

LES ACTIVITÉS INDUSTRIELLES DE L'ARMEMENT : UN SECTEUR D'IMPORTANCE VITALE



par **Jean-Marie Desmarts**, ICA

■ **Conseiller du SGDSN**

X1998 SupAéro, il commence sa carrière au CEV de Cazaux sur des bancs d'essais NG, puis comme chef de département informatique et exploitation. Il s'oriente alors vers les SIC et devient en 2009 directeur du programme RITA. Il poursuit au ministère de la défense avant de créer un département cybersécurité chez DCI. Il est depuis 2016 conseiller du SGDSN.



par **Bertrand Delmas-Marsallet**, ICA

■ **Adjoint au sous-directeur planification, SGDSN**

30 années d'expérience en France et à l'international dans les secteurs technologique (armement, spécialité missiles), stratégique (nucléaire, environnement) et politique (sécurité nationale, prévention de la radicalisation). Actuellement adjoint au sous-directeur de la planification de sécurité nationale, au sein du secrétariat général de la défense et de la sécurité nationale (SGDSN).

Activités, opérateurs, points d'importance vitale sont sans doute des concepts abstraits pour nombre d'entre vous. Ils relèvent pourtant d'une politique publique qui vient de fêter ses 10 ans : la sécurité des activités d'importance vitale ou SAIV, dont l'ambition première est d'assurer la continuité des activités essentielles à la défense, au fonctionnement de la Nation et, par nature, difficilement substituables ou remplaçables. Pour les activités industrielles de l'armement, cela se traduit concrètement aujourd'hui par 18 opérateurs d'importance vitale (OIV) responsables de 55 points d'importance vitale (PIV).

Conçu et piloté par le secrétariat général de la défense et de la sécurité nationale (SGDSN), le dispositif SAIV constitue le cadre permettant d'associer OIV, publics ou privés, à la mise en œuvre de la stratégie de sécurité nationale en termes de protection contre les actes de malveillance (terrorisme, sabotage) et les risques naturels, technologiques et sanitaires. Le Livre blanc de 2013 sur la défense et la sécurité nationale consacre cette politique comme un élément du renforcement de la résilience de la Nation.

Certains se souviennent peut-être du dispositif précédent autour des installations dites d'importance vitale et des points sensibles - PS1, PS2 et PS3 - qui comptait pas moins de 7000 sites. Ce dispositif a été rendu caduc par la fin de la guerre froide et par la montée en puissance du terrorisme dramatiquement incarnée par les attentats du 11 septembre 2001. Il a été remplacé en 2006 par la SAIV.

Au sein des activités militaires de l'État, les activités industrielles de l'armement constituent un sous-secteur à part entière, coordonné par la direction générale de l'armement (DGA) et doté d'une directive nationale de sécurité spécifique.

Le dispositif SAIV confère à l'opérateur d'importance vitale un statut particulier. Dans le cas des activités industrielles de l'armement : - la désignation du délégué à la défense et à la



En amont des programmes : la défense de l'industrie de défense.

sécurité au sein de l'entreprise. Interlocuteur habilité au niveau « Confidentiel défense », il est le destinataire unique des changements de posture du dispositif VIGIPIRATE ;

- la procédure dite de « criblage ». L'OIV peut demander à l'autorité militaire de vérifier que les caractéristiques de la personne souhaitant accéder à son PIV ne sont pas incompatibles avec la sécurité du site concerné ;

- le plan particulier de protection (PPP). Élaboré par l'OIV et approuvé par le délégué général pour l'armement, il décrit les dispositifs de protection physique mis en place au niveau du PIV ;

- le plan de protection externe (PPE). Élaboré par le préfet de département, il décrit et planifie les capacités humaines et matérielles de l'État pour intervenir sur le PIV. Il prévoit également les mesures de surveillance des zones périphériques.



Ces trois dernières années, sous l'impulsion du SGDSN, deux axes de renforcement de cette politique ont été mis en œuvre : la continuité d'activité et la sécurité des systèmes d'information.

Ainsi, le SGDSN a élaboré en interministériel et publié un guide méthodologique pour l'élabo-

ration d'un plan de continuité d'activité (PCA)². Il s'adresse à toutes les administrations et entreprises privées, proposant des aménagements pour tenir compte de la taille des entités.

Le 23 février 2016 a marqué le dixième anniversaire du dispositif de sécurité des activités d'importance vitale établi par décret. A cette occasion, un bilan a été dressé mais, surtout, les principales perspectives ont été dégagées.

Le premier axe est celui de la simplification des dispositifs, notamment en améliorant la cohé-

La SAIV en quelques chiffres


- 9 ministres coordonnateurs
- 12 secteurs d'activités
- 22 directives nationales de sécurité
- 249 opérateurs d'importance vitale
- 1369 points d'importance vitale
- 300 agents de l'État travaillant quotidiennement sur les questions de SAIV

La sécurité des systèmes d'information

L'article L. 2321 de la loi de programmation militaire dispose que :

« Pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'État peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque. Pour être en mesure de répondre aux attaques mentionnées au premier alinéa, les services de l'État déterminés par le Premier ministre peuvent détenir des équipements, des instruments, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs des infractions prévues aux articles 323-1 à 323-3 du code pénal, en vue d'analyser leur conception et d'observer leur fonctionnement. »

Les conditions sont en cours de précision par arrêté. 13 d'entre eux, sur un total de 22 arrêtés à caractère sectoriel, ont déjà paru. La mise en œuvre de ce dispositif a ainsi commencé le 1^{er} juillet dernier.

rence entre les politiques SAIV, de protection du potentiel scientifique et technique (PPST), de protection du secret de la défense nationale. Le second vise à renforcer le réseau d'acteurs par la mise en place de moyens de communication sécurisés, par l'offre de solutions de confiance élaborées dans le cadre des actions du comité de filière industrielle de sécurité (CoFIS³) et de la Nouvelle France industrielle. 

¹ En anglais Critical infrastructures protection (CIP)

² http://www.sgdsn.gov.fr/IMG/pdf/Guide_PCA_SGDSN_110613_normal.pdf

³ <http://www.gouvernement.fr/comite-de-la-filiere-industrielle-de-securite-cofis>





PROTECTIONS
THERMIQUES
DE SATELLITES



BALLONS
STRATOSPHERIQUES



BALLONS
CAPTIFS DE
SURVEILLANCE



TECHNOLOGIES
GONFLABLES
POUR STRATOBUS™



DIRIGEABLES
HYBRIDES

airstar-aerospace.com | +33 (0)4 76 13 12 20

www.madeinmouse.com