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

DISPOSITIFS CYBER

DISPOSITIFS DE CRISE

Organisation du Traité de l'Atlantique Nord OTAN

Le Conseil de l'Europe aide à protéger les sociétés contre les menaces de la cybercriminalité via la **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**).

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).

L'Alliance a pour principale fonction la défense collective, la gestion de crise et la sécurité coopérative. Des équipes de réaction rapide de l'OTAN peuvent intervenir 24 h/24 au nom de la clause d'assistance mutuelle de l'article 5 du traité de l'Atlantique nord (TAN).

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

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 assurera 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, INTCEN et EUMS INT, dans le cadre de la capacité unique du renseignement (SIAC).

L'État-major de l'UE (EMUE), structure militaire intégrée à l'UE, est en mesure de fournir une expertise militaire et opérationnelle via sa division politique et plans (CON/CAP) et sa division des systèmes d'information et de commandement (CIS). Mais ce sont les structures de planification existantes qui ont la charge de la conduite opérationnelle cyber dans les opérations ou le **MPCC** pour les opérations à mandat non exécutif.

Union Européenne **ACTION EXTÉRIEURE**

Le "**CERT-EU**", Computer Emergency Response Team de l'UE intervient en cas d'urgence informatique via une équipe permanente au profit des institutions européennes. Il coopère notamment avec les CERTs des États membres. Le **CSIRTs Network** est le réseau des CERT européens.

L'Agence européenne de la sécurité des réseaux et de l'information (**ENISA**) conseille et assiste la Commission et les États membres en matière de sécurité de l'information. Son rôle se renforce, notamment en matière de certification et d'organisation d'exercices.

Europol est l'agence européenne spécialisée dans la répression de la criminalité internationale et le terrorisme. Elle lutte contre la cybercriminalité, notamment via l'European Cybercrime Centre (**EC3**) qui opère à un niveau stratégique mais également opérationnel, notamment via le Joint Cybercrime Action Taskforce (**J-CAT**).

L'European Union Agency for Criminal Justice Cooperation (Eurojust) a pour principales missions la coordination des enquêtes et des poursuites, et la coopération entre les autorités des États membres. Elle cherche à rendre plus efficaces ces enquêtes et poursuites, notamment en matière de lutte contre la cybercriminalité.

Soutenu par Eurojust, L'European Judicial Cybercrime Network (**EJCN**) forme un réseau de procureurs et de spécialistes du cybercrime. Il vise a rendre plus efficace les enquêtes et poursuites engagées en matière de cybercrime en améliorant la coopération entre autorités judiciaires des États membres.

La Capacité OTAN de réaction aux incidents informatiques, 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 des cyberopérations (CyOC) 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 cyberespace 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 cybedéfense de l'OTAN: Cyber Coalition et Locked Shields y sont organisés.

Comité directeur de la cyberdéfense (DIRCAB PM, CEMP, SGDSN, Min X)

Comité de pilotage de la cybersécurité (DIRCAB PM, ANSSI, Min X)

PREMIER MINISTRE

Le Centre de Cyberdéfense (C2MI) relevant du SHFD assure la défense des SI du ministère de l'Intérieur. Il assure la détection des attaques et coordonne la gestion des incidents de sécurité en lien avec l'ANSSI.

Le MEAE assure le lien avec les homologues étrangers. Il s'appuie sur son Centre de crise et de soutien (CDCS), la Cellule interministérielle d'aide aux victimes (CIAV), mais également le réseau de diplomates en ambassades et consulats.

La cellule de crise JUSTICE est animée par le HFDS qui est responsable de la sécurité et la résilience du secteur d'activités d'importance vitale des activités judiciaires (SAIVAJ).

Le COBER, est le centre opérationnel de Bercy, mis en œuvre par le service du Haut fonctionnaire de défense et de sécurité. Il conduit l'action du réseau de gestion de crise des ministères économiques et financiers. Si la crise a un fort impact sur la vie économique de la Nation, le ministre de l'économie et des finances décide de mettre en œuvre la cellule de continuité économique (CCE).

Le FSSI des ministères sociaux pilote la cellule d'Accompagnement Cybersécurité des Structures de Santé » (ACSS), structure nationale d'assistance et d'appui pour les ARS et autres structures de santé. Le FSSI peut compter sur l'agence du numérique en santé et le portail https://www.cyberveille-sante.gouv.fr. Les signalements remontent également des ARS vers l'ASIP Santé via l'ACSS et notamment grâce au portail signalement.social-sante.gouv.fr.

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 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 cybersécurité concernant les SI concourant à la dissuasion.

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 3 armées et les autres directions et organismes.

Le CCO 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 HFCDS.

CIC

CPCO **FSSI**

Direction du renseignement militaire (DRM)

Direction générale de la sécurité extérieure (DGSE)

Direction du renseignement et de la sécurité de la Défense (DRSD)

État-major des Armées

Direction générale de l'armement (DGA)

Secrétariat général pour l'administration

Centre de coordination des crises cyber C4

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.
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.

Prestataire de réponse aux incidents de sécurité qualifiés (PRIS)

Le secteur privé est fortement impliqué en matière de défense des SI, en témoigne la mise en place de la qualification des prestataires de réponse aux incidents de sécurité qualifiés (PRIS) par l'ANSSI, mais également le dispositif national
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique
de prevention du risque numerique et d'assistance aux victimes piloté par le GIP ACYMA qui permet la mise en relation entre victimes (TPE/PME et citoyens) et services professionnels de sécurité informatique ou bien la Brigade du numérique (BNUM) de la gendarmerie nationale.
À noter la naissance du label pour la reconnaissance des services de sécurité informatique et le rôle de la recherche dans le développement des capacités de réponse.

RZSSI **COZ**

SGZDS

COD **RSSI**

PREFECTURE

RSSI **PCO**

MAIRIE

COGIC **FSSI**
COPN **C2MI**
CROGEND

Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI)

Rattachée 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.

Sous-direction de la Lutte contre la Cybercriminalité (SDLC)

Rattachée 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.

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.

Le C3N coordonne également le réseau CyberGEND, composé d'enquêteurs technologies numériques (NTECH), de correspondants (C-TECH) et de primo-intervenant (P-NTECH).

Division Analyse & Anticipation

Le C-SIRT-POLICE JUDICIAIRE est rattachée à la D2A.

Office central de lutte contre la criminalité liée aux technologies de l'information de la communication (OCLCTIC)

L'OCLCTIC gère PHAROS et THESEE.

Direction générale de la Sécurité intérieure (DGSI)

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

Elle possède un rôle en matière judiciaire, mais également en matière de défense des SI des OIV, OSE et des réseaux gouvernementaux.

Tribunal judiciaire de Paris

La **Section J3 Cybercriminalité** du Parquet de Paris est l'une des trois juridictions interrégionales spécialisées (JIRS) au côté de la section J1 JIRS criminalité organisée et la section J2 JIRS criminalité financière.
Cette division composée de 3 magistrats est en charge des contentieux de très haut vol, de complexe à très complexe, comme ceux relatifs à WannaCry et NotPetya.

La section J3 s'appuie également sur quatre juges d'instruction du pôle financier de Paris formés aux problématiques cyber.

Direction Nationale du Renseignement et des Enquêtes Douanières (DNRED)

La DNRED dispose d'un service spécialisé : Cyberdouane.

Cellule française de lutte contre le blanchiment de capitaux et le financement du terrorisme

Tracfin dispose d'une division d'enquête spécialisée sur la cybercriminalité financière.

Un réseau de magistrats « cyber-référents » opèrent au sein des tribunaux, cours d'appel et JIRS.
La Mission de lutte contre la cybercriminalité de la direction des affaires criminelles et des grâces (DACG) du ministère de la justice contribue aux travaux stratégiques du C4 mais également aux réunions du Groupe de Contact permanent (GCP). piloté par la DMISC.

La Police et la Gendarmerie nationale ont développé des plateformes dédiées à la prise en compte des incidents cyber pour les collectivités, les TPE et PME et les particuliers.

PERCEV@L

En cas d'une attaque qualifiée de terroriste, le parquet de Paris peut saisir la sous-direction anti-terroriste (SDAT), qui dispose d'une compétence judiciaire nationale.

Commandement de cyberdéfense (COMCYBER)

La 807ème compagnie de Transmissions (807e CTRS), est une compagnie spécialisée en LID. Placée sous l'autorité fonctionnelle conjointe de l'armée de Terre (mission Terre) 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 chaine SSI et LID. Placés sous l'autorité fonctionnelle d'un OGCYBER (OGCYBER 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, CTLID pour l'Armée de Terre) et de SOC travaillant en étroite collaboration avec le GCA/CALID et en mesure d'armer des GIC.

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. Elle peut également appuyer le GCA/CALID ou être chargée de certaines tâches d'expertise technique, notamment via son pôle SSI.

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. Pour l'exercice de ses missions de **lutte informatique défensive (LID)**, le COMCYBER dispose d'un état-major et d'un centre cyber opérationnel (CCO) et a une autorité sur différents organismes spécialisés:
le groupement cyberdéfense des armées (GCA) qui regroupe le GCA/CALID, GCA/CRPOC, GCA/CASSI ; les groupements d'intervention cyber (GIC) et SOC. A noter également : les activités de **lutte informatique Offensive (LIO)** désignant l'ensemble des actions entreprises dans le cyberespace visant à produire des effets à l'encontre d'un système adverse, pour en altérer la disponibilité ou la confidentialité des données.

PÔLE D'EXCELLENCE CYBER

Pôle d'Excellence Cyber (PEC) et CyberDefense Factory, sont deux exemples qui témoignent del'importance du partenariat public-privé en matière de cybersécurité et cyberdéfense. Sans oublier la convention cyber impliquant 8 grands maîtres d'œuvre industriels et principaux équipementiers du ministère afin de construire une chaîne cyber défensive « de bout en bout ».

FSSI = Fonctionnaire de la sécurité des systèmes d'information, nommé par le HFDS
RZSSI = Responsable zonal de la sécurité des sytèmes d'information
RSSI = Responsable de la Sécurité des systèmes d'information

Infographie réalisée par **Martial LE GUÉDARD**
Consultez l'article en cliquant **ici**.