

GESTION DE CRISE & CHÂÎNES CYBER : SYNTHÈSE DE L'ORGANISATION EUROPÉENNE ET FRANÇAISE LIÉE À LA SÉCURITÉ NUMÉRIQUE

DISPOSITIFS CYBER



Organisation du Traité de l'Atlantique Nord OTAN



La NATO Communications and Information Agency (NCIA), fournit aux pays de l'Alliance les moyens de communiquer. Elle est autan l'agence unique d'acquisition des moyens que l'opérateur interne Cyber de l'OTAN. La NCIRC lui est rattaché.



La Capacité OTAN de réaction aux incidents informatifs, la NCIRC coopère étroitement avec le CERT-EU. Forte de quelques 200 experts, elle assure la protection des SI de l'Alliance en temps de paix et en temps de crise. D'ici 2023, un Centre de cyberopérations (CVO) devrait être également intégré à la structure de commandement de l'OTAN.



Le Centre d'excellence de cyberdéfense coopérative, basé à Tallinn est le centre de l'OTAN spécialisé dans la recherche et l'éducation en élaborant notamment les règles de comportement dans le cyberspace et notamment la question de l'applicabilité du droit international aux cyberattaques employées dans le cadre de conflits armés via le "Manuel de Tallinn". Les exercices européens de cyberdéfense de l'OTAN: Cyber Coalition et Locked Shields y sont organisés.

Rattachée à l'Etat-major des Armées (EMA), il faut souligner le rôle de la Direction interarmées des réseaux d'infrastructure et des systèmes d'information (DIRISI) qui est un service interarmées. Son centre d'audits de la sécurité des systèmes d'information (CASSI) et le SOC DIRISI sont notamment impliqués dans la défense des SI du ministère des Armées, qu'elle conçoit, développe et protège. La DIRISI appuie le CPCO lors des opérations, mais également les armées et les autres directions et organismes.

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.

DSGE et DRSD assurent elles-mêmes la protection de leurs systèmes d'information, en plus de leurs activités de renseignement s'agissant des menaces et enjeux du secteur de la défense. La DRSD a également la responsabilité de la partie cyberdéfense concernant les SI concourant à la dissuasion.



Direction du renseignement militaire (DRM)
Direction générale de la sécurité extérieure (DSGE)
Direction du renseignement et de la sécurité de la Défense (DRSD)



État-major des Armées



Direction générale de l'armement (DGA)
Secrétariat général de l'administration (SGA)

La 807th compagnie de Transmissions (807th CRS), est une compagnie spécialisée en LID. Placée sous l'autorité fonctionnelle conjointe de l'Armée de Terre (mission Terra) et du COMCYBER (mission EMA). Elle contribue à la LID en opération.



L'ensemble des états-majors, directions et services (EMDS) rattachés au ministère des Armées, animent chacun une chaîne SSI et LID. Placés sous l'autorité fonctionnelle d'un OGCYBER (OCYBER Terre, Air, et ALCYBER pour la Marine). Les 3 armées disposent de centres techniques dédiés (ESIOC pour l'Armée de l'Air, CSC pour la Marine, CTUD pour l'Armée de Terre) et de SOC travaillant en étroite collaboration avec le GCA/CALID en mesure d'armer des GIC.



Armée Nationale



DIRISI

Le Conseil de l'Europe aide à protéger les sociétés contre les menaces de la cybercriminalité via le **Convention de Budapest**, qui reste encore aujourd'hui le cadre juridique international contraignant de référence pour les différentes législations nationales, mais aussi via son comité de la convention sur la cybercriminalité (T-CY) ou encore son bureau du programme sur la cybercriminalité (C-PROC).



En cas de crise ou incident majeur, la coordination pourra s'effectuer dans le cadre du système d'alerte rapide « ARGUS » au sein de la Commission, tandis que le Conseil de l'UE assure la coordination politique via le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR). Enfin, lorsque la crise comporte d'importantes implications liées à la politique extérieure ou à la politique de sécurité et de défense commune (PSDC), le système de réponse aux crises (SRC) du Service européen pour l'action extérieure (SEAE) pourra être activé, tout comme les services de renseignement, INT-CEN et EUMS INT, dans le cadre de la capacité unique du renseignement (SIAC).



Le COO évalue le niveau de menace dans le but de fixer ensuite le stade d'alerte de la chaîne défensive dans le cadre de la posture permanente de cyberdéfense (PPC). L'officier général commandant de la cyberdéfense (OGCYBER) fixe le stade d'alerte à adopter par la chaîne défensive, en lien avec le SCOPS de l'EMA et le HFCD5.



Rôles : anticipation, détection de la menace, réponse aux incidents. Opération de cyberdéfense ouverte à ce niveau. Sous-direction des opérations (SDO) : assure au niveau opérationnel et tactique la défense des systèmes numériques d'intérêt pour la nation. Le CERT-FR est le CERT national, il est le point de contact international privilégié pour tout incident de nature cyber touchant la France. Il assure une permanence de ses activités 24h/24, 7j/7.



RZSSI
COZ



COD
RSSI



RSSI
PCO



RSSI
PCO



RSSI
PCO



RSSI
PCO



RSSI
PCO



RSSI
PCO



CIC



SGDSN



ANSSI



ANSSI



ANSSI



ANSSI



ANSSI



ANSSI



ANSSI



ANSSI



ANSSI



ANSSI



ANSSI



ANSSI



ANSSI



Conseil de l'UE



Commission européenne



CSIRT's NETWORK



ENISA



ENISA



ENISA



ENISA



ENISA



ENISA



ENISA



ENISA



ENISA



ENISA



ENISA



ENISA



ENISA



ENISA



ENISA



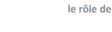
ENISA



ENISA



ENISA



ENISA



ENISA

La Commission a adopté en 2017 une recommandation : le **Blueprint**, définissant les procédures de coopération et d'échanges européens pour la gestion des incidents majeurs et des crises cyber. Le commissaire au marché intérieur est en charge du renforcement de la cybersécurité de l'Europe, la sécurité des réseaux et des systèmes d'information, des mécanismes d'urgence en cas de cyber-incident et le déploiement de l'unité commune pour la cybersécurité (Joint Cyber Unit).



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



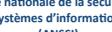
CERT-EU



CERT-EU



CERT-EU



CERT-EU



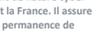
CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



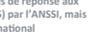
CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU



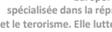
CERT-EU



CERT-EU



CERT-EU



CERT-EU



CERT-EU

