **secteur bancaire**, par la voie de la Fédération bancaire française (FBF) [(1)], s'est récemment affirmé **prêt à monter en puissance dans le financement de l'industrie de défense** : « *[l]es banques françaises réaffirment leur soutien à l'industrie de défense française […] et sont pleinement mobilisées pour financer les besoins attendus du secteur. Elles sont prêtes à un dialogue de place avec l'industrie, les acteurs financiers, et les pouvoirs publics, pour continuer à renforcer collectivement l'effort national, et échanger sur les pistes de renforcement de la structure financière des entreprises de défense* ».

La FBF a également tenu à clarifier sa position sur les critères ESG : « *[l]es banques rappellent régulièrement qu'il convient d'éviter les signaux qui considéreraient le secteur de la défense comme une activité problématique en soi ou nocive (taxonomie verte et taxonomie sociale, approches des notations ESG, cadre du devoir de vigilance…).* ***Les politiques sectorielles des six principales banques n'excluent pas l'industrie de la Défense des secteurs financés****. Chacune examine de façon continue les formulations de ces politiques pour lever toute éventuelle ambiguïté ou imprécision. Ce même travail de transparence devrait être fait par les constructeurs d'indice, par les gestionnaires d'actifs, plus globalement par les investisseurs. Cette transparence est nécessaire pour que le financement des*

(1) Fédération bancaire française, « Les banques françaises prêtes pour la montée en puissance du financement de l'industrie de la défense », communiqué de presse, 18 mars 2025.

fonds propres de l'industrie de défense soit mieux accessible aux investisseurs institutionnels et particuliers ».

La FBF a également mis en avant le montant actuel des financements consentis aux entreprises du secteur de la défense : « *les six plus grandes banques françaises soutiennent les entreprises de défense à hauteur de 37 milliards d'euros, avec une hausse importante depuis 2021. Cet accompagnement montre la capacité des banques françaises à accompagner l'effort pour la défense, avant et après la montée en puissance liée à l'invasion de l'Ukraine par la Russie en 2022. Selon cette estimation, les banques françaises financent près de deux fois plus la base industrielle et technologique de défense (BITD) que son poids statistique dans l'économie. L'engagement des banques françaises en soutien de l'industrie de Défense va au delà des prêts, cautions ou lignes de crédit aux entreprises : elles financent aussi l'acquisition des matériels français exportés, avec au moins 12 milliards d'euros de prêts aux clients et partenaires des industriels français. Aucun grand projet d'exportation français n'a été financé sans le soutien d'une banque française* ».

Ce **positionnement favorable au financement de la BITD** a été **répété** lors de la conférence du 20 mars 2025 par les différents représentants des établissements bancaires :

– M. Nicolas Namias, président du directoire de BPCE, a tenu à « *affirmer et réaffirmer l'engagement des banques français en faveur du financement de la BITD. […] S'agissant du financement bancaire, notre politique de crédit est simple :* ***on accompagne tout ce qui n'est pas interdit****. Et s'il y a matière à revoir et à clarifier les politiques de crédit, nous le ferons. […] Nous avons mis en place des référents défense.* ***Le moment doit nous conduire à faire davantage****. Les besoins vont être plus importants, les commandes vont augmenter, il est probable que les exportations augmentent aussi. Cela va générer des besoins de trésorerie chez les PME et ETI. On va l'accompagner de différentes manières* » [(1)] ;

– M. Renaud Dumora, directeur général adjoint de BNP Paribas, a ajouté : « ***[i]l faut qu'on accélère. Il y a des besoins. Il y a aussi de la demande de la part de nos clients****. Il faut que dans tous les compartiments – assurance, gestion d'actifs, banque privée – on accélère. On va lancer de nouveaux fonds, créer des mandats spécifiques pour la défense : deux nouveaux fonds côté gestion d'actifs, et doublement de nos engagements côté assurance. […]* ***Nous avons besoin d'aide pour flécher les fonds****. Je suis demandeur d'une nouvelle initiative, sur le modèle de l'initiative Tibi, qui serait spécifique à la défense et à la souveraineté, validée par la DGA, qui permettrait de savoir si tel ou tel fonds agit dans le bon sens. Ce serait un soutien pour le marché et une aide pour les gestionnaires d'actifs. On va également élargir l'univers d'investissement. Il faut le faire au niveau européen. Au*

(1) Commission des finances, d'après les propos tenus lors de la conférence sur le financement de l'industrie de la défense, organisée le 20 mars 2025 au ministère de l'économie et des finances.

niveau français, ce n'est pas suffisant. Il faut avoir de l'ambition. Et il faut le faire sur plusieurs classes d'actifs, l'equity, la dette » [(1)].

Ces discours doivent toutefois **être nuancés sur plusieurs points**. D'une part, les engagements actuellement détenus par les banques dans le secteur de la défense se concentrent très majoritairement sur les grands groupes de la BITD, qui n'ont par définition pas de difficulté à se financer. Les problèmes soulevés par l'industrie de défense comme par les parlementaires concernent bien les PME et les ETI.

En outre, la bonne volonté affichée des banques pour soutenir les industriels de la BITD souffre d'un **« ruissellement » aléatoire des décisions des sièges vers le niveau opérationnel local**. Il en découle des décisions de refus de dossiers justifiés sur le seul terme « défense », alors même que les produits de la société concernée ne sont en aucun cas létaux. Il est fréquent que ces refus ne soient exprimés qu'oralement, et aillent à l'encontre des politiques sectorielles des banques, dont la plupart n'excluent pas la défense de leurs activités. Bien que les grandes banques soient engagées dans le financement de la BITD, il est important que cet engagement se diffuse dans l'ensemble des réseaux, pour que toutes les PME, dans l'ensemble de nos territoires, soient financées à la hauteur de leurs besoins.

2. Un certain nombre de PME ont encore récemment rencontré des refus de financement en raison de leur appartenance au secteur de la défense

Preuve que certaines difficultés demeurent, **un certain nombre de dirigeants de PME entendus par le rapporteur spécial ont rencontré, au cours de l'année écoulée, des refus de financement de la part d'un établissement bancaire ou d'un fonds** (refus d'un prêt ou d'une garantie bancaire, refus de participer à une levée de fonds, clôture de compte bancaire, etc.). Tous les grands acteurs de l'écosystème bancaire et financier, y compris certains ayant contribué à la conférence du 20 mars 2025, sont concernés.

Les difficultés les plus répandues concernent des **entreprises ayant une forte activité à l'export** qui font face à des refus de financement, y compris sur des équipements non spécifiquement militaires. Les réticences, rarement explicitement justifiées, consistent le plus souvent en un refus d'offrir des garanties bancaires au fournisseur alors qu'il s'agit souvent d'une exigence du client final, de gérer des flux de paiement de clients étrangers ou d'accompagner une entreprise pour certaines zones géographiques pourtant prisées par les investisseurs d'autres secteurs économiques (Moyen-Orient, Amérique du sud), malgré des licences d'exportation validées et marquées du sceau de l'État.

Cette situation est **préjudiciable pour les entreprises de la BITD face à la concurrence internationale**. Elle porte atteinte aux relations commerciales des

(1) Commission des finances, d'après les propos tenus lors de la conférence sur le financement de l'industrie de la défense, organisée le 20 mars 2025 au ministère de l'économie et des finances.

PME avec des pays qui sont des clients solvables et importent tout ou partie de leurs équipements de défense. Les refus d'accompagner les industriels français peuvent avoir pour conséquence de priver des acteurs essentiels de l'écosystème de défense des petits contrats qui sont essentiels à leur modèle économique. En outre, ils n'empêchent en rien ces pays d'importer ce dont ils ont besoin auprès d'autres industriels, soutenus par des banques moins frileuses bien que soumises aux mêmes règles prudentielles.

Le **cas d'une PME spécialisée dans la dépollution de matériels pyrotechniques** mérite d'être mis en avant. Cette PME, qui était engagée depuis 2016 avec un État du Moyen-Orient pour des prestations de destruction de stocks de munitions obsolètes, s'est vu attribuer un nouveau contrat avec ce même État en septembre 2024. Une fois la licence export délivrée par l'État, et après avoir obtenu le soutien de Bpifrance, l'entreprise a sollicité sa banque pour obtenir une garantie bancaire. Elle échangeait alors de manière fluide avec cette banque, qui a confirmé, oralement, sa volonté de garantir le projet, ce qui a conduit l'entreprise à ne plus solliciter d'autres banques. Fin octobre 2024, tandis que l'entreprise était sur le point de signer son contrat, **le service *compliance* de la banque lui a subitement opposé un refus de financement**, sans en expliciter formellement le motif. Quelques jours plus tard, la carte bleue de l'entreprise et son accès en ligne à ses comptes ont été fermés, et la **banque a annoncé à l'entreprise la clôture de l'ensemble de ses comptes sous trois mois**. Si l'entreprise, avec le soutien de la DGA et de Bpifrance, a pu trouver une solution alternative, les décisions, inexpliquées, soudaines et brutales de sa banque l'ont mise en grande difficulté.

Par ailleurs, **les fonds et les banques sont encore très réticents à monter dans le capital des entreprises de défense**. La presse s'est récemment fait l'écho d'une entreprise spécialisée dans la production de drones en pleine croissance, finalement délaissée par un fonds au motif qu'elle produit des munitions télé-opérées, lesquelles sont pourtant destinées à protéger les armées ukrainiennes contre les assauts des armées russes. De la même manière, le rapporteur a auditionné une PME spécialisée dans les équipements électroacoustiques pour les secteurs civils et militaires, qui n'a aucune difficulté à lever de la dette auprès des banques mais s'est récemment vu opposer de nombreux refus de participer à un tour de table.

Ces difficultés trouvent leur origine dans le **sentiment qu'ont les acteurs du secteur bancaire que leur intervention dans le secteur de la défense, si elle est visible, va affecter leur réputation**. C'est ainsi qu'une banque accepte de financer la dette bancaire d'une PME membre de la BITD, ce qui lui permet de rester anonyme, mais refuse une opération destinée à renforcer ses fonds propres, qui peut être connue du grand public.

On observe aussi des **difficultés dans les relations entre certaines entreprises de la BITD et leurs compagnies d'assurance**, avec une remontée du coût des cotisations d'assurance pour couvrir les programmes militaires. Le rapporteur spécial a ainsi eu connaissance du cas d'une PME fabriquant du matériel pour les armées et les forces de l'ordre qui, en raison de ses activités dans le secteur

de la défense, doit faire face à une augmentation déraisonnable et injustifiée de sa cotisation à une assurance multirisques industrielle (+ 250 % en six ans), et qui subit en outre une hausse du coût de son assurance responsabilité civile de 20 % en 2025.

Un autre dirigeant d'entreprises de la BITD entendu par le rapporteur spécial lui a indiqué avoir dû faire face à des fonds français qui lui demandaient explicitement de cesser ses activités dans le domaine de la défense dans la mesure où ces dernières allaient compliquer le passage de son dossier devant leur comité compliance. Ce même dirigeant n'a toutefois eu aucun mal à lever près de 200 millions d'euros en à peine deux mois auprès de fonds étrangers.

Ces exemples montrent que **les politiques de crédit portées par les banques et leurs dirigeants ne sont pas toujours comprises et appliquées au sein des réseaux bancaires locaux**. Certains conseillers, peu acculturés aux enjeux industriels et de la défense, peuvent encore faire preuve de frilosité par peur de voir la réputation de leur établissement entachée. Bien sûr, la FBF continue d'arguer du faible nombre de cas de refus de financement qui remontent auprès des centrales bancaires, des médiateurs ou des référents défense.

Il convient néanmoins de souligner que les dossiers refusés ne sont que la partie émergée de l'iceberg. Dans certains cas, le refus est opposé oralement, sans qu'un dossier soit constitué, et sans que le dossier ait à être refusé. En outre, les PME qui se voient opposer un refus de financement n'ont ni l'intérêt ni le temps de faire remonter leur dossier. Elles sont contraintes de garder de bonnes relations avec les banques, dont elles ne peuvent se passer. Et, au moment d'un refus de financement, elles ont intérêt à concentrer leurs efforts sur des solutions de financement alternatives pour tenter de sauver leur projet.

Par ailleurs, la décision d'Euronext, en novembre 2024, d'exclure les entreprises Thalès, Safran et Airbus de l'indice « CAC 40 ESG » était non seulement incompréhensible mais surtout déconnectée du contexte géopolitique. Si la société a été contrainte de revenir sur sa décision, cet épisode n'en est pas moins révélateur du manque grave « d'esprit de défense » dans certains milieux financiers.

Il faut donc saluer les engagements pris par les établissements bancaires et les fonds d'investissement, tout **en restant attentifs à ce que les choses s'améliorent sur le terrain**, au contact des PME de la BITD qui sont indispensables à notre défense et à notre autonomie stratégique.

C. FACE AUX TENTATIVES DE PRÉDATION, LA NÉCÉSSITÉ DE TROUVER DE NOUVELLES SOURCES DE FINANCEMENT PUBLIQUES ET PRIVÉES

Remédier aux difficultés de financement des entreprises de la BITD passe avant tout par **une meilleure mobilisation des fonds privés**. Les fonds publics, au delà de la commande publique, ne doivent intervenir qu'en dernier recours, pour répondre à des défaillances de marché, notamment lorsqu'un investissement est particulièrement à risque.

1. Le renforcement des fonds d'investissement visant à protéger les entreprises et les technologies stratégiques ou innovantes

Face aux menaces capitalistiques et aux tentatives de prédation étrangère vis-à-vis des entreprises critiques ou des innovations de rupture innovantes, **le contrôle des investissements étrangers en France ne suffit pas**. L'État ne peut se contenter d'encadrer ou de bloquer les opérations d'investissement étrangères portant atteinte aux intérêts nationaux. Encore faut-il qu'il puisse offrir des voies de recours aux investisseurs désireux de sortir de leur investissement et aux entreprises souhaitant poursuivre leur développement. Or l'État ne dispose aujourd'hui que de peu de moyens budgétaires pour soutenir les entreprises stratégiques ou innovantes.

Dans le secteur de la défense, l'État s'est doté de fonds d'investissement spécifiques pour soutenir ses entreprises stratégiques, dont la gestion est confiée à la direction générale de l'armement et à Bpifrance. Trois fonds sont financés par le programme 144 de la mission *Défense* :

– le **fonds *Definvest***, créé en 2018, est destiné à soutenir les PME stratégiques pour la défense au moyen de prises de participation minoritaires, notamment pour éviter les tentatives de prédation étrangères. Doté de 100 millions d'euros [(1)], ce fonds a consommé plus de la moitié de son enveloppe et investi dans une vingtaine d'entreprises, avec des tickets de 0,5 à 5 millions d'euros ;

– le **fonds pour l'*innovation de défense***, créé en 2021, a vocation à prendre des participations dans des entreprises innovantes développant des technologies duales et transverses intéressant la défense. Doté de 200 millions d'euros, et pouvant investir jusqu'à 20 millions d'euros par opération, il investit entre 20 millions et 35 millions d'euros par an et est entré au capital d'une dizaine d'entreprises ;

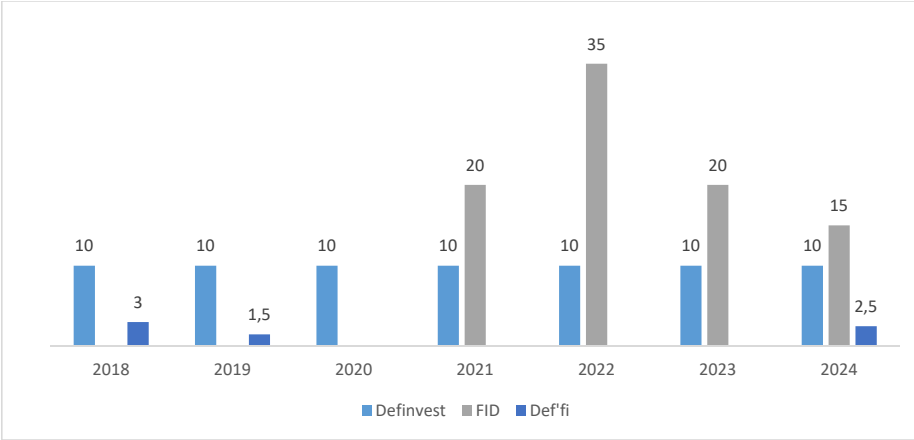
– le **fonds *Def'fi*** est destiné à financer le développement et la transmission de PME stratégiques en phase de croissance. Il propose des prêts participatifs allant de 300 000 euros à 1 million d'euros aux PME stratégiques. Inutilisée entre 2020 et 2023, cette dotation retrouve un intérêt dans un contexte de remontée des taux d'intérêt et de fin des prêts garantis par l'État.

---

(1) Initialement fixée à 50 millions d'euros, en 2018, la dotation du fonds a été augmentée à 100 millions d'euros en 2022.

ÉVOLUTION DES DÉPENSES AU TITRE DES FONDS FINANCÉS PAR LA MISSION *DÉFENSE*

(en millions d'euros)



Source : commission des finances d'après les notes d'analyse de l'exécution budgétaire de la mission Défense *de la Cour des comptes.*

En complément des fonds de soutien à l'innovation de défense, le SISSÉ, notamment, s'appuie sur le **fonds *French tech souveraineté***, qui permet à l'État de prendre des participations dans une entreprise pour éviter qu'elle ne tombe sous le contrôle d'investisseurs étrangers. Doté de 650 millions d'euros au sortir de la crise du covid, et réabondé de 200 millions d'euros en 2025, il a réalisé une dizaine d'opérations depuis 2020.

Ces fonds sont indispensables pour soutenir les PME et les *start-ups* de la BITD. Ils **utilisent l'effet de levier pour mobiliser des investisseurs privés** qui, sans une intervention de l'État, n'auraient pas apporté de soutien financier. Un rapport de la Cour des comptes de 2023 (1) a ainsi montré que les opérations réalisées par le fonds Definvest ont un effet d'entraînement moyen de 4, avec un écart-type de 3,2. En outre, l'investissement de Definvest, pour les entreprises bénéficiaires, améliore la fluidité de leurs relations avec la DGA et leur confère un poids accru dans leur rapport de force avec les grands donneurs d'ordre industriels.

Ainsi que le rapporteur spécial l'avait indiqué dans son rapport sur l'économie de guerre, **les fonds existant sont toutefois insuffisants à deux titres**. D'une part, leur dotation est limitée et le nombre d'opérations réalisées chaque année est faible. D'autre part, ils comblent une partie des lacunes de la chaîne de capital-investissement mais ne couvrent qu'une partie de la série A et de la série B (2). Au delà des levées de 20 millions à 50 millions d'euros, nos entreprises sont trop souvent portées à se tourner vers des fonds anglo-saxons, voire vers des fonds des États du Golfe. Cela constitue un réel frein pour les opérations de

(1) Cour des comptes, « Le fonds Definvest – Exercices 2018 à 2022 », Observations définitives, délibéré le 13 juillet 2023.

(2) La série A est constituée des levées de fonds de quelques millions d'euros, tandis que la série B concerne des levées d'un montant de plusieurs dizaines de millions d'euros.

consolidation de certains sous-secteurs de la BITD, qui peuvent nécessiter des levées de fonds d'une ou de plusieurs centaines de millions d'euros. Le rapporteur spécial note que ce constat est partagé par le rapport de M. Geoffroy Roux de Bézieux sur la sécurité économique des entreprises, qui estime que « *l'absence de fonds de capital-risque de très grande taille en France et en Europe oblige à faire appel à des capitaux extra-européens* ».

Les grands groupes industriels, y compris ceux de la BITD, ont quant à eux leurs propres stratégies d'investissement ou de rachat d'entreprises innovantes, pas toujours compatibles avec celle de l'État.

Quant aux **fonds d'investissement privés**, la France ne dispose, en comparaison de ses homologues étrangers, que de peu de fonds à la hauteur de ses ambitions, même si des solutions ont émergé dans la période récente pour soutenir l'industrie de défense. Il faut ici saluer les fonds Ace Aéro Partenaires et Brienne de Tikehau Capital ainsi que le fonds Eirené de Weinberg Capital Partners – fonds dans lesquels se sont impliqués Bpifrance ainsi que la Caisse des dépôts et consignations – mais aussi le réseau *Defense Angels* et le nouveau fonds défense de la société ISALT.

Le rapporteur spécial appelle donc une nouvelle fois à **augmenter les moyens budgétaires alloués par l'État à la protection des entreprises stratégiques et des technologies sensibles**, de façon à maximiser les effets de levier qu'il est possible d'obtenir en associant des fonds publics et des fonds d'investissement privés. Compte tenu du contexte budgétaire actuel, une telle augmentation de moyens nécessiterait naturellement **des économies sur d'autres pans moins stratégiques de la dépense publique**. Rappelons néanmoins que tout euro supplémentaire dépensé en la matière ne le serait pas à pure perte mais engendrerait un certain nombre de retombées économiques (emploi, recettes fiscales, cotisations sociales), contribuerait à **préserver notre souveraineté** ainsi que notre **croissance économique à moyen et long terme**.

Recommandation n° 12 : Renforcer les moyens budgétaires alloués aux fonds publics destinés à la protection des entreprises stratégiques et des technologies sensibles (notamment Definvest et le fonds pour l'innovation de défense).

Les **annonces** présentées par le Gouvernement lors de la conférence sur le financement de l'industrie de la défense **du 20 mars 2025** constituent **un premier pas dans la bonne direction**, avec :

– **un soutien accru de Bpifrance et de la Caisse des dépôts et consignations**, qui mobiliseront 1,7 milliard d'euros en capital, avec l'objectif d'atteindre jusqu'à 5 milliards d'euros de fonds propres grâce aux co-investissements privés ;

– la prolongation de la durée de vie du fonds Definvest de vingt à trente ans, afin de mieux accompagner les PME et ETI stratégiques ;

– un réabondement du fonds Innovation défense à hauteur de 75 millions d'euros, financés par Bpifrance, par la Caisse des dépôts et consignations ainsi que par des investisseurs privés (notamment l'assureur Allianz), portant le volume du fonds à 275 millions d'euros.

Le rapporteur spécial estime par ailleurs que **le rôle de l'Agence des participations de l'État** (APE) **dans la protection des entreprises et des technologies stratégiques pourrait être renforcé**. À l'heure actuelle, l'APE se concentre sur les objets les plus volumineux, avec de gros montants et peu d'opérations réalisées par an [(1)]. Ses moyens d'action pourraient être étendus pour garantir le maintien sur le territoire d'activités consubstantielles à notre défense et à notre souveraineté. Pour cela, le produit des dividendes perçus par l'État, qui est aujourd'hui affecté au budget général de l'État, pourrait être affecté au compte d'affectation spéciale (CAS) *Participations financières de l'État*, en complément des produits de cession et dotations budgétaires spécifiques dont il bénéficie. Ces 2 à 3 milliards d'euros annuels pourraient conférer à l'APE une possibilité d'intervention contra-cyclique dont elle est en grande partie dépourvue. Le solde du CAS devant rester positif en permanence, l'APE doit nécessairement vendre pour pouvoir acheter ; or les périodes de crise, qui créent des vulnérabilités pour certaines entreprises stratégiques et donc des opportunités de rachat, sont souvent les pires périodes pour vendre, d'où le besoin de trouver des ressources complémentaires, régulières et moins cycliques. Le rapporteur spécial note que cette proposition faite de longue date par l'APE, également reprise dans un récent rapport du Comité d'évaluation et de contrôle [(2)], pourrait faire l'objet d'un accord transpartisan.

Recommandation n° 13 : Pour accroître le rôle de l'Agence des participations de l'État dans la protection des entreprises stratégiques, affecter le produit des dividendes perçus par l'État au compte d'affectation spéciale *Participations financières de l'État*.

2. L'impérative nécessité d'orienter l'épargne des Français vers la défense et les secteurs de souveraineté

En complément des financements de l'État et des fonds d'investissement spécialisés dans la défense, le rapporteur spécial est convaincu que l'épargne des Français peut être mise à contribution pour financer les PME de la BITD.

Fort d'un taux d'épargne particulièrement élevé (17,7 %), **la France dispose d'un volume d'épargne important**, avec un patrimoine financier des particuliers estimé à 6 412 milliards d'euros, dont 953 milliards d'euros pour l'épargne réglementée (livret A, livret de développement durable et solidaire, livret

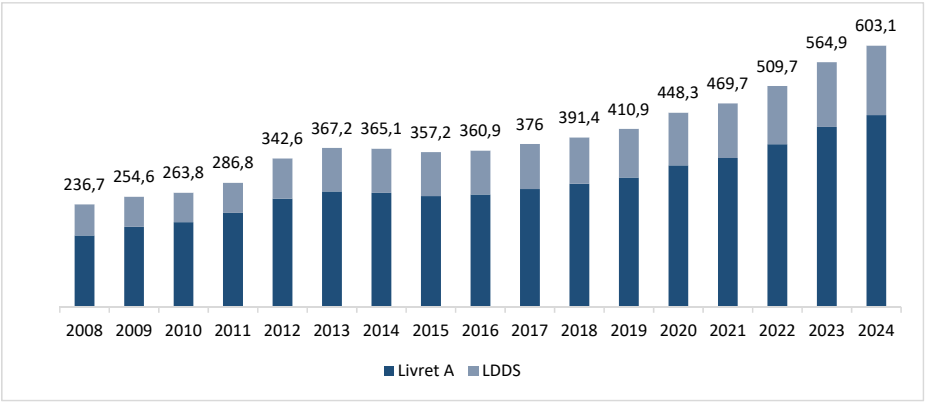
(1) En 2024, l'APE a acquis 80 % du capital de la société Alcatel Submarine Networks, a porté sa part au capital de la société Orano à 90,33 % et a acquis 10 % de la société belge John Cockerill Defense lors du rachat de l'industriel Arquus. Plus récemment, l'APE a acquis l'activité des supercalculateurs d'Atos, tandis qu'un renforcement des parts de l'État au capital d'Eutelsat est envisagé.

(2) Assemblée nationale, rapport d'information n° 1453 (XVII^e législature), de MM. François Jolivet et Hervé de Lépinau, au nom du Comité d'évaluation et de contrôle des politiques publiques, sur l'évaluation du contrôle des investissements étrangers en France, enregistré à la présidence le 22 mai 2025.

d'épargne solidaire, plan épargne logement) [1]. Les derniers chiffres publiés par la Caisse des dépôts et consignations [2] confirment que la collecte sur le livret A et le livret de développement durable et solidaire se ralentit, mais que le stock d'encours demeure massif, avec 603 milliards d'euros à la fin de l'année 2024. Entre 2023 et 2024, ce stock a encore augmenté de 38,2 milliards d'euros.

ÉVOLUTION DE L'ENCOURS DU LIVRET A ET DU LIVRET DE DÉVELOPPEMENT DURABLE ET SOLIDAIRE

(en milliards d'euros)



Source : commission des finances d'après les données de la Caisse des dépôts et consignations.

Seule une partie de cette épargne profite à l'économie réelle. En effet, seuls 60 % des encours du livret A et du livret de développement durable et solidaire sont centralisés dans le fonds d'épargne de la Caisse des dépôts et consignations et utilisés par la Caisse pour financer le logement social, la politique de la ville et des projets d'infrastructures locales [3]. Les 40 % restants demeurent au sein des établissements bancaires qui les collectent, pour financer des PME (80 %), la transition énergétique (10 %) et l'économie sociale et solidaire (5 %).

Évidemment, l'État ne fera jamais main basse sur l'épargne des Français, qui doivent en disposer librement. Il est toutefois du devoir de l'État d'orienter autant que possible cette épargne vers des dépenses d'avenir, utiles au pays et aux générations futures, parmi lesquelles la protection des entreprises stratégiques et des technologies sensibles, plutôt que les laisser à la quasi-discrétion des établissements bancaires qui peuvent encore les placer presque sans contrôle. Il convient en outre de rappeler que les solutions proposées ne visent pas à faire participer l'épargne des Français aux dépenses de l'État, mais bien de l'orienter vers les entreprises qui en ont besoin.

---

(1) Banque de France, « Épargne et patrimoine financiers des ménages – quatrième trimestre 2024 », Stat info, 14 février 2025.

(2) Caisse des dépôts et consignations, « Épargne réglementée : collecte mensuelle en avril 2025 du Livret A et du LDDS ainsi que du LEP », communiqué de presse, 22 mai 2025.

(3) Environ 30 % des ressources centralisées sont placées par la Caisse des dépôts et consignations, notamment pour garantir la liquidité des livrets réglementés en cas de retrait des épargnants.

a. La mise en place de fonds d'investissement ouverts aux particuliers

Si les difficultés d'accès au crédit demeurent, des avancées s'opèrent sur le renforcement des fonds propres des entreprises de la BITD. Le 20 mars 2025, le Gouvernement a annoncé le lancement d'**un nouveau fonds de *private equity* accessible aux particuliers souhaitant investir dans le secteur de la défense**, avec un ticket de souscription minimal de seulement 500 euros. Ce fonds *retail*, qui doit être mis en place par Bpifrance, vise une taille cible de 450 millions d'euros, soit pour investir directement dans des entreprises de la BITD, soit pour investir au sein de fonds spécialisés dans le domaine de la défense.

Le rapporteur spécial salue évidemment la mise en place de ce fonds, solution soutenue par le ministère de l'économie et des finances pour mobiliser l'épargne privée au service de l'industrie de défense. Il note toutefois que le calendrier très rapide initialement évoqué ne sera pas tenu, avec une mise en place au plus tôt en fin d'année. Il souligne également qu'un fonds de *private equity* s'adresse à des investisseurs expérimentés disposant d'un certain volume d'épargne, d'une appétence au risque et d'un horizon d'investissement d'au moins cinq ans, donc à un public moins large que l'épargne réglementée. Par ailleurs, un tel fonds permettrait de renforcer les fonds propres des PME, mais pas leur BFR.

La société Tikehau Capital a aussi annoncé la mise en place d'un autre fonds retail spécialisé dans la défense et ouvert aux particuliers, dont le lancement est prévu en septembre. La multiplication des fonds défense est un signal positif envoyé aux investisseurs désireux de s'engager dans des projets de souveraineté.

Par ailleurs, le rapporteur spécial tient à **saluer les initiatives organisées par la direction générale de l'armement pour rapprocher le monde de la défense des institutions financières** et pour mettre en relation les offres de capitaux proposées par les fonds d'investissement avec les besoins de financement exprimés par les PME et ETI de la BITD. Le 23 juin 2025, pas moins de 80 fonds de *private equity* ont ainsi accepté de signer une charte dans laquelle ils s'engagent à investir de façon durable dans les entreprises de la défense sur le long terme et à ne pas mettre en place des structures de financement qui viendraient empêcher leur développement ou contraindre leur trésorerie. En contrepartie, la charte engage également l'État à garantir un cadre d'investissement stable, transparent et lisible.

Le rapporteur spécial regrette toutefois que les parlementaires demeurent peu associés aux initiatives prises par le Gouvernement sur les enjeux de financement de la BITD. Les nombreux travaux parlementaires réalisés sur le sujet ces dernières années constituent pourtant une expertise qu'il pourrait utile de capitaliser dans ces moments de mobilisation collective.

b. Le fléchage de l'épargne réglementée vers les PME de l'industrie de défense

Compte tenu du volume d'épargne disponible et de sa croissance dynamique, **il semble également pertinent d'orienter une partie des encours des livrets réglementés vers les PME de la BITD, notamment pour leurs besoins de trésorerie de court terme**. En cohérence avec ses recommandations passées et les propositions de loi discutées sur le sujet à l'Assemblée nationale comme au Sénat, le rapporteur spécial réitère donc sa proposition de créer un livret défense et souveraineté ou de flécher une partie des encours des livrets réglementés vers les PME de la BITD.

Un tel fléchage ne permettrait pas de résoudre toutes les difficultés rencontrées par l'industrie de défense. Néanmoins, en s'adressant à un public beaucoup plus large qu'un fonds de *private equity*, il aurait **une portée symbolique** plus forte. Il monterait la détermination de l'État à protéger ses intérêts nationaux. Il permettrait également de **mobiliser non seulement l'épargne des Français, mais aussi les Français eux-mêmes**, autour de la protection des entreprises stratégiques. Cela pourrait être un moyen de consolider le lien armées – Nation et de renforcer l'attention des citoyens aux enjeux de la défense nationale.

Recommandation n° 14 : Créer un livret défense et souveraineté ou flécher une partie des encours du livret A et du livret de développement durable et solidaire vers les PME de l'industrie de défense.

Le rapporteur spécial rappelle, à toutes fins utiles, et comme il l'avait fait en tant que rapporteur d'une proposition de loi en 2024 (1), que ce fléchage n'enlèverait aucun financement au logement social, à la transition écologique ou à l'économie sociale et solidaire. Les ressources mobilisées ne financeraient non plus aucune activité illégale, ni en France ni à l'étranger.

Le rapporteur spécial note que sa proposition est défendue à l'Assemblée nationale par des députés de tout bord politique. Elle a d'ailleurs récemment été reprise par le Rassemblement national (2), qui s'était auparavant prononcé contre. Elle est donc **susceptible de faire l'objet d'un accord transpartisan** à l'Assemblée nationale, comme l'avait été, au Sénat, la proposition de loi de M. Pascal Allizard, adoptée à la quasi-unanimité.

(1) Assemblée nationale, rapport n° 2244 (XVI^e législature) de M. Christophe Plassard, fait au nom de la commission des finances, de l'économie générale et du contrôle budgétaire, sur la proposition de loi visant à flécher l'épargne non centralisée des livrets réglementés vers les entreprises du secteur de la défense nationale (n° 2094), enregistré à la présidence le 28 février 2024.

(2) Assemblée nationale, rapport d'information n° 1645 (XVII^e législature) de M. Émeric Salmon, fait au nom de la commission des finances, de l'économie générale et du contrôle budgétaire, sur le soutien public à l'industrie de défense, enregistré à la présidence le 25 juin 2025.

c. L'incitation des particuliers à investir dans l'économie européenne

Les menaces capitalistiques qui pèsent sur les PME de la BITD proviennent, en partie, des liquidités financières abondantes dont disposent certains de nos compétiteurs stratégiques, notamment anglo-saxons. Le niveau de liquidités plus faible dont disposent l'Europe, et singulièrement la France, s'explique notamment par l'absence de régime de retraite par capitalisation et de fonds de pension désireux d'investir à moyen et long terme. Il procède également du fait qu'**une large partie de l'épargne des Européens, et parmi eux des Français, part à l'étranger**, notamment aux États-Unis, à la recherche de rendements plus élevés, et ne profite donc pas au financement des entreprises européennes.

À cet égard, il convient de souligner que la fiscalité du capital est indifférente à la destination du placement. Afin d'inciter les investisseurs français à soutenir l'économie française et européenne, et en particulier les secteurs stratégiques, il pourrait être envisagé de créer un crédit d'impôt spécifique qui permettrait de réduire le montant de l'imposition due au titre des produits des investissements **dans des entreprises établies en France ou au sein de l'Union européenne**, ce qui leur donnerait un avantage comparatif par rapport aux entreprises du reste du monde. Les fonds, et notamment les ETF (*exchange trading funds*), seraient classés dans l'une ou l'autre de ces catégories en fonction de la localisation de l'indice boursier dont ils visent à répliquer le rendement.

Recommandation n° 15 : Créer un crédit d'impôt permettant de réduire l'imposition due au titre des produits des investissements dans les entreprises françaises et européennes.

Compte tenu de la situation des finances publiques, il paraît toutefois difficile de réduire la fiscalité tant que le pays n'a pas retrouvé une trajectoire de dépense publique soutenable. En conséquence, le coût de ce crédit d'impôt pourrait être financé par un relèvement à due concurrence du prélèvement forfaitaire unique (PFU).

3. Rendre les autorisations d'exportation plus contraignantes

Comme l'a rappelé le ministre des armées le 20 mars 2025 *(voir le 1 du A du présent IV)*, et ainsi que le rapporteur spécial a déjà plusieurs eu l'occasion de le rappeler, la France dispose d'un **cadre juridique solide, éprouvé et exemplaire** en matière de vente d'armes et de biens à double usage.

L'article L. 2335-2 du code de la défense prévoit que « *l'exportation sans autorisation préalable de matériels de guerre et matériels assimilés vers des États non-membres de l'Union européenne [...] est prohibée* ». La production et l'exportation de matériels de guerre sont donc interdites par principe et ne sont autorisées que par exception, au cas par cas, avec des contrôles stricts.

Sous l'autorité du Secrétariat général de la défense et de la sécurité nationale (SGDSN), la Commission interministérielle pour l'exportation des matériels de guerre (CIEEMG) instruit les demandes d'autorisation d'exportation et émet un avis préalable à la délivrance d'une licence d'exportation, en tenant compte des

conventions internationales sur la vente d'armes ratifiées par la France, de la situation intérieure du pays de destination finale et de ses pratiques en matière de respect des droits de l'Homme, des conséquences de l'exportation pour la paix et la sécurité dans la région concernée ainsi que du risque de détournement.

Les règles et procédures assurent un haut niveau de contrôle sur les équipements exportés En 2023, la Cour des comptes estimait que l'organisation du soutien à l'exportation de matériel militaire était « *globalement satisfaisante* » et que le contrôle était « *rigoureux* » [(1)]. À titre d'illustration, la France s'interdit d'exporter des armes de poing, ce que ne font pas l'ensemble de nos alliés ; or les armes de poing sont bien plus facilement détournées de leur usage souhaité que des équipements plus sophistiqués. En réponse à une fausse information récemment relayée concernant de prétendues ventes d'armes de la France à Israël, il convient également de souligner que la France ne vend pas d'armes à Israël mais uniquement des composants qui servent exclusivement à la fabrication d'équipements militaires à vocation purement défensive.

Or, **malgré ce cadre juridique exemplaire, certaines banques s'autorisent à refuser de financer des opérations qui ont pourtant été autorisées par l'État**. Le cas d'une PME visitée par le rapporteur spécial dans le cadre de sa mission est à cet égard très emblématique. Leader mondial dans son secteur, et donc sans difficulté financière, cette entreprise a, à plusieurs reprises depuis 2020, fait face à des refus de financement bancaire visant à garantir les acomptes que lui versaient des clients dans le cadre de contrats conclus dans un pays du Moyen-Orient. Raison invoquée : les contrats concernés approvisionnent des exportations d'équipements qui, selon les banques, sont susceptibles d'être utilisés dans le conflit au Yémen. Or, pour chacune des opérations refusées, l'entreprise avait obtenu une licence d'exportation. Est-il acceptable que des banques françaises se permettent de mener une politique différente de celle de l'État et contraire à nos intérêts militaro-industriels ? Est-il normal qu'elles le fassent, en outre, de façon opaque, souvent sans trace écrite, et en contradiction avec les lignes directrices ou les discours publics qu'elles veulent bien afficher publiquement ?

En conséquence, le rapporteur spécial estime nécessaire d'envisager la possibilité de conférer aux licences d'exportation délivrées par l'État un caractère plus contraignant, qui s'impose d'une manière ou d'une autre aux établissements bancaires. Dès lors qu'une opération a été autorisée par la CIEEMG, une banque ne devrait plus avoir la possibilité de refuser à l'entreprise qui la porte un quelconque financement, sauf à ce que les motifs du refus soient justifiés par des raisons financières objectives et documentées.

Recommandation n° 16 : Envisager une évolution du cadre législatif permettant de conférer aux licences d'exportation délivrées par l'État un caractère contraignant pour les établissements bancaires.

(1) Cour des comptes, « Le soutien aux exportations de matériel militaire », rapport public thématique, janvier 2023.

Le rôle des entreprises de la BITD est de produire pour équiper nos armées à la hauteur de leurs besoins, pas de perdre leur temps à chercher des financements alors même qu'elles sont soutenues par l'État. Notre intérêt national est que les entreprises soient financées convenablement, pour assurer le développement de nos capacités. La préservation de leur image par les banques ne doit pas prendre le pas sur leur mission première qui est de soutenir l'activité économique et de permettre à nos filières de souveraineté de perdurer.

TRAVAUX EN COMMISSION

Lors de sa réunion de 10 heures, le mercredi 16 juillet 2025, la commission a entendu M. Christophe Plassard, rapporteur spécial des crédits des programmes 144 et 146 de la mission Défense*, sur son rapport d'information sur la guerre économique, présenté en application de l'article 146, aliéna 3, du règlement de l'Assemblée nationale.*

M. le président Éric Coquerel. L'ordre du jour appelle l'examen du rapport d'information sur la guerre économique, présenté par M. Christophe Plassard en sa qualité de rapporteur spécial de la mission *Défense* pour les programmes consacrés à la préparation de l'avenir. C'est d'actualité après les annonces du chef de l'État.

M. Christophe Plassard, rapporteur spécial (*Préparation de l'avenir*). Je souhaite vous faire part de nos constats, notamment sur les vulnérabilités de notre base industrielle et technologique de défense (BITD), avant de formuler les recommandations essentielles pour y répondre dans l'intérêt de la nation.

La France fait face à une intensification sans précédent de la guerre économique. Celle-ci ne se limite plus à la simple concurrence commerciale : elle prend la forme d'une véritable confrontation où tous les moyens – humains, physiques, numériques, juridiques, capitalistiques, informationnels – sont employés pour affaiblir ou déstabiliser nos entreprises stratégiques. C'est le constat unanime issu des auditions menées auprès des acteurs de la défense, des services de renseignement, des industriels et du monde académique. Il était donc urgent d'actualiser notre diagnostic et d'évaluer les moyens de protéger durablement nos actifs essentiels.

Notre rapport révèle d'abord un niveau élevé et croissant de menace contre la BITD : on relève 500 à 550 atteintes avérées par an et plus de 750 alertes de sécurité économique recensées pour l'année 2024, contre à peine la moitié quatre ans plus tôt. 80 % des attaques visent nos PME, qui sont essentielles à notre autonomie stratégique mais restent le maillon faible de la chaîne de valeur, car elles sont moins dotées pour se défendre que les grands groupes.

Les menaces sont désormais protéiformes. Les atteintes humaines – espionnage, recrutement ciblé de compétences, indiscrétions internes – représentent plus d'un tiers des actions hostiles. Le nombre d'atteintes physiques – intrusion, sabotage, survol de sites sensibles par des drones – a quasiment doublé en un an. Celui des cyberattaques explose : l'Anssi (Agence nationale de la sécurité des systèmes d'information) a traité en 2024 plus de 4 000 incidents de sécurité sur des entités stratégiques, ce qui représente une hausse de 15 %. Les menaces capitalistiques concernent des entreprises fragilisées financièrement qui peuvent devenir la cible de prises de contrôle hostiles ou d'investissements indirects étrangers. Ces menaces peuvent enfin prendre la forme d'une instrumentalisation du droit – *lawfare* – et de campagnes d'influence, menées souvent à distance, pour détruire des réputations ou bloquer des contrats stratégiques à l'export.

Dans ces menaces, il n'y a pas d'ennemi unique. La Russie, la Chine, mais aussi des alliés stratégiques comme les États-Unis sont engagés dans cette compétition, chacun mobilisant ses moyens – influence, finance, espionnage, normes – pour protéger et favoriser ses propres industries de défense. Il ne s'agit pas de condamner ces pratiques, mais d'appeler à la fin de la naïveté pour défendre, nous aussi, nos intérêts.

Nos travaux mettent en lumière de réels progrès dans l'organisation de l'intelligence économique nationale. Les moyens humains et budgétaires de la direction générale de l'armement (DGA) et de sa direction de l'industrie de défense (DID), du service de l'information stratégique et de la sécurité économiques (SISSÉ) et des services de renseignement – DRSD (direction du renseignement et de la sécurité de la défense) et DGSE (direction générale de la sécurité extérieure), dont les effectifs et les budgets sont en hausse constante depuis 2018 – ont été renforcés. La DGA s'est organisée pour accompagner et soutenir les entreprises, notamment celles en difficulté, grâce à des rencontres de terrain régulières – près de 900 visites par an. Enfin, les dispositifs juridiques ont été modernisés. Ainsi, le contrôle des investissements étrangers en France (IEF) a été densifié et élargi à de nouveaux secteurs stratégiques : 200 lettres d'engagement sont activement suivies pour éviter le dépeçage, le transfert sensible ou la délocalisation des activités de recherche et développement. Par ailleurs, la loi dite de blocage de 1968, qui a été réactivée et concrétisée, est devenue une protection crédible pour les entreprises exposées à des injonctions étrangères abusives.

Cependant, malgré les progrès, nos dispositifs restent trop permissifs, nos moyens parfois éclatés et notre posture trop défensive face à des adversaires dotés de stratégies offensives assumées. Le rapport formule plusieurs axes d'action qui doivent, selon moi, devenir des priorités partagées par la représentation nationale : consolidation et renforcement des moyens dédiés à la sécurité économique ; renforcement des points faibles de nos chaînes d'approvisionnement ; durcissement de la réponse face aux menaces capitalistiques et juridiques ; amélioration de la mobilisation de l'épargne nationale pour investir dans notre industrie de défense.

La consolidation et le renforcement des moyens dédiés à la sécurité économique passent par l'augmentation des moyens humains et budgétaires de la DGA, de la DRSD et du SISSÉ pour couvrir tout le territoire, accélérer les enquêtes de sécurité et anticiper les menaces émergentes, notamment informationnelles ou cognitives. Il faut également assurer une meilleure coordination, éviter la dispersion des responsabilités administratives, garantir la stabilité et la transversalité du SISSÉ et renforcer le dialogue avec le secteur privé.

Nos points faibles sont nos PME, leur souveraineté numérique et les ressources humaines. Il faut généraliser la sensibilisation et l'accompagnement des PME de la BITD, renforcer les exigences de protection du potentiel scientifique et technique et imposer progressivement le stockage souverain des données critiques sur des serveurs situés en France ou en Europe. Il faut également mettre en place un cadre facilitant la constitution d'un vivier de personnels habilités pour répondre aux besoins massifs de recrutement en cas de crise.

Le durcissement de la réponse face aux menaces capitalistiques et juridiques demande de mieux anticiper la sortie des fonds d'investissement étrangers, d'organiser la gouvernance pour renforcer le suivi des engagements dans les entreprises stratégiques, d'alourdir de manière significative les sanctions en cas de méconnaissance de la loi de blocage et de rendre plus contraignantes les licences d'exportation délivrées par l'État pour qu'aucun établissement bancaire n'ait la possibilité d'aller à l'encontre d'une décision souveraine, sauf motif financier objectif et documenté.

Enfin, une meilleure mobilisation de l'épargne nationale passe par la création de canaux de financement publics et privés, par la mise en place de fonds d'investissement publics ouverts aux particuliers, par un fléchage de l'épargne réglementée – livret A ou livret de développement durable et solidaire (LDDS) – vers les PME de défense et par la création d'un crédit d'impôt pour orienter l'investissement vers l'économie française et européenne.

Nous proposons également d'affecter une part des dividendes perçus par l'État à la protection des entreprises stratégiques en renforçant ainsi la capacité d'intervention de l'Agence des participations de l'État (APE) en cycle difficile.

Notre cadre juridique national est solide, mais la France seule ne peut répondre à toutes les menaces. Il faut impulser une réponse européenne ambitieuse pour adopter un règlement de blocage sur le modèle de notre loi de 1968, créer un label similaire à l'Itar (*International traffic in arms regulations*) américain pour protéger les technologies et marchés sensibles et nous doter d'armes normatives comparables à celles de nos principaux compétiteurs. Il faut également pousser à une harmonisation réelle des mécanismes de filtrage des investissements étrangers pour empêcher la prédation de nos innovations par des acteurs non européens. Il revient à la France, qui est en pointe en Europe sur l'ensemble des outils juridiques de protection économique, de porter ces sujets au niveau européen.

Quatre des seize recommandations du rapport sont prioritaires. La première est la généralisation du conseil d'administration alternatif, appelé *proxy board* aux États-Unis, pour renforcer le suivi des engagements imposés aux investisseurs étrangers. La deuxième est l'affectation du produit des dividendes perçus par l'État au compte d'affectation spéciale *Participations financières de l'État*, afin que les résultats des entreprises détenues par l'État puissent alimenter ce fonds. La troisième consiste à conférer un caractère contraignant pour les établissements bancaires aux licences d'exportation d'armes délivrées par l'État. La dernière est la création d'un livret défense souveraineté ou le fléchage d'une partie des encours des livrets réglementés vers les PME de la défense.

La France a les atouts pour défendre sa souveraineté économique. Ce rapport n'est ni un constat de défaite, ni un plaidoyer pour le repli. Il est un appel à une mobilisation collective, lucide et déterminée. La guerre économique n'est pas un concept abstrait, c'est une guerre du réel, qui se joue chaque jour sur nos territoires, dans nos entreprises, dans nos laboratoires et dans nos infrastructures numériques. Nos adversaires ont compris que la dépendance technologique et financière est la clé de la domination moderne. La meilleure réponse est de bâtir une protection à la hauteur de nos ambitions. Plutôt que de céder à la naïveté ou de sombrer dans la frilosité, il faut assumer une posture offensive, pragmatique et ouverte à l'innovation et à la coopération européenne.

M. le président Éric Coquerel. Selon votre rapport, « les menaces viennent de tous nos compétiteurs stratégiques », « les ingérences étrangères les plus graves proviennent naturellement de la Russie et de la Chine, ainsi que d'autres pays dont l'industrie de défense est concurrente de la nôtre, mais certaines proviennent aussi de pays qui sont nos alliés sur le plan géostratégique, en tête desquels les États-Unis ». Je ne nie pas que la Russie et la Chine soient des compétiteurs stratégiques – j'ai même cru comprendre que le chef de l'État fait de la Russie un adversaire. En revanche, l'idée que les États-Unis seraient un allié me laisse très dubitatif à un moment où ils poussent à son paroxysme la logique selon laquelle ils n'ont que des intérêts et aucun allié, se replient sur eux-mêmes et engagent une guerre commerciale avec à peu près tous les blocs politico-économiques, y compris l'Europe, coupent l'aide publique au développement, ce qui menace des millions de personnes vulnérables dans le monde, et enfreignent le droit international, notamment en bombardant l'Iran.

Le chancelier allemand a récemment exprimé le souhait que l'armée allemande devienne l'armée conventionnelle la plus importante en Europe et le président du groupe CDU au Bundestag a déclaré que, s'il y avait une dissuasion européenne, il serait naturel que ce soit l'Allemagne qui en dispose. Cela m'inquiète d'autant plus que l'Allemagne a annoncé un effort considérable pour porter à 3,5 % la part de son budget consacrée à la défense d'ici 2029-2030. S'agit-il, pour vous, de quelque chose d'anodin et de normal, de quelque chose qui

pourrait être intégré à une défense européenne, quoi qu'on pense de cette idée ? Ou bien devons-nous prendre en compte le fait que notre voisin, avec lequel nous avons connu plus que des blessures depuis 150 ans, envisage de se réarmer à ce point, et nous demander dans quel but ?

Les Forges de Tarbes produisent des corps creux d'obus de 155 mm, nécessaires aux canons Caesar. Le 17 mai 2024, leur propriétaire, Europlasma, a signé un accord avec la société Bizzell Europe, filiale du groupe Bizzell Corporation, qui opère principalement au profit du gouvernement américain. Cette proximité avec un groupe états-unien est de nature à susciter une inquiétude légitime face à l'éventuel projet d'entrée du groupe Bizzell dans le capital des Forges de Tarbes, dont la situation est fragile. La matérialisation de ce scénario conduirait à une influence, voire à un contrôle, états-unien sur les corps creux d'obus français de 155 mm, donc, incidemment, sur les canons Caesar, qui jouent un rôle majeur dans l'autonomie stratégique française. Lors d'une audition au ministère de l'industrie, les syndicats des Forges de Tarbes ont exprimé leur inquiétude face aux investissements prévus par Europlasma, qui sont loin de ce qui avait été prévu.

Vous concluez dans votre rapport, qui ne parle pas des Forges de Tarbes, que le cadre juridique national est complet et efficace et qu'il appelle peu d'évolutions législatives ou réglementaires. Ne pensez-vous pas que le cadre juridique pourrait être amélioré afin de prévenir plus efficacement ce genre de rapprochements, qui peuvent, à terme, porter atteinte à notre souveraineté ? Il me semble souhaitable que l'État contrôle sur place les investissements promis. Qu'en pensez-vous ?

Vous écrivez dans votre rapport : « S'agissant de Vencorex, sous la menace d'un rachat par le groupe chinois Wanhua, il faut souligner que ce rachat ne concerne pas l'activité de production de sels purifiés qui sont utilisés dans certains matériels stratégiques et qu'il n'induit aucun transfert technologique. La France dispose de stocks suffisants et de sources d'approvisionnement alternatives. » À ce propos, le ministre a parlé de sources allemandes lors des questions au Gouvernement, ce qui ne me paraît pas une bonne alternative du point de vue de notre souveraineté.

Lors de son audition du 28 avril à l'Assemblée nationale, Jean-Luc Béal, PDG de Vencorex, a déclaré que le groupe chinois reprend « l'ensemble des actifs incorporels, c'est-à-dire le savoir-faire, mais pas les installations de production » de sel. Or, dans les actifs incorporels, il y a les brevets. L'acheteur chinois peut-il, dans ces conditions, obtenir les brevets de production de sel pour la fabrication de missiles de la dissuasion nucléaire même s'il ne prend pas le contrôle de la mine de Hauterives ? Ne faudra-t-il pas adapter le cadre juridique en cas de vulnérabilité ?

Le groupe chinois n'a récupéré qu'un atelier sur quatre, suscitant une vive inquiétude des salariés sur la pérennité du site. N'aurait-il pas fallu privilégier, sinon une nationalisation, du moins le projet de coopérative proposé par les salariés, qui semble plus sûr du point de vue de la souveraineté ?

Enfin, vous écrivez que « la guerre économique implique également la mise en œuvre de manœuvres plus offensives. On ne peut pas se contenter de subir en permanence. Il faut dans certains cas être proactif. En la matière, force est de constater que nos compétiteurs stratégiques, ennemis ou alliés, hésitent moins que nous. C'est donc une évolution des mentalités qui doit s'opérer ». Et, plus loin : « Nous faisons encore preuve d'une retenue que ne connaissent pas tous nos compétiteurs. »

Sur ce point, nos analyses divergent. J'entends dans votre propos l'écho du discours appelant à se préparer à une guerre qui vient. Le chef de l'État a ainsi parlé du risque d'un conflit de haute intensité en Europe dans les années à venir, sans que l'on sache si cela impliquerait l'intervention directe de la France. Mais quand on prépare une guerre, on produit de plus en plus d'armes ; or la logique de l'économie capitaliste veut que ce qui est produit, dans ce secteur comme dans n'importe quel autre, soit utilisé ; en l'occurrence, cela met encore plus en danger la paix dans le monde. La production d'armes va-t-elle servir à assurer notre défense nationale, ce à quoi je serais évidemment très favorable, ou contribuer à la provocation et à l'aggravation des conflits ? Sur ce débat important – est-ce une économie de paix ou une économie de guerre que nous voulons ? –, j'aimerais entendre votre réaction.

M. Christophe Plassard, rapporteur spécial. Selon moi, les États-Unis sont un allié face au risque de guerre – nous ne pourrions pas imaginer, d'ailleurs, que ce pays nous déclare la guerre.

Cela étant, le rapport d'information, entre autres travaux, montre que l'orientation stratégique des États-Unis a changé. Ce pays fait converger ses efforts vers d'autres parties du monde que l'Europe. Les Français et, plus globalement, les Européens doivent donc prendre ou reprendre en main les questions de défense.

En outre, les États-Unis sont des compétiteurs industriels – je les ai cités en tant que tels et c'est en ce sens que je dis qu'il ne faut pas faire preuve de naïveté. Les forces européennes sont très majoritairement équipées de matériel américain. Or il faut établir quelles dépendances fragilisent notre souveraineté.

Certes, la France a désigné la Russie comme ennemie, mais c'est surtout la Russie qui l'a désignée comme son ennemie principale en Europe.

Non, ce qui se passe en Allemagne n'est pas anodin, y compris pour le peuple allemand, fortement marqué par son histoire. Est-ce normal ? Une défense européenne doit s'appuyer sur le couple franco-allemand, puisque c'est en grande partie la réconciliation franco-allemande qui a permis d'installer durablement la paix sur notre continent. Et il est normal que la part de l'Allemagne dans un effort européen soit à la hauteur de son poids en Europe. Vous me demandiez si cette démarche est susceptible d'être intégrée à une défense européenne ; je préfère évoquer des efforts européens de défense, dans lesquels, je le répète, l'Allemagne doit avoir toute sa part. Les industries de nos deux pays sont très liées. Airbus constitue un bon exemple de notre collaboration fructueuse sur les plans civil et militaire.

Je ne connais pas le détail du dossier des Forges de Tarbes, faute d'avoir auditionné les représentants de cette entreprise. Toutefois, nous sommes plutôt bien dotés sur les plans administratif et juridique pour faire face à ce type de prise de capital. Les investissements étrangers en France sont contrôlés et la DGA peut bloquer des transactions. Je fais confiance aux experts de la direction de l'industrie de défense de la DGA et à ceux du SISSÉ, entre autres services de Bercy, pour agir dans le cadre juridique adéquat, ou en demandant une action prioritaire.

Nous pourrions effectivement envisager des évolutions juridiques. J'ai parlé du *proxy board* dont les États-Unis imposent la création aux étrangers investissant sur leur territoire – un conseil d'administration parallèle composé uniquement de citoyens américains. Puisque des étrangers investissent également en France, et c'est tant mieux, nous pourrions soumettre les entreprises concernées à un tel dispositif, afin de bénéficier d'un droit de regard sur leur gouvernance – par exemple concernant la délocalisation des unités de production ou le

recrutement du patron d'une *business unit* située en France. Cet outil de contrôle national pourrait s'ajouter aux *golden shares*, ou actions prioritaires.

De même, je fais confiance à la DGA pour contrôler la reprise de Vencorex et, si nécessaire, la bloquer. Les représentants de cette entreprise indiquent que les brevets et les éléments critiques et stratégiques sont placés dans une entité à part. Si les étrangers qui ont acquis une partie de Vencorex souhaitent bénéficier des informations stratégiques que détient cette entité sur le processus de production et les produits, la loi de blocage de 1968, qui a été renforcée depuis 2020, permettra de l'empêcher. La situation est ainsi sécurisée grâce à la loi et à la DGA.

Depuis que je travaille sur les questions de défense – je produirai cette année mon quatrième rapport spécial pour la mission *Défense*, pour lequel nous avons envoyé le 10 juillet nos questions au ministère des armées, j'ai été rapporteur pour avis de la LPM (loi de programmation militaire) et j'avais déjà lancé précédemment une mission d'information sur l'économie de guerre –, j'ai appris comment fonctionne notre stratégie. Heureusement ou malheureusement, la logique actuelle est celle des rapports de force et se caractérise par une forme de brouillage stratégique.

Notre production d'armes s'inscrit clairement dans une logique de défense et non d'attaque – ainsi avons-nous équipé l'armée arménienne avec des équipements radar ou de défense sol-air. La France n'a pas vocation à déclarer la guerre à d'autres pays, mais à se défendre, à défendre sa souveraineté et la souveraineté européenne, ainsi qu'à honorer ses engagements auprès de l'Otan.

La situation internationale nous commande de peser davantage dans les rapports de force. Pendant des dizaines d'années, au nom des dividendes de la paix, nous avons réduit nos dépenses militaires, jusqu'à nous fragiliser. Actuellement, le pourcentage de la richesse nationale consacré à la défense reste éloigné de celui des années 1970 dans le contexte de la guerre froide.

M. le président Éric Coquerel. Si j'ai évoqué la défense européenne, ce n'est pas parce que j'y suis favorable, mais pour préciser que l'effort militaire allemand ne s'inscrit pas dans ce projet : il s'agit bien pour l'Allemagne de bâtir l'armée conventionnelle la plus importante d'Europe. Ce projet devrait nous interroger au vu des 150 dernières années.

Mme Sophie Mette (Dem). Je salue la qualité de vos travaux, qui mettent en évidence la montée de menaces protéiformes pesant sur la base industrielle et technologique de défense et les efforts de l'État pour y faire face.

Pourriez-vous préciser vos recommandations ? Vous évoquez des créations de postes et des moyens humains supplémentaires pour les services de protection et de renseignement. Disposez-vous d'un chiffrage précis ? Sur quelle trajectoire budgétaire et quels crédits ces hausses pourraient-elles s'appuyer ? Supposent-elles des redéploiements internes ou envisagez-vous de nouveaux financements ?

Vous évoquez également des solutions souveraines pour le stockage des données. Cela soulève la question de leur soutenabilité économique pour les PME. Disposez-vous d'une évaluation des surcoûts pour ces dernières ? Un mécanisme de soutien pour les accompagner serait-il envisageable ?

Votre rapport insiste à juste titre sur la montée en puissance de la loi de blocage, mais pointe la faiblesse des sanctions actuelles. Quelles sanctions seraient pertinentes ? Une modification législative est-elle déjà en préparation ?

M. Christophe Plassard, rapporteur spécial. Non, les engagements financiers nécessaires ne sont pas chiffrés. Nous avons toutefois une idée des masses nécessaires. Le SISSÉ – qui est rattaché à la direction générale des entreprises, à Bercy, et non au ministère de la défense – compte quelques dizaines de postes. Dix ou vingt postes supplémentaires permettraient une croissance énorme de ce service, pour un coût assez faible. De même, les services de renseignement dédiés à ces questions ne comptent que quelques centaines de postes alors que le budget de la défense s'élèvera à plus de 50 milliards d'euros cette année.

Le discours du président de la République le 13 juillet laisse augurer une loi de programmation militaire rectificative. Elle permettra à la commission des finances et à la commission de la défense d'adapter la programmation à l'évolution des menaces en matière de guerre économique et d'intelligence économique. Dans la version actuelle de la LPM, le budget des services de renseignement est celui qui a connu la plus grosse croissance.

La loi de blocage de 1968 prévoit une pénalité maximale de 18 000 euros. Alors que les enjeux se chiffrent en millions d'euros, voire en dizaines ou centaines de millions d'euros, ce montant paraît un peu faible. Cette loi a été renforcée et elle est appliquée beaucoup plus fréquemment depuis le début des années 2020. Elle fonctionne et elle est prise en compte par nos compétiteurs, grâce à de nouvelles jurisprudences. Toutefois, nous pourrions nous pencher sur le montant des pénalités qu'elle prévoit, pour renforcer leur effet dissuasif.

La commission autorise, en application de l'article 146, alinéa 3 du Règlement de l'Assemblée nationale, la publication du rapport d'information.

LISTE DES PERSONNES AUDITIONNÉES

Dans le cadre de ce rapport, le rapporteur spécial a mené vingt-neuf auditions et un déplacement.

Il a notamment rencontré les représentants de :

– 13 entreprises, dont 8 PME ;

– 5 groupements d'entreprises ;

– 5 directions ou services d'administration centrale ;

– 2 personnalités qualifiées.

L'identité des personnes auditionnées est volontairement gardée confidentielle, afin de ne pas les exposer et de conserver la plus grande liberté de parole possible.