



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Objectifs et règles de sécurité numérique du ministère de l'Intérieur

PGSN – B05

**Dispositif opérationnel de cyberdéfense et
plan ministériel de gestion de crise cyber**

Version 0.7

(ce document doit être mis à jour en fonction du retour d'expérience de l'exercice Piranet 22)

TABLE DES MATIERES

1. Dispositif opérationnel de cyberdéfense du ministère de l'Intérieur	4
1.1. Le mode nominal	4
1.2. Le mode « dispositif renforcé »	4
1.3. Le mode « crise ministérielle cyber »	5
1.4. Le déclenchement du plan PIRANET	5
2. Fonction au sein du dispositif opérationnel de cyberdéfense	6
2.1 Direction du dispositif (fonction activée dès le mode nominal)	6
2.2 Coordination du dispositif et appui à la conduite (fonction activée à partir du mode renforcé)	6
2.3 Connaissance de la situation (fonction activée dès le mode nominal) ..	7
2.4 Management de l'information (fonction activée à partir du mode « dispositif renforcée »)	7
2.5 Logistique (fonction activée à partir du mode gestion de crise)	8
2.6 Communication (fonction activée à partir du mode renforcé)	8
2.7 Retour d'expérience (fonction activée à partir du mode renforcé)	9
3. Interactions du dispositif de gestion de crise cyber	10
3.1 Interaction avec les équipes opérationnelles du numérique	10
3.2 Interactions avec les autorités qualifiées	10
3.3 Interactions avec le niveau zonal	11
3.4 Interactions avec la DGSI	11
3.5 Interactions avec les autres dispositifs de gestion de crise au sein du ministère	11
3.6 Interactions avec l'ANSSI et les autres ministères	11
4. Moyens et outils de gestion de crise	12
4.1 Documentation	12
4.2 Annuaire	12
4.3 Moyens de communications	12
5. Actions immédiates et armement des fonctions	13
5.1 Armement des fonctions en mode nominal	13
5.2 Actions immédiates et armement des fonctions en mode « dispositif renforcé »	14

5.3	Actions immédiates et armement des fonctions en mode « dispositif renforcé »	15
6.	Plan de remédiation technique	18
6.1	Construction	18
6.2	Validation	18
6.3	Communication	18
6.4	Suivi	18
7.	Dépôt de plainte	18
8.	Annexes	19
8.1	Annexe 1 : Phase d'une crise cyberdéfense	19
8.1.1.	Synoptique – vision global du processus de crise	19
8.1.2.	Phase 1 – Alerte	19
8.1.3.	Phase 2 – Gestion de la crise	19
8.1.4.	Phase 3 – Retour à la normale	19
8.1.5.	Phase 4 – Retour d'expérience	19
8.2	Annexe 2 : Organisation ministérielle de gestion de crise cyber	20
8.3	Annexe 3 : Organisation gouvernementale de gestion de crise cyber	21

1. Dispositif opérationnel de cybersécurité du ministère de l'Intérieur

La politique générale de sécurité numérique du ministère de l'intérieur (PGSN-MI) dote le ministère de trois objectifs stratégiques :

- 1 Éviter la déstabilisation des missions du ministère, en se préparant aux attaques ciblées et sophistiquées dont il fait l'objet.
- 2 Rendre indolores les très nombreuses cyberattaques d'intensité moyenne contre le ministère et son écosystème numérique.
- 3 S'attacher à intégrer le risque numérique dans l'organisation et les procédures internes du ministère, en particulier dans la gestion de crise.

En s'appuyant sur un dispositif opérationnel de cybersécurité capable de s'adapter au niveau de menace, le ministère de l'intérieur peut apporter une réponse adaptée à l'ensemble des incidents et des événements, des plus anodins aux plus sophistiqués.

Ce dispositif est mis en œuvre par la chaîne opérationnelle de sécurité numérique et de cybersécurité, qui est articulée autour du centre de cybersécurité du ministère de l'Intérieur (C2MI) placé sous l'autorité du haut fonctionnaire de défense et du FSSI.

Le dispositif opérationnel de cybersécurité est gradué en quatre modes d'engagement.

1.1. Le mode nominal

En mode nominal, l'action de la chaîne opérationnelle de cybersécurité suffit à répondre à la menace et permet de traiter la totalité des incidents et des alertes.

1.2. Le mode « dispositif renforcé »

Face à une menace élevée ou à un incident important de par son ampleur ou sa criticité, il peut être décidé de renforcer les moyens engagés pour le traitement, de mobiliser les parties prenantes et d'augmenter la fréquence d'information des autorités.

Le mode « dispositif renforcé » peut être déclenché notamment dans les cas suivants :

- Une menace crédible et imminente sur des systèmes d'information du ministère (ex : menace en marge des manifestations des gilets jaunes, en décembre 2018) ;
- Un événement à forte visibilité publique (ex : organisation d'un sommet international ou d'une compétition sportive) ;
- Un incident en cours, sur un large spectre mais avec un impact modéré (ex : attaque EMOTET en septembre 2020) ;
- Un incident en cours, avec un impact sérieux mais sur un périmètre contenu (ex : attaque France-Visas en août 2021).

Le déclenchement et la levée du mode « dispositif renforcé » sont décidés par le haut fonctionnaire de défense adjoint.

1.3. Le mode « crise ministérielle cyber »

Lorsque l'impact d'un incident sur l'activité ou l'image du ministère est estimé grave à majeur, il peut être décidé de déclencher le plan de gestion de crise ministérielle cyber.

Le mode « crise ministérielle cyber » permet de traiter au niveau ministériel à la fois la réponse cyber (traitement des causes) et la continuité des activités (gestion des effets).

Le déclenchement et la levée du mode « crise ministérielle cyber » sont décidés par le secrétaire général, haut fonctionnaire de défense.

1.4. Le déclenchement du plan PIRANET

Lorsque la crise est nationale, le Premier ministre peut décider de déclencher le plan PIRANET.

Le présent document décrit les fonctions inscrites dans le dispositif opérationnel, les interactions et les moyens mis en œuvre, en particulier lors du déclenchement du mode « dispositif renforcé » et du mode « crise ministérielle cyber ».

2. Fonction au sein du dispositif opérationnel de cyberdéfense

Le pilotage stratégique du dispositif opérationnel de cyberdéfense du ministère de l'intérieur est assuré par plusieurs fonctions. Certaines sont activées dès le mode nominal et d'autres sont activées dans le mode « dispositif renforcé » et dans le mode « crise ministérielle cyber ».

2.1 Direction du dispositif (fonction activée dès le mode nominal)

La direction du dispositif opérationnel de cyberdéfense :

- Décide des orientations et des priorités de l'ensemble des fonctions du dispositif ;
- Réalise les arbitrages en fonction de la situation présentée ;
- Décide du passage d'un mode à un autre ;
- Mobilise les parties prenantes et s'assure des moyens engagés dans la gestion de la crise ;
- Assure les interactions avec les autorités politiques hiérarchiques.

En mode « crise ministérielle cyber », cette fonction est appelée « direction de crise ».

En fonction du mode, la direction du dispositif est assurée par des autorités différentes :

En mode nominal :	Haut fonctionnaire de défense adjoint
En mode « dispositif renforcé » :	Haut fonctionnaire de défense adjoint
En mode « crise ministérielle cyber » :	Haut fonctionnaire de défense

2.2 Coordination du dispositif et appui à la conduite (fonction activée à partir du mode renforcé)

La fonction de coordination du dispositif :

- Coordonne les fonctions du dispositif ;
- Prend en charge le relevé des actions décidées par la direction et s'assure de sa diffusion ;
- Pilote le suivi des actions ;
- S'assure du rythme des réunions et des points de situation.

En fonction du mode, la fonction de coordination est assurée par des acteurs différents :

En mode nominal :	N/A
En mode « dispositif renforcé » :	Fonction de sécurité des systèmes d'information
En mode « crise ministérielle cyber » :	Haut fonctionnaire de défense adjoint

2.3 Connaissance de la situation (fonction activée dès le mode nominal)

La fonction de connaissance de la situation :

- Consolide et présente régulièrement une synthèse ou un état des lieux de la situation ;
- Réalise l'interface avec les parties prenantes de la crise.

En mode « crise ministérielle cyber », la fonction de connaissance de la situation est séparée en deux cellules :

- La réponse cyber (traitement des causes) :
 - o Définit une méthode de réponse aux incidents de sécurité adaptée au contexte ;
 - o Recherche, collecte et analyse des éléments issus du système d'information ;
 - o Identifie le mode opératoire et l'objectif de l'attaquant ;
 - o Qualifie l'étendue de la compromission ;
 - o Aide à évaluer les risques et les impacts associés ;
 - o Préconise des mesures de remédiation ;
- La continuité des activités (gestion des effets) :
 - Mesure les impacts métiers ;
 - Propose le plan de continuité d'activité métier.

En fonction du mode, la fonction de connaissance de la situation est assurée par des acteurs différents :

En mode nominal :	Centre de cyberdéfense du MI
En mode « dispositif renforcé » :	Centre de cyberdéfense du MI
En mode « crise ministérielle cyber » :	Fonction de sécurité des systèmes d'information + Centre de cyberdéfense du MI

2.4 Management de l'information (fonction activée à partir du mode « dispositif renforcée »)

La fonction de **management** de l'information :

- Gère l'annuaire de crise et assure sa diffusion ;
- Recueille, classe et archive les informations utiles à la gestion de la crise;
- S'assure que l'information essentielle est partagée ;
- Tient à jour la main courante.

En fonction du mode, la fonction de management de l'information de la situation est assurée par des acteurs différents :

En mode nominal :	N/A
En mode « dispositif renforcé » :	Centre de cyberdéfense du MI
En mode « crise ministérielle cyber » :	À désigner au sein du pôle SSI

2.5 Logistique (fonction activée à partir du mode gestion de crise)

La fonction logistique :

- Est le point de contact de toutes les fonctions de gestion de crise, sur les aspects logistiques ;
- Traite toute demande matérielle utile à la gestion de crise.

En fonction du mode, la fonction logistique est assurée par des acteurs différents :

En mode nominal :	N/A
En mode « dispositif renforcé » :	N/A
En mode « crise ministérielle cyber » :	À désigner au sein du SHFD

2.6 Communication (fonction activée à partir du mode renforcé)

La fonction de communication :

- Est le point de contact de toutes les fonctions de gestion de crise, sur les aspects logistiques ;
- Traite toute demande matérielle utile à la gestion de crise.

En fonction du mode, la fonction de communication est assurée par des acteurs différents :

En mode nominal :	N/A
En mode « dispositif renforcé » :	Délégation à l'information et à la communication
En mode « crise ministérielle cyber » :	Délégation à l'information et à la communication

2.7 Retour d'expérience (fonction activée à partir du mode renforcé)

La fonction de retour d'expérience :

- Recueille les avis des parties prenantes sur les points positifs et les axes d'amélioration du dispositif ;
- Propose des solutions et des actions à mener pour améliorer le dispositif ;
- Assure le suivi de la réalisation des actions identifiées ;
- Met à jour la documentation relative au dispositif à l'issue du RETEX.

En fonction du mode, la fonction de retour d'expérience est assurée par des acteurs différents :

En mode nominal :	N/A
En mode « dispositif renforcé » :	À désigner au sein du pôle SSI
En mode « crise ministérielle cyber » :	À désigner au sein du pôle SSI

3. Interactions du dispositif de gestion de crise cyber

3.1 Interaction avec les équipes opérationnelles du numérique

Les équipes opérationnelles sont responsables de l'administration, de l'exploitation et de la sûreté de fonctionnement des systèmes d'information. Elles assurent le maintien en condition opérationnelle, le maintien en condition de sécurité et interviennent dans la résolution des incidents de sécurité numérique.

Il s'agit notamment des entités suivantes :

- La direction du numérique (DNUM). Compte tenu du rôle primordial de la DNUM dans le dispositif opérationnel de cyberdéfense, un protocole formalisé encadre les échanges opérationnels avec le C2MI ;
- Le service des technologies et des systèmes d'information de la sécurité intérieure (ST(SI)²) ;
- Les agences (ANTS, ANTAI, ANSC, etc.)

Le RSSI de chaque entité opérationnelle est le point de contact initial en cas de déclenchement du mode « renforcé » ou du mode « crise ».

En cas de déclenchement du mode « crise », le directeur de l'entité opérationnelle est directement informé. Un contact opérationnel dédié à la gestion de la crise est désigné pour la durée de la crise par le directeur de l'entité opérationnelle et est intégré à l'annuaire de crise. Il a en charge de mobiliser et désigner les équipes utiles dans le cadre de la crise.

Chaque RSSI est systématiquement informé et associé dès le déclenchement. Il reste informé tout au long de la crise, même s'il n'est pas partie prenante.

Il reste associé à la fonction « Connaissance de la situation », s'il est concerné par l'événement et/ou sa résolution.

Chaque RSSI s'assure que les instructions décidées par la direction du dispositif opérationnel sont mises en œuvre sur son périmètre.

3.2 Interactions avec les autorités qualifiées

Les autorités qualifiées en sécurité des systèmes d'information (AQSSI) du ministère de l'intérieur sont désignées par un arrêté du 20 mai 2016. Elles sont responsables de la sécurité des systèmes d'information au niveau de leur direction générale, organisme ou établissement (entité métier).

Le conseiller de sécurité numérique (CSN) auprès de chaque autorité qualifiée est le point de contact en cas de déclenchement du mode « renforcé » ou du mode « crise ».

Chaque CSN est systématiquement associé dès le déclenchement. Il reste informé tout au long de la crise. Dès le début de la crise, il a en charge de mobiliser et de désigner, pour la durée de la crise, les contacts métiers en mesure d'évaluer les impacts. Ces contacts sont ajoutés à l'annuaire de crise.

Il est associé à la fonction « Connaissance de la situation ». Son rôle est notamment l'évaluation des impacts de l'incident sous-jacent à la crise et des mesures de remédiation proposées.

En préparation à une crise cyber, chaque CSN doit maintenir à jour une cartographie des activités essentielles par métier et leur dépendance par rapport aux systèmes d'information.

Chaque CSN s'assure que les instructions décidées par la direction du dispositif opérationnel sont mises en œuvre sur son périmètre.

3.3 Interactions avec le niveau zonal

En cas de déclenchement du mode « renforcé » ou du mode « crise », les délégués zonaux à la sécurité numérique (DZSN) auprès des PDDS sont informés par le FSSI et sont associés en tant que de besoin. Ils restent informés tout au long de la crise, même s'ils ne sont pas partie prenante.

En cas de déclenchement du mode « crise », les PDDS sont directement informés par le HFDA.

3.4 Interactions avec la DGSI

En cas de déclenchement du mode « renforcé » ou du mode « crise », la DGSI est informée par le FSSI. Un contact opérationnel est désigné pour la durée de la crise.

Elle est associée à la fonction « Connaissance de la situation », qu'elle appuie grâce à sa capacité d'analyse de la menace. Elle est destinataire de tous les points de situation.

3.5 Interactions avec les autres dispositifs de gestion de crise au sein du ministère

< A développer en fonction des retours d'expérience >

Les interactions vis-à-vis des autres dispositifs de gestion de crise :

- COGIC ;
- Centre de veille ;
- Autres.

3.6 Interactions avec l'ANSSI et les autres ministères

L'ANSSI (SDO) est informée du passage en mode « dispositif renforcé ». Le DG de l'ANSSI est informé par le HFDA du passage en mode « crise ministérielle cyber ». L'assistance de l'ANSSI peut être sollicitée en tant que de besoin, en fonction de la nature de l'incident cyber sous-jacent. Elle est destinataire des points de situation produits par la fonction « Connaissance de la situation ».

L'ensemble des FSSI ministériels est informé du passage en mode « dispositif renforcé » et mode « crise ministérielle cyber » par le FSSI.

4. Moyens et outils de gestion de crise

4.1 Documentation

La documentation relative au fonctionnement du dispositif opérationnel de cyberdéfense et à la gestion de crise cyber est rassemblée à l'adresse : <adresse à définir>.

Elle est constituée :

- Du présent document ;
- Du protocole d'échanges opérationnels entre la DNUM et le C2MI ;
- Du plan Piranet ;
- Des modèles de point de situation ;
- Des retours d'expérience des précédentes crises ;
- Etc.

4.2 Annuaire

En mode nominal, l'annuaire des points de contact opérationnels est maintenu à jour par le C2MI, en s'appuyant notamment sur l'outil Capitole.

Au déclenchement du mode « dispositif renforcé » et du mode « crise ministérielle cyber », la fonction « management de l'information » est chargée de constituer un annuaire de crise et de le diffuser aux parties prenantes.

4.3 Moyens de communications

Les moyens de communication utilisés par les parties prenantes sont précisés dans l'annuaire de crise. En fonction de la nature de la crise, certains pourront être indisponibles.

Les moyens d'échange pour des informations de niveau « non protégé » :

- Messagerie électronique : pour assurer une traçabilité, tous les messages concernant la gestion de crise seront adressés en copie à la fonction « management de l'information » (adresse à déterminer).
- Téléphone fixe et mobile ;
- Visioconférence COMU (étudier la possibilité d'un pont de visioconférence robuste dédié à la gestion de crise cyber).

Les moyens d'échange pour des informations de niveau « diffusion restreinte » :

- Téléphone mobile CallMI ;
- Fichiers chiffrés avec l'outil Zed ! (à privilégier) ou ACID.

Les moyens d'échange pour des informations classifiées au niveau « Secret » de l'IGI 1300 :

- Téléphone OSIRIS (ou TEOREM) ;
- Visioconférence OSIRIS-Visio ou HORUS ;
- Messagerie ISIS.

5. Actions immédiates et armement des fonctions

5.1 Armement des fonctions en mode nominal

	Responsable	Participants	Missions	Actions/productions
Direction du dispositif	HFDA	-	• Décide des orientations et des priorités de l'ensemble des fonctions du dispositif ; • Réalise les arbitrages en fonction de la situation présentée ; • Décide du passage d'un mode à un autre ; • Mobilise les parties prenantes et s'assure des moyens engagés dans la gestion de la crise; • Assure les interactions avec les autorités politiques hiérarchiques.	
Connaissance de la situation	C2MI	-	• Consolide et présente régulièrement une synthèse ou un état des lieux de la situation ; • Réalise l'interface avec les parties prenantes de la crise.	

5.2 Actions immédiates et armement des fonctions en mode « dispositif renforcé »

Actions immédiates en cas de déclenchement du mode « dispositif renforcé » :

- Désignation des responsables de chaque fonction ;
- Mobilisation des équipes opérationnelles et métiers ;
- Information des RSSI des équipes opérationnelles ;
- Information des CSN des directions métier ;
- Fixation du rythme des productions de l'état de la situation ;
- Autres.

	Responsable	Participants	Missions	Actions/productions
Direction du dispositif	HFDA	-	• Décide des orientations et des priorités de l'ensemble des fonctions du dispositif ; • Réalise les arbitrages en fonction de la situation présentée ; • Décide du passage d'un mode à un autre ; • Mobilise les parties prenantes et s'assure des moyens engagés dans la gestion de la crise; • assure les interactions avec les autorités politiques hiérarchiques.	• Note indiquant le passage en dispositif renforcé et demandant de mobiliser les parties prenantes pour la durée du dispositif renforcé • Mise en place d'une organisation attendue. • Annuaire de crise transmis au C2MI.
Coordination du dispositif et appui à la conduite	FSSI	-	• Coordonne les fonctions du dispositif ; • Prend en charge le relevé des actions ; • Pilote le suivi des actions ; • S'assure du rythme des réunions et des points de situation.	• Détermine la fréquence des points de situation et les attendus en fonction de la menace ou de l'incident ;

	Responsable	Participants	Missions	Actions/productions
Connaissance de la situation	C2MI	DGSI, DNUM, ST(SI) ² , AQSSI, ANSSI	- Consolide et présente régulièrement une synthèse ou un état des lieux de la situation ; - Réalise l'interface avec les parties prenantes de la crise.	Désigne les parties prenantes en fonctions du type d'incident ou de menace
Communication	DICOM	FSSI C2MI	- Réalise une veille médiatique ; - Anticipe les éléments de langage et élabore les argumentaires ; - Gère la communication externe.	
Retour d'expérience	À désigner au sein du pôle SSI	-		

5.3 Actions immédiates et armement des fonctions en mode « dispositif renforcé »

Actions immédiates en cas de déclenchement du mode « dispositif cyber renforcé » :

- Information du cabinet du ministre ;
- Désignation des responsables de chaque fonction ;
- Information des directeurs et des RSSI des équipes opérationnelles ;
- Information des autorités qualifiées et des CSN dans les directions métier ;
- Organisation d'une première réunion de crise ;
- Fixation du rythme des productions de l'état de la situation ;
- Autres.

	Responsable	Participants	Missions	Actions/productions
Direction du dispositif	SG/HFD	-	- Décide des orientations et des priorités de l'ensemble des fonctions du dispositif ; - Réalise les arbitrages en fonction de la situation présentée ; - Décide du passage d'un mode à un autre ; - Mobilise les parties prenantes et s'assure des moyens engagés dans la gestion de la crise; - Assure les interactions avec les autorités politiques hiérarchiques.	- Note indiquant le passage en mode « gestion de crise cyber » et demandant de mobiliser les parties prenantes pour la durée de la crise - Mise en place d'une organisation attendue. - Annuaire de crise transmis à la fonction « management de l'information »
Coordination du dispositif et appui à la conduite	HFDA	-	- Coordonne les fonctions du dispositif ; - Prend en charge le relevé des actions ; - Pilote le suivi des actions ; - S'assure du rythme des réunions et des points de situation.	
Connaissance de la situation	FSSI/C2MI	C2MI, DGSI, DNUM, ST(SI) ² , AQSSI, ANSSI	- Consolide et présente régulièrement une synthèse ou un état des lieux de la situation ; - Réalise l'interface avec les parties prenantes de la crise - Le C2MI coordonne la connaissance de la situation d'un point de vue technique	
Management de l'information	À désigner au sein du pôle SSI	-	- Recueille, classe et archive les informations utiles à la gestion de la crise; - S'assure que l'information essentielle est partagée ; - Tient à jour la main courante.	

	Responsable	Participants	Missions	Actions/productions
Logistique	A désigner au sein du SHFD	-	Est le point de contact de toutes les fonctions de gestion de crise, sur les aspects logistiques ; traite toute demande matérielle utile à la gestion de crise.	
Communication	DICOM	C2MI, autres équipes de communication	- Réalise une veille médiatique ; - Anticipe les éléments de langage et élabore les argumentaires ; - Gère la communication externe.	
Retour d'expérience	À désigner au sein du SHFD	-		

6. Plan de remédiation technique

6.1 Construction

- Sous le pilotage du C2MI ;
- Contributeurs :
 - Experts ANSSI ;
 - Experts techniques en fonction du périmètre ciblé ;
 - Experts métiers.

6.2 Validation

- Avis du C2MI ;
- Validation de la direction de crise.

6.3 Communication

- Fonction « Communication ».

6.4 Suivi

- Suivi initial des mesures immédiates : C2MI ;
- Suivi post-crise : SHFD/SMR.

7. Dépôt de plainte

Les incidents avérés, constatés lors d'un passage en mode renforcé ou en mode « gestion de crise » font systématiquement l'objet d'un dépôt de plainte auprès de la direction générale de la sécurité intérieure (DGSI).

Si un système d'information en particulier a été visé, il revient à l'autorité qualifiée de désigner le responsable qui va déposer la plainte.

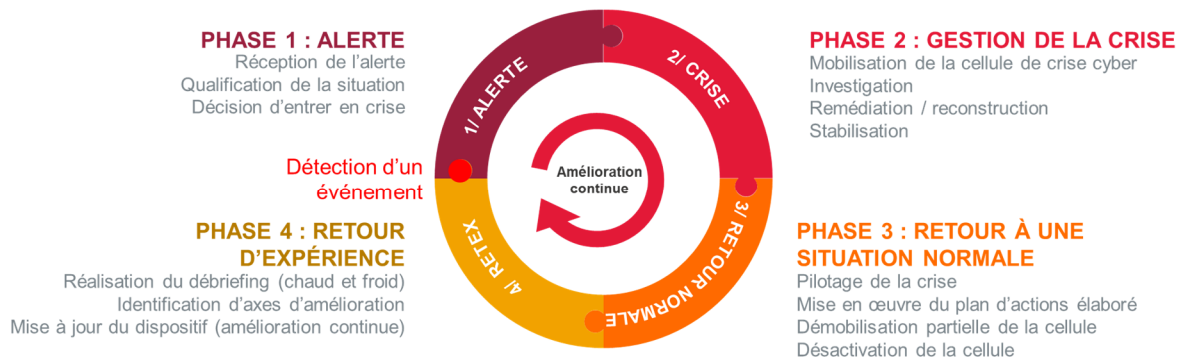
Si l'attaque a visé des systèmes de plusieurs autorités qualifiées, il revient au secrétaire général, haut fonctionnaire de défense, de déposer la plainte.

8. Annexes

8.1 Annexe 1 : Phase d'une crise cyberdéfense

8.1.1. Synoptique – vision global du processus de crise

Le schéma ci-dessous, produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI) présente le cycle de la crise, de la détection d'un événement cyber et le lancement de l'alerte au retour d'expérience. Il est valable que le dispositif opérationnel escalade jusqu'au mode « gestion de crise cyber » ou seulement jusqu'au mode « dispositif renforcé ».



8.1.2. Phase 1 – Alerte

Il s'agit de la phase de détection d'une menace cyber. Le passage de la première phase à la seconde de gestion de la crise se fait dès la réception d'une alerte ou par la remontée d'un événement cyber.

Durant cette phase, l'alerte est prise en compte par le C2MI, qui évalue la situation et peut proposer une escalade de posture dans le mode du dispositif opérationnel.

8.1.3. Phase 2 – Gestion de la crise

Il s'agit de la phase durant laquelle le dispositif opérationnel voit sa posture escaladée (en mode « renforcé », voire en mode « crise »). Cette phase est marquée par le passage en organisation de crise. Dès l'activation de la cellule cyber, le secrétaire opérationnel de crise mobilise les experts concernés.

8.1.4. Phase 3 – Retour à la normale

La phase de retour à la normale débute lorsque la situation est sous contrôle, elle passe par la démobilisation des acteurs de la cellule et la désactivation de la cellule de crise cyber. Cette phase est marquée par la désescalade de la posture du dispositif opérationnel.

La communication aux utilisateurs sur le retour à la normale est réalisée. La direction du dispositif reste mobilisée afin d'assurer le suivi des actions jusqu'au retour à la normale. La phase de sortie de crise se clôture avec l'annonce de la fin de la crise cyber. Les exceptions nécessaires lors de la phase de reconstruction pendant la sortie de crise sont tracées et remédiées au cours du temps.

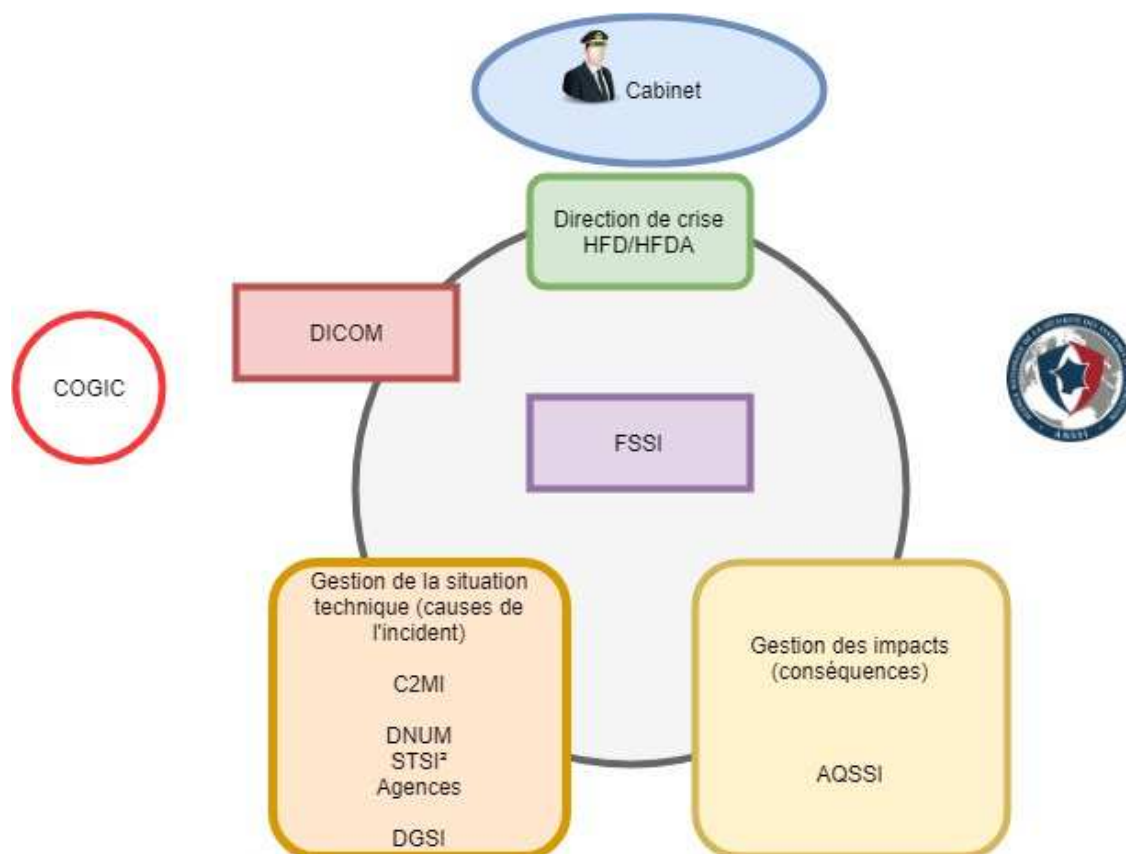
8.1.5. Phase 4 – Retour d'expérience

Une fois la crise terminée et le retour à une situation normale assuré, il est primordial d'analyser la gestion de la crise passée et de mettre en place des actions afin d'améliorer le dispositif en place.

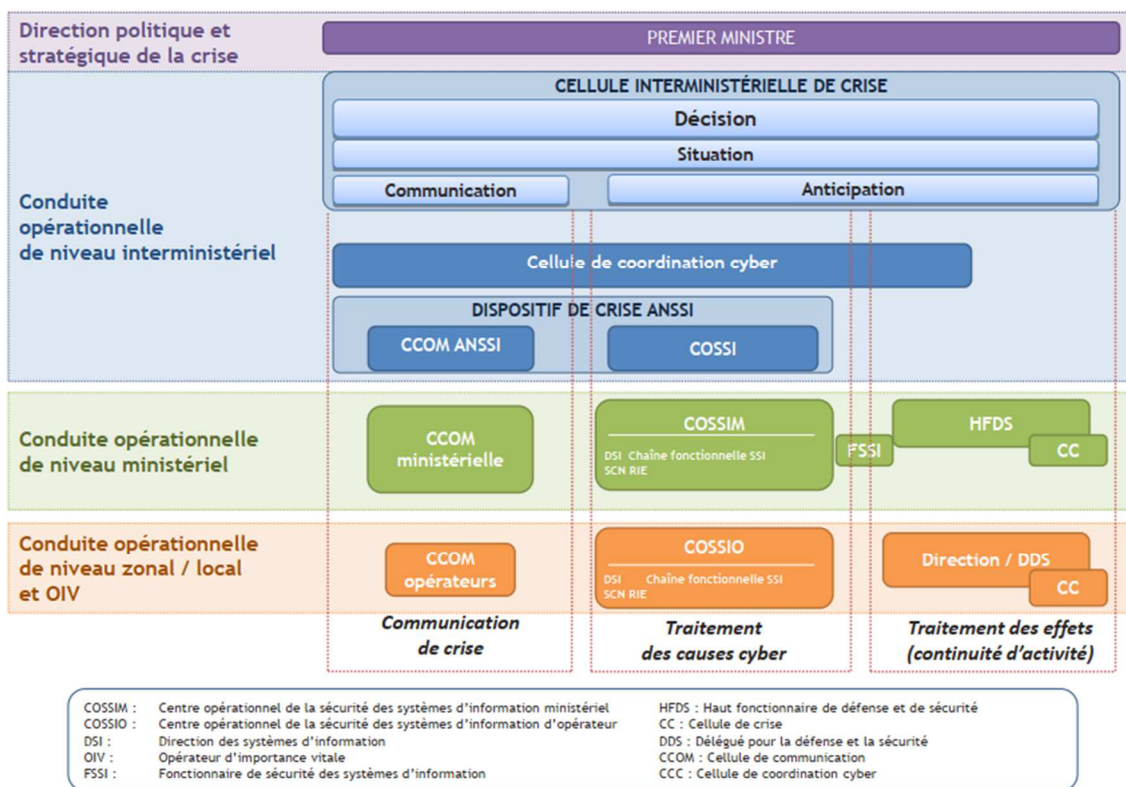
Durant cette phase, un retour d'expérience est réalisé par les parties prenantes à la crise passée.

Les forces et faiblesses dans la gestion de la crise sont identifiées afin de mettre en place un plan d'action dans le but d'améliorer le dispositif de crise cyber. Une fois les procédures de crises cyber revues avec les éléments remontés lors du retour d'expérience, il convient d'organiser des formations de gestion de crise et de tester à nouveau le dispositif via des exercices de simulation

8.2 Annexe 2 : Organisation ministérielle de gestion de crise cyber



8.3 Annexe 3 : Organisation gouvernementale de gestion de crise cyber



FIN DU DOCUMENT