

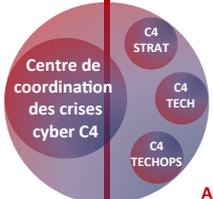
Communauté publique cyber française



*Primo-intervenants en cas de crise majeure



Le COMCYBER assure la protection des systèmes d'information placés sous la responsabilité du chef d'état-major des armées en sa qualité d'autorité qualifiée pour la sécurité des systèmes d'information et la conduite de la défense du ministère des Armées.



Agence nationale de la sécurité des systèmes d'information (ANSSI)*

Rôles : anticipation, détection de la menace, réponse aux incidents. Opération de cyberdéfense ouverte à ce niveau. Sous-direction des opérations (SDO) : assure au niveau opératif et tactique la défense des systèmes numériques d'intérêt pour la nation.



Rattaché à la préfecture de police de Paris, elle lutte contre la cybermenace à Paris et en petite couronne. Elle traite principalement des atteintes aux systèmes de traitement automatisés de données.



Rattaché à la Direction centrale de la police judiciaire (DCPJ), elle est en charge du pilotage et de la coordination de la lutte contre la cybercriminalité au plan national. Elle détecte les nouvelles menaces, aide les victimes et enquête afin de réprimer les crimes. (Pharos et Info escroqueries sont des plateformes de l'office central de lutte contre la criminalité liée aux technologies de l'information de la communication (OCLCTIC)



Direction générale de l'armement (DGA)

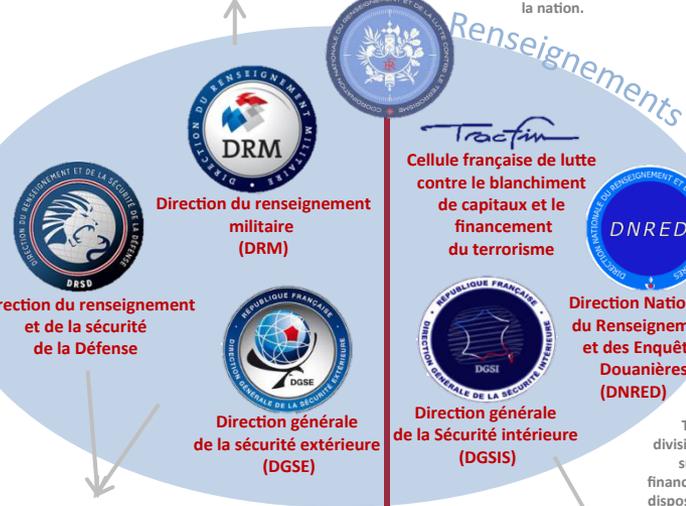
La DGA est le maître d'ouvrage des programmes d'armement. La DGA-Maîtrise de l'information (DGA-MI) est en charge de concevoir les armes cybernétiques au profit du ministère des Armées, que ce soit pour les services de renseignement ou pour les forces du COMCYBER



Commandement de cyberdéfense (COMCYBER)*

Pour l'exercice de ses missions, le COMCYBER dispose d'un état-major et a une autorité sur trois organismes interarmées : CALID, CASSI et CPROC

Au sein de la DRM, le Centre de recherche et d'analyse cyber concourt à informer, éclairer, renseigner les autorités dans leurs décisions, notamment relatives aux opérations sur théâtres extérieurs.



DGSE et DRSD assurent eux-mêmes la protection de leurs systèmes d'informations, en plus de leurs activités de renseignements s'agissant des menaces et enjeux du secteur de la défense



Réserve opérationnelle de cyberdéfense (RCD)*

Prévention, surveillance et répression des actes d'ingérence portant atteinte au potentiel économique, industriel et scientifique du pays.



Centre de lutte contre les criminalités numériques (C3N)

Rattaché au pôle judiciaire de la gendarmerie nationale (PJGN), est chargé d'identifier les phénomènes émergents et de conduire des investigations d'initiative sur internet. Il coordonne également le réseau des enquêteurs technologiques numériques (NTECH) et leurs correspondants (C-TECH)



INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE



Télécharger la RSC de 2018



Télécharger le LBDSN de 2013