FOCUS

# Organisation de l'État français en gestion de crise cybernétique majeure

par Martial Le Guédard

RÉSUMÉ

La France s'est dotée de capacités de réponses face à la cybermenace et à la cybercriminalité. Un schéma de réponse se dessine en cas de crise majeure d'origine cybernétique, c'est-à-dire en cas de crise provoquée par la mise à mal de systèmes d'information comme ce fut le cas pour nombre d'entreprises et d'administrations françaises ces dernières années. Pourtant, des interrogations subsistent quant au schéma organisationnel de réponse. Le périmètre de chacune des institutions gagnerait à être précisé, spécifié, mais surtout partagé et connu de tous.
Cet article a pour vocation de partager une première ébauche d'un travail de cartographie des acteurs qui devra évoluer dans les mois à venir pour intégrer les retours permis par sa publication ainsi que pour y intégrer le volet européen et international si pertinent lorsque l'on souhaite aborder la gestion des crises provenant de cet espace transfrontière qu'est l'espace numérique.

**Cybersécurité / cyberdéfense : quelle organisation pour l'État français ?**

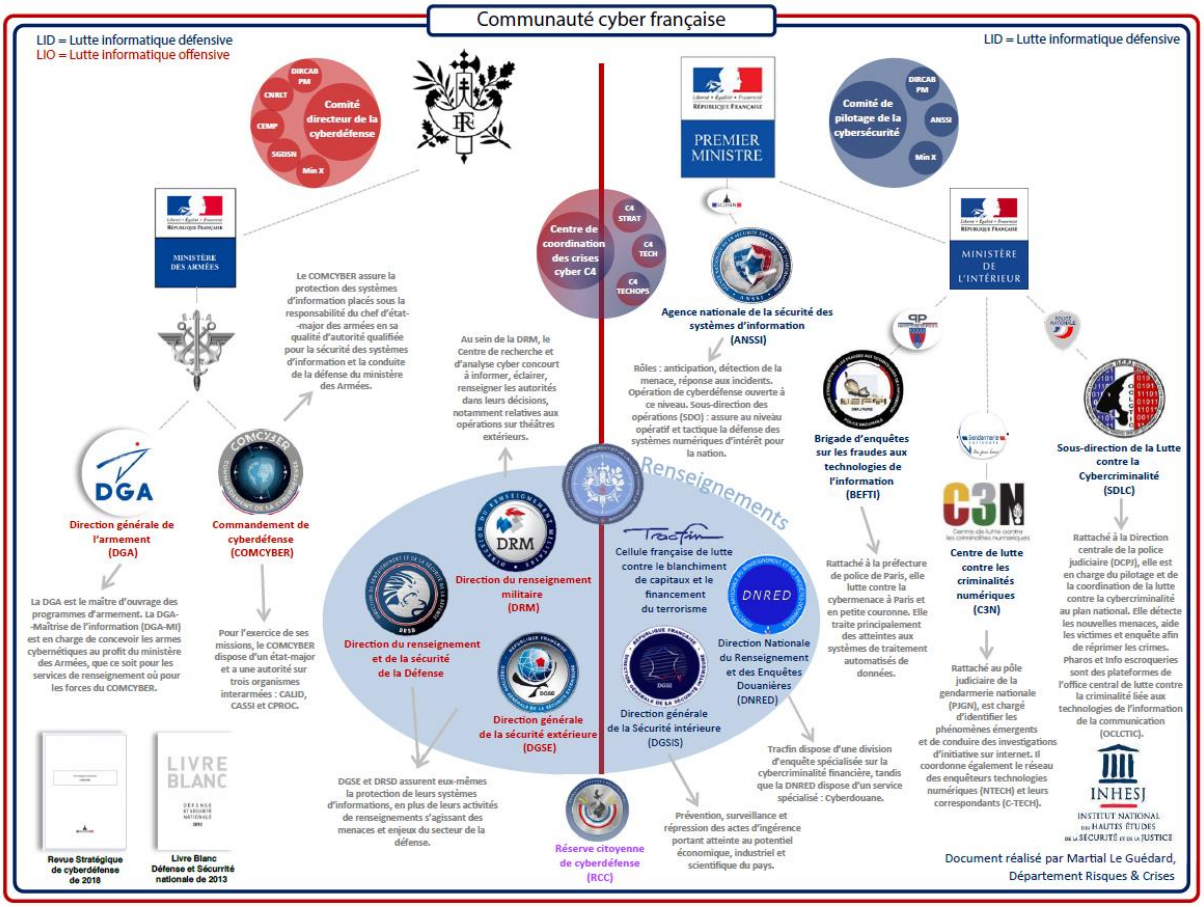
Présentée comme le « premier grand exercice de synthèse stratégique dans ce domaine », la Revue stratégique de cyberdéfense[1] (RSC) publiée en février 2018 par le Secrétariat général à la défense et la sécurité nationale (SGDSN) affirmait le cadre organisationnel et sommital français en matière de cyberdéfense et cybersécurité. Pourtant, il n'en demeure pas moins difficile d'établir une cartographie précise des acteurs institutionnels - compétents – amenés à répondre aux crises cybernétiques majeures.

La création de scénarios de crise axés sur la cybersécurité au sein du département « risques et crises » de l'Institut national des hautes études de la sécurité et de la justice (INHESJ) en lien avec l'ANSSI et l'animation d'exercices de crise et de media training a permis de questionner l'organisation gouvernementale des instances et échelons de gestion de crise en fonction des chaînes de responsabilité afférentes.

Si les périmètres d'action semblent bien définis, la connaissance de ces derniers par les acteurs et les décideurs en gestion de crise – hors acteurs techniques du champ de la sécurité, et plus spécifiquement de la sécurité informatique – reste trop peu développée. Cette méconnaissance pourrait contraindre une réponse non adéquate en temps de crise.

Cette première ébauche de cartographie des acteurs a vocation à être amendée dans les mois à venir pour intégrer les retours permis par sa publication ainsi que pour y intégrer le volet européen et international si pertinent lorsque l'on souhaite aborder la gestion des crises provenant de cet espace transfrontière qu'est l'espace numérique.

[1] http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/




**Rappel du particularisme du modèle de gouvernance français : la séparation des capacités défensives et offensives**

Le modèle français d'organisation de la réponse aux incidents numériques repose sur la séparation entre le volet offensif (lutte informatique Active, LIA) et défensif (lutte informatique Défensive, LID).

La **LIA**, c'est-à-dire la stratégie offensive, est la prérogative de l'Elysée *via* le Conseil de défense et de sécurité nationale (CDSN) qui est en charge de produire les orientations et directives dans le domaine cyber. C'est le Comité de direction de la cyberdéfense (CDC) qui les met en œuvre en allouant aux services étatiques les moyens nécessaires. Co-présidé par le coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT), le chef d'état-major particulier du Président de la République (CEMP) et le directeur de cabinet du Premier ministre, le CDC est également en charge de coordonner les diverses chaînes opérationnelles – cyberdéfense, contre-ingérence cyber, répression.

L'arme informatique est donc un usage souverain. La Direction générale de l'armement-Maîtrise de l'information (DGA-MII) est en charge de concevoir ces armes cybernétiques au profit du ministère des Armées, que ce soit pour les services de renseignement où pour les forces du COMCYBER.
Créé en 2017, le commandement des forces de cyberdéfense des armées françaises (COMCYBER)[2] 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. Il assure également la conduite de la défense des systèmes d'information du ministère des Armées à l'exclusion de ceux de la direction générale de la sécurité extérieure (DGSE) et de la direction du renseignement et de la sécurité de la défense (DRSD). Si le COMCYBER a autorité sur 3 organismes interarmées – que sont le Centre d'analyse en lutte informatique défensive (CALID), le Centre d'audits de la sécurité des systèmes d'information (CASSI) et le Centre de la réserve et de la préparation opérationnelle de cyberdéfense (CPROC) – le CALID en est le bras armé en tant que centre

[2] https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation

opérationnel défendant l'espace numérique des armées. Le COMCYBER s'appuie sur le centre des opérations cyber (CO Cyber) pour orienter le travail du CALID et des SOC[3].

La **LID**, c'est-à-dire la stratégie défensive, est la prérogative du Premier ministre via le Comité de pilotage de la cybersécurité (CPC) dirigé par l'ANSSI, autorité nationale de défense des systèmes d'information[4] qui a à sa charge l'organisation de la réponse et le pilotage des opérations en cas d'attaque informatique majeure contre la Nation. Il s'agit de l'institution en charge de la réponse à incident en cas de crise majeure. Plus précisément, c'est la sous-direction des opérations (SDO) de l'ANSSI qui joue un rôle opérationnel lorsque surviennent des crises d'origine cyber : 14 opérations de cyberdéfense ont ainsi été menées en 2018[5].

En fonction de l'importance de la crise, le plan Piranet[6] et la cellule interministérielle de crise (CIC) seront ou non activés par le Premier ministre, et le directeur général de l'ANSSI en prendra la tête. La direction générale de la sécurité intérieure (DGSI), pourra venir en appui pour mener l'enquête. La création du centre de coordination des crises cyber (C4) souhaitée de ses vœux par la RSC assoie l'importance des échanges et du soutien interministériel et inter-service nécessaire pour préparer la doctrine de réponse en cas d'attaque – doit-on attribuer les cyberattaques ? Que faire le cas échéant ? Jusqu'à quel niveau d'escalade ? Etc. – mais également pour faciliter la réponse opérationnelle, notamment via le C4 TECH qui assure le partage d'information et le dialogue entre acteurs.

A ce titre, l'ANSSI a renforcé ses partenariats public-privé, avec plusieurs autorités nationales sectorielles[7] : l'Autorité de contrôle prudentiel et de résolution (ACPR), l'Autorité des marchés financiers (AMF), l'Établissement public de sécurité ferroviaire (EPSF), la Direction de la sécurité de l'aviation civile (DSAC). Elle continue son travail auprès des opérateurs d'importance vitale (OIV), des opérateurs de services essentiels (OSE), des fournisseurs de service numérique (FSN) et peut à présent s'appuyer sur les opérateurs de communications électroniques (OCE) pour détecter les attaques.

Les liens entre les organismes préposés à la LIA et ceux préposés à la LID restent néanmoins serrés puisque CALID comme DGA-MII partagent avec l'ANSSI les savoirs qui lui permettent de protéger l'espace numérique français.

### Cybercriminalité : un maillage territorial, des capacités de réponses

Alors que le cybercrime agit quotidiennement sans émettre de bruit médiatique, il est prioritairement la prérogative d'autres institutions que l'ANSSI et le ministère des Armées. En effet, la lutte contre la cybercriminalité est principalement le fait du ministère de l'Intérieur, mais également du ministère de l'Action et des Comptes publics.

Au sein du ministère de l'Intérieur, trois institutions agissent quotidiennement pour lutter contre la cybercriminalité : la Police nationale *via* la Sous-direction de la lutte contre la cybercriminalité (SDLC)[8], la Préfecture de police *via* la brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI)[9] et enfin la Gendarmerie nationale *via* son centre de lutte contre les criminalités numériques (C3N)[10].

---

[3] https://www.defense.gouv.fr/salle-de-presse/dossiers-de-presse/dossier-de-presse_politique-ministerielle-de-lutte-informatique-defensive

[4] https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Communique_de_presse_strategie_publique.pdf

[5] https://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/

[6] https://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/

[7] https://www.ssi.gouv.fr/uploads/2019/04/anssi_rapport_annuel_2018.pdf

[8] https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite

[9] https://www.prefecturedepolice.interieur.gouv.fr/Cybersecurite/Les-actions-PP/Les-brigades-de-police-judiciaire/La-BEFTI

[10] https://www.gendarmerie.interieur.gouv.fr/pjgn/SCRCGN/Le-centre-de-lutte-contre-les-criminalites-numeriques-C3N

La SDLC est notamment composée d'un bureau de coordination stratégique, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), et une division en charge de l'anticipation et de l'analyse (D2A). C'est cette dernière qui a « vocation à construire une réponse publique aux particuliers et aux entreprises non identifiées comme des « opérateurs d'importance vitale » et cibles privilégiées des cyber-attaques »[11].
La BEFTI exerce, elle, sa compétence sur le ressort de Paris et de la petite couronne, sous l'autorité des Procureurs de la République et des juges d'instruction. Service de police judiciaire rattachée à la Direction centrale du renseignement intérieur (DCRI) au sein de la Préfecture de Police de Paris et spécialisé dans la lutte contre la cybercriminalité, la Brigade et ses Investigateurs en CyberCriminalité (ICC) apporte aussi son soutien technique et matériel aux autres services de la police judiciaire et aux commissariats du ressort.
Enfin, au sein du C3N, la chaîne cybercriminalité bénéficie d'un réseau de proximité au niveau local composé de référents Cyber, de spécialistes au niveau départemental (Cyber N'tech). Des experts travaillent également à l'échelle nationale au sein du Pôle judiciaire de la Gendarmerie nationale (PJGN) qui réunit les compétences du C3N mais aussi du département informatique et électronique de l'Institut de recherche criminelle de la Gendarmerie nationale (IRCGN).
Le C3N travaille essentiellement d'initiative et assure le pilotage et l'appui spécialisé de l'action de la Gendarmerie contre la cybercriminalité et les criminalités numériques de façon plus générale. Il mène et coordonne les investigations d'ampleur nationale ayant trait à la cybercriminalité et réalise une surveillance permanente de l'Internet pour y détecter et collecter les preuves des infractions qui peuvent y être commises. Le réseau d'enquêteurs spécialisés de la Gendarmerie forme une chaîne globale et cohérente de 3 500 gendarmes. Le C3N pilote et anime le réseau CYBERGEND, composé de 3 500 gendarmes spécialisés en technologie numérique.[12]

Au sein du ministère de l'Action et des Comptes publics, deux institutions agissent contre la criminalité numérique : la Direction nationale du renseignement et des enquêtes douanières (DNRED) et l'organisme de Traitement du renseignement et action contre les circuits financiers clandestins (Tracfin).
La DNRED[13] dispose d'un service spécialisé nommé cellule Cyberdouane, en charge de la détection des fraudes douanières sur Internet. Sur la base de son travail de veille, la cellule Cyberdouane est amenée à diligenter des enquêtes menées par la DNRED dans le cas d'une procédure administrative ou le Service national de douane judiciaire (SNDJ) dans le cas d'une procédure judiciaire.
Tracfin[14] est en charge de la lutte contre la fraude, le blanchiment d'argent et le financement du terrorisme. À ce titre, il dispose d'une division d'enquête spécialisée sur la «cybercriminalité financière ».

### Gestion de crise majeure d'origine cyber : quelle articulation du dispositif institutionnel ?

Ainsi le dispositif institutionnel de gestion des incidents cyber est déjà particulièrement structuré, avec notamment des espaces de discussions interministérielles, un plan dédié, des périmètres d'intervention pour les différents acteurs des chaînes de responsabilité afférentes. Néanmoins, la méconnaissance de ces dernières par les acteurs et les décideurs en gestion de crise – hors acteurs techniques du champ de la sécurité, et plus spécifiquement de la sécurité informatique – reste un frein pour la mise en œuvre d'une réponse optimale à la crise. En effet, comment alerter, lorsque l'on ne connaît pas qui doit l'être et qui est en mesure d'apporter son soutien ?
C'est pourquoi la réalisation d'un document unique de cartographie des acteurs est apparue nécessaire pour participer à la sensibilisation des acteurs de gestion de crise.

Le développement de scénarios de crise majeure d'origine cybernétique, impactant notamment des systèmes industriels (SCADA), a ainsi permis de questionner les capacités de réponse des services de l'État sur l'ensemble du territoire, mais également en fonction de scénarios multi-acteurs face auxquels les ressources de la seule ANSSI pourraient ne pas être suffisantes.

---

[11] https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite
[12] https://www.gendarmerie.interieur.gouv.fr/pjgn/SCRCGN/Le-centre-de-lutte-contre-les-criminalites-numeriques-C3N
[13] https://www.douane.gouv.fr/fiche/la-direction-nationale-du-renseignement-et-des-enquetes-douanieres
[14] https://www.economie.gouv.fr/tracfin

La question territoriale entre en compte, alors que les services de sécurités informatiques de l'État sont principalement présents en région parisienne. L'ANSSI qui concentre son activité sur les opérateurs d'importance vitale (OIV) et les opérateurs de services essentiels (OSE), ne possède pas de maillage territorial en région – si ce n'est la présence de 13 délégués territoriaux[15] – contrairement aux services de la Police nationale et de la Gendarmerie.

Ainsi, en cas de crise majeure impliquant différents services de l'État (une préfecture par exemple), des systèmes d'information essentiels (SIE) d'un OIV (un système industriel par exemple), mais également des sites non classés OIV, OSE ou Seveso, comme des salles de concerts ou de spectacles, quel(s) acteur(s) serai(en)t amener à prendre la main ? Les services de la SDLC la conserveraient-ils, s'ils étaient les premiers à avoir été sollicités par la société en question ? L'ANSSI assurerait-elle la conduite de toutes les opérations dès lors que la conscience de la situation permettrait d'évaluer l'ampleur de l'attaque ? Le délégué territorial de l'ANSSI pourrait-il être projeté au sein du Centre opérationnel départemental (COD) aux côtés des acteurs de la gestion de crise de la préfecture ? Les CYBERGEND, ou commissaires spécialisés sur les questions de cybersécurité pourraient-ils être projetés en COD pour éclairer le décideur public que représente le préfet et / ou assurer une liaison avec les services de l'ANSSI ?

La France s'est aujourd'hui dotée d'un paysage d'acteurs performants et complémentaires, il est maintenant du devoir de l'État – pour assurer sa mission régalienne de sécurité des Français – de s'interroger sur l'articulation opérationnelle et stratégique de ce dispositif en cas de crise majeure d'origine cybernétique.

[15] https://www.ssi.gouv.fr/agence/cybersecurite/action-territoriale/

# A PROPOS DE L'AUTEUR

## Martial LE GUÉDARD

Martial Le Guédard est chargé de mission Gestion de Crise – Environnement numérique au sein du Département Risques et Crises de l'Institut national des hautes études de la sécurité et de la justice (INHESJ), Service du Premier ministre. Il développe et porte la thématique cyber dans les formations et scénarii d'exercices de gestion de crise pour des partenaires publics et privés. Diplômé de l'Institut Français de Géopolitique (IFG), il s'est spécialisé sur les problématiques liées au cyberespace et s'intéresse au développement d'un numérique responsable et sécurisé. Il a travaillé pour différents cabinets de conseil en sûreté et cybersécurité auprès de clients publics – Ministères des armées notamment – et privés, principalement auprès d'EDF. Il officie par ailleurs en tant que Superviseur de rédaction du Pôle Cyber au sein du CESED – Centre d'Études de la Sécurité et de la Défense – un Think Tank, qui élabore des propositions dans les domaines de compétence de la sécurité et de la défense.