La cyberdéfense

Mise à jour : 30/04/2014 11:55 - Auteur : La rédaction

Priorité stratégique pour la souveraineté nationale, la cyberdéfense représente l'avenir de la Défense dans un milieu virtuel et sans frontière. Par le biais de nombreux acteurs, le ministère de la Défense participe activement à la protection et à la défense des systèmes d'information dans le cyberespace.

Présentation FIC DEFNET Portraits Pacte Défense Cyber **Organisatio**

L'organisation de la cyberdéfense française

Pour faire face aux risques et aux menaces qui pèsent sur des systèmes d'information devenus indispensables au fonctionnement de la Défense et aux missions conduites par les armées, le ministère s'est doté d'une organisation cyberdéfense. Plusieurs acteurs complémentaires travaillent ensemble, en collaboration avec différents partenaires, pour une cyberdéfense efficace et performante.

Les acteurs de la cyberdéfense

Une chaîne de commandement opérationnel interarmées et ministérielle, placée sous l'autorité du chef d'état-major des armées et intégrée au sein du Centre de planification et de conduite des opérations (CPCO), a été mise en place pour organiser et conduire la cyberdéfense militaire.

Un officier général a été désigné pour commander cette chaîne opérationnelle. Dans le cadre de ses attributions, il exerce une double fonction : sa responsabilité est à la fois opérationnelle au sein du CPCO, pour la planification, la coordination, et la conduite des opérations de défense des systèmes d'information du Ministère et des armées, et transverse, pour animer et coordonner les travaux relatifs au domaine de la cyberdéfense et à sa montée en puissance au sein des trois armées.

Pour une réaction rapide en cas de menace, le Centre d'analyse de lutte informatique défensive (CALID) est le bras armé du ministère de la Défense. En collaboration avec les autres entités ministérielles en charge de la sécurité informatique, il participe en permanence à la protection des systèmes d'information. Il surveille les réseaux du ministère, détecte les anomalies mettant en danger les systèmes d'information et agit en conséquence.

Le pendant technique de la cyberdéfense est confié à la Direction générale de l'armement (DGA), au pôle « sécurité des systèmes d'information ». En partenariat avec le monde industriel, la DGA-Maîtrise de l'information (DGA-MI) favorise l'innovation et le développement de solutions techniques inédites et performantes. De manière coordonnée, la DGA-MI approfondit la recherche selon cinq axes : cryptographie, méthodes formelles, sécurité des systèmes d'exploitation et des réseaux, électronique sécurisée et logiciels embarqués, analyses et manipulation des codes logiciels.

Le réseau cyberdéfense de la réserve citoyenne (RCC) a pour objectif de sensibiliser la Nation aux enjeux de la cyberdéfense. Le réseau de la RCC fonctionne sur le principe de groupes de travail, chacun mené par un chargé de mission. Chaque groupe opère sur une thématique définie : élus et journalistes, jeunes, évolution de l'engagement citoyen, thinks tanks et réflexion stratégique, petites et moyennes entreprises (PME/PMI), grandes entreprises et OIV.
Enfin, un travail étroit est assuré avec l'ensemble des services du ministère de la Défense en charge de la sécurité des systèmes d'information (opérateur, DPSD, etc).

Les partenaires du ministère de la Défense

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN), sous l'autorité du Premier ministre, constitue un partenaire privilégié et un soutien actif pour le ministère de la Défense.
En outre, le ministère de la Défense entretient un lien étroit avec le ministère de l'Intérieur, et le ministère des affaires Etrangères.
Les opérateurs d'importance vitale (OIV) liés à la défense et les industriels participants aux systèmes d'information de la Défense contribuent également à la protection des systèmes d'information.

Une coopération internationale est constamment entretenue avec l'OTAN, l'Union

européenne et d'autres organisations internationales. L'OTAN a adopté un concept de cyberdéfense en mars 2011. Pour promouvoir la coopération en matière de cyberdéfense, l'organisation a mis en place dès 2008 le centre d'excellence en cyberdéfense de Tallinn (NATO CCD COE), en Estonie. La France a adhéré à ce centre d'excellence et un officier français y est détaché depuis l'été 2013. De son côté l'Union européenne se dote peu à peu de structures visant à faire face aux menaces cybernétiques. L'ENISA (European Network Information Security Agency / Agence européenne chargée de la sécurité des réseaux et de l'information), basée à Héraklion en Crète, assiste les pays qui le souhaitent. La France construit un cercle très restreint de partenaires de confiance avec lesquels des échanges opérationnels très approfondis sont menés.

Enfin, des coopérations bilatérales sont développées avec les partenaires traditionnels du ministère de la Défense.