Le ministère de la Défense et la protection des industries du **secteur d'activité d'importance vitale** « activités industrielles de l'armement »

Dominique Pierron

Le ministère de la Défense coordonne, dans le cadre de la réglementation sur la sécurité des activités d'importance vitale (SAIV) la sécurité des opérateurs d'importance vitale (OIV) du secteur des activités industrielles (AIA) de l'armement. Ce dispositif s'insère dans une planification nationale de défense et de sécurité définie au niveau interministériel par le secrétariat général de la défense et de la sécurité nationale (SGDSN), et qui comprend d'autres mécanismes répondant à des enjeux différents, notamment la protection du potentiel scientifique et technique, et la protection du secret de la défense nationale. Dominique Pierron, chargé d'études à la Direction de la Protection des Installations, moyens et activités de la Défense (DPID), fait le point dans cet article sur l'organisation mise en place au ministère de la Défense pour travailler et échanger avec les OIV, ainsi que sur le lien entre la SAIV et les deux autres dispositifs.

Les industries du secteur de l'armement et le ministère de la Défense sont liés non seulement par des contrats mais aussi par des enjeux de sécurité nationale, portés par différents dispositifs : la protection physique des installations d'importance vitale, la cybersécurité, la protection du secret de la défense nationale et la protection du potentiel scientifique et technique (PPST).

Ce sont plus spécialement les deux premiers champs qui sont étudiés dans cet article, sous l'angle de la réglementation relative à la sécurité des activités d'importance vitale (SAIV).

Fondements de la sécurité des activités d'importance vitale (SAIV)

Rappelons d'abord dans les grandes lignes les tenants et les aboutissants de la SAIV. La protection des installations vitales était historiquement mise en œuvre sur la base d'une ordonnance du 29 décembre 1958 complétée par une instruction dont la dernière version datait de 1993[1]. Ce dispositif avait conduit à la désignation, de manière plus ou moins rationnelle, d'un certain nombre d'installations comme points sensibles de différentes catégories (1, 2 ou 3) selon leur importance, sur l'ensemble du territoire national. Ce système, né dans le contexte de la guerre froide, juridiquement insuffisamment étayé, avait fini par perdre sa pertinence au regard de l'évolution de la menace. En effet, celle-ci avait profondément changé tant du point de vue de sa motivation idéologique (montée en puissance de l'islamisme radical) que de ses modes d'action (terrorisme et cybermenace) et des conséquences en cascade potentielles sur des organisations publiques et privées complexes et interdépendantes (« effets domino » causés par des coupures d'alimentation énergétique, pannes informatiques, ruptures d'approvisionnement de fournisseurs, etc.).

Pensé et conçu après les attentats terroristes de New-York (11 septembre 2001), de Madrid (11 mars 2004) et de Londres (7 juillet 2005) le dispositif national de la sécurité des activités d'importance vitale[2] (SAIV) a remplacé l'ancien système et est ainsi venu compléter en 2006 un dispositif de planification de défense et de sécurité nationale contre les actes de malveillance, notamment à caractère terroriste, composé schématiquement de trois éléments : plan Vigipirate[3], SAIV et plans d'intervention de la famille « pirate ». Cet ensemble est piloté et coordonné au niveau interministériel par le SGDSN.

Le dispositif SAIV a ainsi donné une assise juridique plus solide à l'organisation des relations entre l'Etat et les opérateurs d'importance vitale, ces derniers étant définis[4] comme « gérant ou utilisant un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :

> a) d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;
>
> b) ou de mettre gravement en cause la santé ou la vie de la population. »

Ces installations sont qualifiées de points d'importance vitale (PIV).

L'architecture de la planification SAIV, désormais bien connue des acteurs, consiste en :

- des directives nationales de sécurité (DNS) par secteur d'activité (énergie, santé, transport, défense, etc.), élaborées sous l'égide des ministères coordonnateurs concernés[5] et approuvées par le Premier ministre, et qui définissent les scénarios de menace et les objectifs de sécurité auxquels les OIV

1 *Instruction générale interministérielle n°4600 du 8 février 1993 sur la sécurité des points et réseaux sensibles.*

2 *Articles L.1332-1 à L.1332-7 et décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale, codifié aux articles R.1332-1 à R.1332-42 du code de la défense. L'instruction générale interministérielle n°6600 du 7 janvier 2014 (IGI 6600) complète l'ensemble.*

3 *Plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroriste du 17 janvier 2014.*

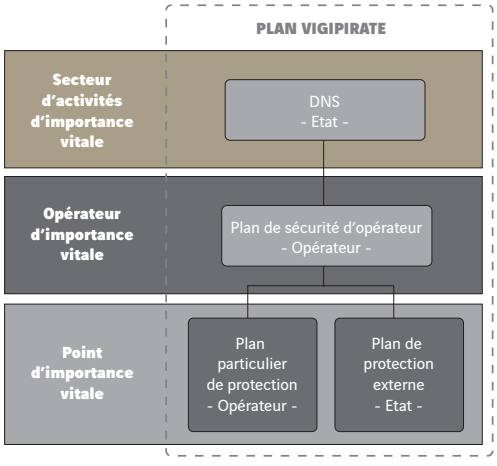
4 *Article R.1332-1 du code de la défense.*

5 *Arrêté du Premier ministre du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs, modifié par l'arrêté du 3 juillet 2008.*

doivent se conformer ; précisons que les DNS n'imposent pas de réponse toute faite aux OIV, ni de moyens prédéterminés à mettre en œuvre ;

- un plan de sécurité d'opérateur (PSO), par lequel l'OIV va élaborer sa propre évaluation des risques[6] à partir des scénarios de la DNS, déterminer ses PIV et définir sa politique et ses mesures concrètes de protection ;

- un plan particulier de protection (PPP) élaboré par l'OIV et un plan de protection externe (PPE) élaboré par le préfet de département, pour chaque PIV.



Source : instruction générale interministérielle relative à la sécurité des activités d'importance vitale du 7 janvier 2014

Tous ces documents étant classifiés, il ne s'agit pas ici d'entrer dans le fond du sujet. Notons cependant qu'au sein de ce dispositif interministériel, le secteur d'activité « activités militaires de l'Etat », qui inclut le sous-secteur « activités industrielles de l'armement », fait l'objet de procédures dérogatoires par rapport aux secteurs d'activités civils, portant notamment, d'une part sur des restrictions de diffusion des plans de protection vers les autres acteurs étatiques impliqués, d'autre part sur un régime d'audit et d'inspection des PIV qui incombent exclusivement aux services spécialisés de la défense.

Ce dispositif continue d'évoluer et a notamment ajouté dans son corpus juridique, via l'article 22 de la loi de programmation militaire du 18 décembre 2013 (voir encadré), la notion de systèmes d'information d'importance vitale (SIIV) pour lesquels, au titre des dispositions du décret n°2015-351 du 27 mars 2015 « l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, ou pourrait présenter un danger grave pour la population ». Les SIIV font à ce titre l'objet de mesures de sécurité renforcées. On voit bien que la logique présidant à l'identification et à la protection des SIIV est la même que celle qui prévaut pour les PIV, les SIIV s'apparentant en quelque sorte à des « PIV logiques ».

La sécurité des systèmes d'information des opérateurs d'importance vitale

La loi de programmation militaire (loi n° 2013-1168 du 18 décembre 2013) a introduit d'importantes dispositions relatives à la sécurité des systèmes d'information des opérateurs d'importance vitale.

Ces nouvelles dispositions permettront de renforcer significativement la sécurité de ces opérateurs dont le rôle est primordial pour le fonctionnement de la Nation.

Le décret n°2015-351 du 27 mars 2015 précise les conditions dans lesquelles :

6 *Selon une méthode simple proposée par l'Etat, mais non obligatoire, inspirée de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité).*

- sont fixées les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs d'importance vitale,

- sont mis en œuvre les systèmes de détection d'événements affectant la sécurité de ces systèmes d'information,
- sont déclarés les incidents affectant la sécurité ou le fonctionnement de ces systèmes d'information,
- sont contrôlés ces systèmes d'information.

Source : ANSSI (Agence nationale de la sécurité des systèmes d'information).

Quels sont les opérateurs d'importance vitale du périmètre des activités industrielles de l'armement ? Sans surprise, on retrouvera les entreprises du secteur de l'armement les plus stratégiques pour la défense nationale, notamment dès lors qu'elles participent via l'équipement des armées au maintien du potentiel de défense. A cet égard, il convient de noter que les critères de sélection des OIV font que ceux-ci ne comprennent pas l'ensemble des sociétés en lien avec le ministère de la Défense au titre des contrats sensibles.

En fait, les OIV constituent l'ossature essentielle du « complexe militaro-industriel » français. Ils sont actuellement un peu moins d'une vingtaine. Quels sont les enjeux communs entre le ministère de la Défense et les OIV ? Il s'agit d'organiser le dialogue et la coopération public-privé entre les acteurs du secteur de la Défense, concernant l'analyse de la menace, les vulnérabilités qui en résultent et les moyens d'y faire face.

A cet égard, les années 2014-2015 ont constitué un tournant, comme pour l'ensemble de la communauté nationale : menace terroriste à un niveau extrêmement élevé, attaques d'une importance jamais atteinte en France, apparition de nouveaux modes d'actions potentiels comme l'utilisation des drones, cibles de tous ordres plus ouvertes sur l'extérieur (non seulement les sites industriels mais aussi les transports collectifs et la population civile dans son ensemble). L'importation sur le sol national de scénarios et modes d'actions réservés jusqu'à maintenant à des Etats déstabilisés et à des zones de guerre (tels que prise d'otages massive, emploi d'engins explosifs improvisés) est désormais un fait. A ces menaces à caractère purement terroriste s'ajoutent les cyber-attaques et l'espionnage qui demeurent au sommet de l'échelle des risques pris en compte par les acteurs de la défense et de la sécurité nationale.

C'est dans ce cadre normatif et ce contexte de menaces que se joue donc le partenariat et le dialogue entre les opérateurs d'importance vitale du secteur des activités industrielles de l'armement et le ministère de la Défense. Vis-à-vis des OIV, ce dernier est organisé autour de trois acteurs principaux : la Direction de la Protection des Installations, moyens et activités de la Défense (DPID), la Direction Générale de l'Armement (DGA) et la Direction de la Protection et de la Sécurité de la Défense (DPSD).

Directement rattachée au ministre de la Défense et tête de chaîne ministérielle de la fonction « Défense-Sécurité », la DPID[7] est une instance de direction, de coordination et d'expertise, qui a pour mission de garantir au ministre que les installations, les moyens et les activités de la Défense sont protégés contre les actes malveillants ou hostiles, les atteintes au secret de la défense nationale et la cyber-menace.

7 *Décret n° 2015-1029 du 19 août 2015 relatif à la direction de la protection des installations, moyens et activités de la défense.*

La DPID élabore la politique générale de protection du ministère et en contrôle l'application. Cette mission est réalisée, notamment, sur la base de l'analyse des menaces produite par les services de renseignement, des vulnérabilités constatées sur les installations, moyens et personnel de la Défense ainsi que des capacités technologiques existantes en matière d'équipements de sécurité.

Elle coordonne les actions et constitue un échelon de synthèse pour les armées, directions et services sur les questions de défense et de sécurité, en liaison avec les grands subordonnés du ministre de la Défense que sont le chef d'état-major des armées (CEMA), le secrétaire général pour l'administration (SGA) et le délégué général pour l'armement (DGA). La DPID est un « fédérateur » au service des OIV, dont elle peut notamment relayer les préoccupations et les besoins aux niveaux ministériel et interministériel.

C'est précisément à travers le service de sécurité de défense et des systèmes d'information de la Direction générale de l'armement (DGA/SSDI) que s'exercent le pilotage et la coordination des OIV. La DGA va ainsi valider les PSO avant leur approbation par la DPID et approuver les PPP après avis de la DPID. Le rôle de la DGA vis-à-vis des entreprises est également primordial dans le domaine de la PPST et de la protection du secret : elle instruit les dossiers de création de zones à régime restrictif (ZRR) des industries d'armement ainsi que les demandes d'accès afférentes, forme les acteurs de la sécurité des entreprises, traite les demandes d'habilitation.

La DPSD, service de renseignement du ministère de la Défense, mais aussi d'enquête et d'inspection, contribue activement à la protection du personnel, des informations, du matériel et des installations sensibles du ministère et de certaines entreprises travaillant au profit du ministère.

En sus de la mission de contre-ingérence qui constitue le fondement de son action, la DPSD apporte son concours aux entreprises par :

- sa participation au contrôle du personnel (contrôles élémentaires, criblages par exemple) ;

- ses conseils techniques ;

- le contrôle des mesures prises en matière de protection et de sécurité générale, notamment vis-à-vis des entreprises titulaires de marchés intéressant la défense (et susceptibles de détenir des informations classifiées), des points d'importance vitale, des établissements détenant du potentiel scientifique et technique relevant du ministère de la Défense ;

- l'appui à la formation des officiers de sécurité et la sensibilisation du personnel en matière de sécurité.

Son maillage territorial assure en outre un lien de proximité avec les entreprises. Le champ d'intervention de chaque service est ainsi clairement défini. Par ailleurs, depuis fin 2015, l'animation « haute » du réseau des OIV relevant du ministère de la Défense a été relancée, avec par exemple l'organisation de commissions de défense et de sécurité spécifiques au secteur des activités industrielles de l'armement.

Des dispositifs complémentaires de protection des intérêts fondamentaux de la Nation

Les bases du domaine de la SAIV ayant été rappelées, il convient de décrire brièvement le dispositif de la protection du potentiel scientifique et technique (PPST) et celui de la protection du secret de la défense nationale, qui font également partie du corpus réglementaire visant à protéger les intérêts fondamentaux de la nation[8]. Ces dispositifs peuvent recouper partiellement la SAIV, bien que les actifs à protéger et les risques pris en compte soient différents.

La protection du potentiel scientifique et technique[9] a pour but de réunir les garanties optimales afin de protéger l'accès à celui-ci, lorsque le détournement ou la captation de savoirs, savoir-faire et technologies pourrait :

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

Ce potentiel est constitué de « l'ensemble des biens matériels et immatériels propres à l'activité scientifique fondamentale et appliquée, et au développement technologique ».

La protection du secret de la défense nationale[10] vise quant à elle à protéger « certaines informations [qui] présentent, en cas de divulgation, un risque tel d'atteinte à la défense et à la sécurité nationale que seules certaines personnes sont autorisées à y accéder. Considérer qu'une information présente ce risque conduit la puissance publique à la classifier, c'est-à-dire à lui conférer le caractère de secret de la défense nationale et à la faire bénéficier d'une protection juridique et matérielle stricte ».

Tentons d'établir, non pas des correspondances, mais un simple comparatif[11] entre quelques-uns des principaux éléments constituant les trois dispositifs considérés : SAIV, PPST, protection du secret.

Il apparaît assez clairement que des chevauchements, *a minima* géographiques, sont inévitables. Cette superposition de plusieurs réglementations peut sembler dans certains cas redondante, d'autant que chacune génère également des audits et inspections réguliers des services spécialisés.

A cet égard, l'Etat, soucieux d'éviter autant que possible les « mille-feuilles » administratifs, en a tenu compte en prévoyant certaines équivalences entre les dispositifs mis en œuvre par les entreprises pour satisfaire à leurs obligations de protection. Le fait est que, par exemple, un OIV mettant en œuvre un PPP sur une installation classée PIV au titre du dispositif SAIV répondra souvent, *de facto* et *de jure*, aux obligations découlant de la PPST et de la protection du secret. La réciproque est cependant moins vraie. De même, l'habilitation au secret de la défense nationale est valable pour accéder dans une ZRR sans autre autorisation. Enfin, les services de la

8 Citons également l'intelligence économique : circulaire du Premier ministre du 15 septembre 2011 concernant l'action de l'Etat en matière d'intelligence économique ; 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 »

9 Circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation, du 07 novembre 2012.

10 Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale du 30 novembre 2011 (IGI 1300).

11 Dont la pertinence n'engage que l'auteur de l'article.

	Sécurité des activités d'importance vitale	Protection du potentiel scientifique et technique	Protection du secret de la défense nationale
Fondement juridique	Art. R332-1 et suivants du code de la défense	Art. R413-5-1 du code pénal Décret n°2011-1425 du 2 novembre 2011	Art. R2311-1 et suivants du code de la défense
Menaces / risques principaux	Malveillance, terrorisme	Espionnage, terrorisme, prolifération	Espionnage, divulgation
Obligations principales de sécurité	Protection physique et logique	Protection physique et logique, autorisation d'accès renforcée	Protection physique et logique, habilitation
Cible locale des mesures de protection	PIV, composants névralgiques et SIIV	Biens matériels et immatériels constituant le potentiel scientifique et technique	Information et support classifiés[12] (ISC)
Zone juridique associée	Non formalisé	Zone à régime restrictif (ZRR)	Zone protégée (ZP) Zone réservée (ZR)
Plan de protection associé	PSO, PPP, PPE	Non formalisé	Dossier de sécurité de l'information
Responsable au sein de l'entreprise	Délégué à la défense et à la sécurité (DDS)	Chef de la ZRR	Officier de sécurité (OS)

Défense en charge des inspections, comme la DPSD, s'efforcent de traiter l'ensemble des dispositifs lors de leurs contrôles.

Par ailleurs, une même personne au sein de l'entreprise pourra exercer plusieurs fonctions (délégué à la défense et à la sécurité, officier de sécurité, responsable de la ZRR), facilitant de la sorte la mise en cohérence des dispositifs.

Conclusion

La liste de l'ensemble des enjeux, données et concepts susceptibles d'apparaître, à des degrés divers, dans le spectre des missions des responsables de la sûreté, en tant que facteurs de risque à prendre en compte pour assurer la protection de leur entreprise, est virtuellement infinie : activités d'importance vitale, infrastructures critiques, réseaux électrique ou de télécommunication, systèmes d'information, informations sensibles, sous-traitants, fournisseurs, clients, sécurité des approvisionnements (composants technologiques, matières rares, etc....) risque pays, terrorisme, malveillance, aléas, interdépendances entre les secteurs d'activités, continuité et reprise d'activité, résilience...

Pour certains de ces domaines, l'Etat a défini des politiques déclinées par chaque ministère en direction des entreprises dont ils assurent la coordination en matière de défense et sécurité nationale. Il s'agit donc non seulement de prioriser les risques comme les réponses, mais aussi d'assurer la cohérence des politiques et des dispositifs réglementaires entre eux. C'est ce que s'attache à faire le ministère de la Défense en partenariat, notamment, avec les opérateurs

12 *IGI 1300 : « procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier présentant un caractère de secret de la défense nationale (art.413-9 du code pénal) »*

d'importance vitale du secteur des activités industriels de l'armement. ■

Dominique Pierron,
chargé d'études à la Direction de la Protection
des Installations

Bibliographie

Livre blanc sur la défense et la sécurité nationale, La Documentation française, 2013.

Code de la défense, Journaux officiels.

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

A. Coursaget, « La sécurité des activités d'importance vitale : premier bilan du SGDSN. », Sécurité et stratégie 2/2010 (4), p. 5-17, novembre 2010-mars 2011.