ACCD'OM 33ème CONGRÈS

SESSION D'ATELIER - JEUDI 13 NOVEMBRE 2025

Gestion de Crise d'origine cyber : Comment réagir ? *Conseils et bonnes pratiques*

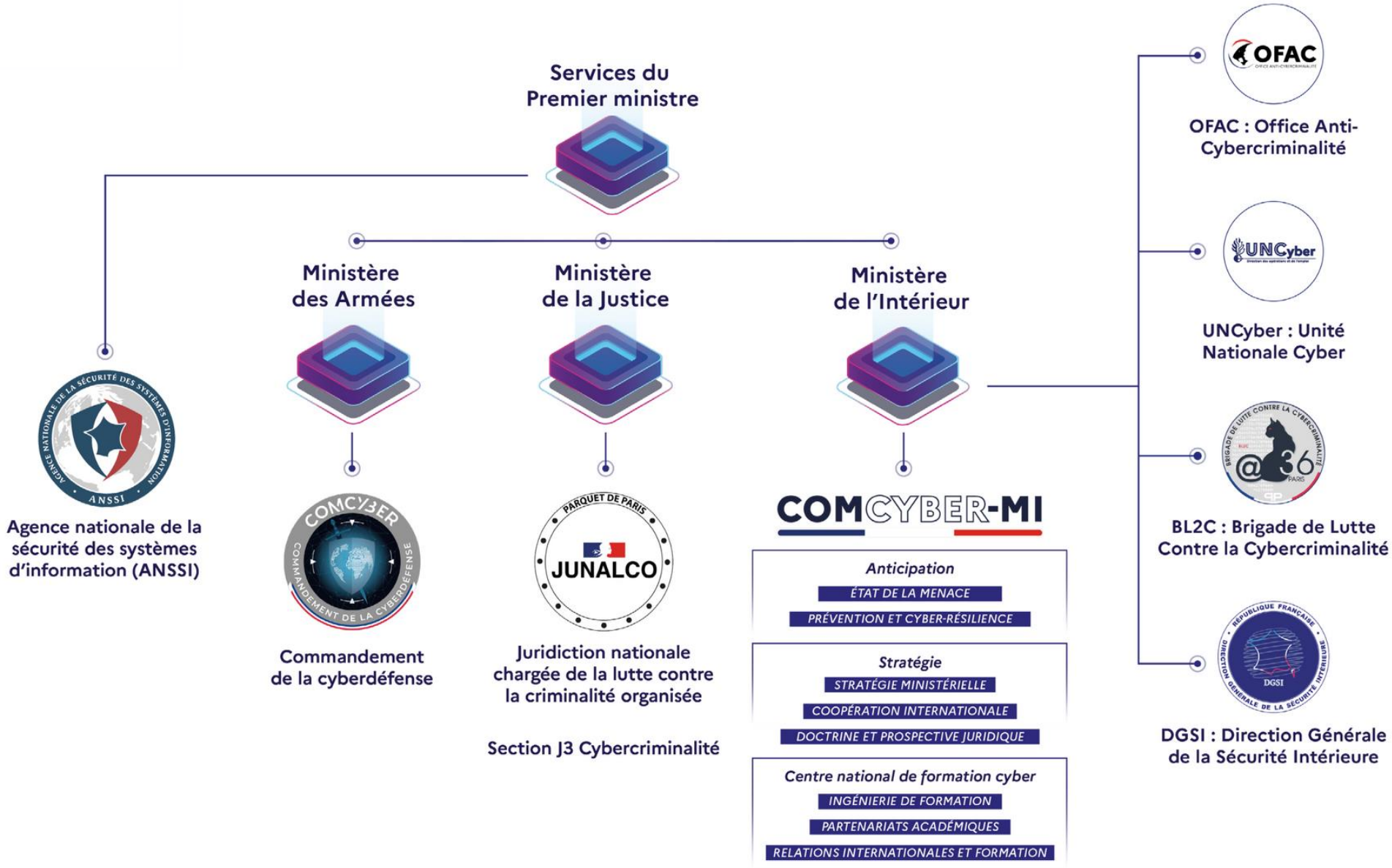
Moïse MOYAL - Agence Nationale de la Sécurité des Systèmes d'Information
Délégué à la sécurité numérique aux outre-mer
outre-mer@ssi.gouv.fr

Loic CARTIER – COMCYBER – MI
Département prévention et cyber resilience

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

ÉCOSYSTÈME



Services du Premier ministre

SGDSN

Secrétariat général de la Défense et de la Sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Service à compétence nationale,
d'environ 650 agents

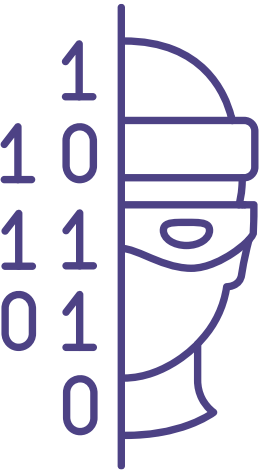
Autorité nationale en matière
de cybersécurité et de cyberdéfense

Vocation exclusivement défensive
(Connaître, Partager, Défendre, Accompagner, Réguler)

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

Lutte contre la cybercriminalité



Cybercriminalité :

à l'encontre ou au moyen d'un système d'information

Les missions de la gendarmerie

Prévention et proximité numérique

Investigations judiciaires numériques

Traitement de la preuve numérique

Principe de subsidiarité au sein de la gendarmerie

National

Unité Nationale Cyber :

- Division de l'animation renseignement coordination
- Division des opérations (ou C3N)
- Division technique

Régional

Antennes Unité Nationale Cyber (UNCyber) au sein des Sections de Recherche

Départemental

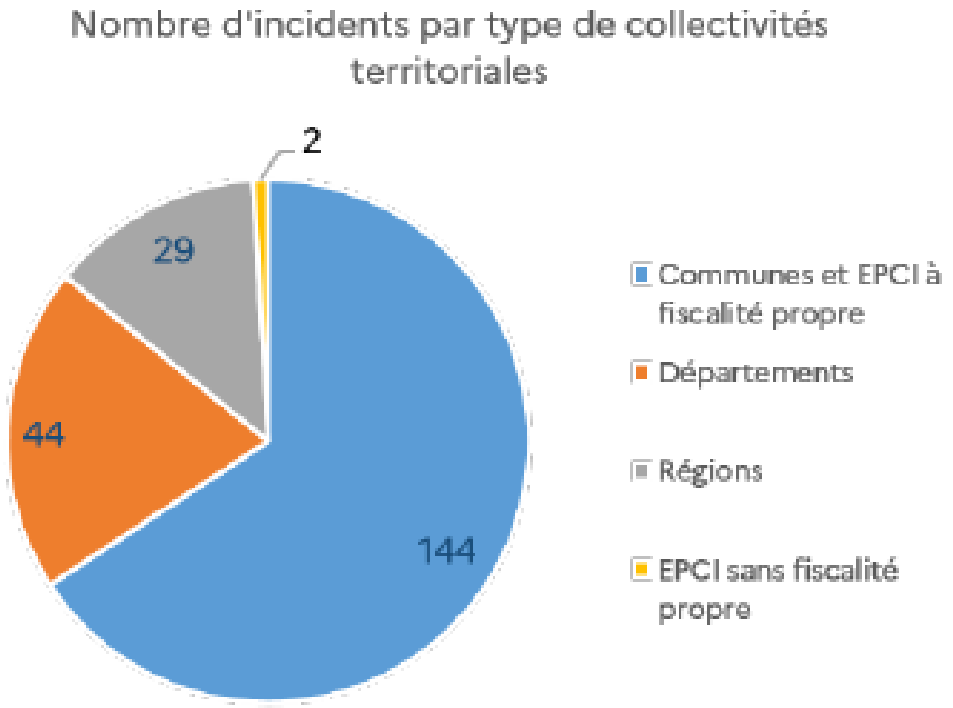
Sections opérationnelles de lutte contre les cybermenaces "SOLC"

Local

Enquêteurs numériques de proximité "cybergendarmes"


Brut.

Menace au sein de nos collectivités en 2024



- **Augmentation significative des incidents :** l'ANSSI a traité **228 incidents*** affectant les collectivités territoriales en 2024, soit **18 incidents par mois**.
- **Variété des victimes :** Régions, Départements, Communes, EPCI,
- La motivation lucrative représente la majorité des incidents

*Ce nombre n'est pas exhaustif et ne reflète que les incidents qui ont été porté à la connaissance de l'ANSSI

Source : Collectivités territoriales – Synthèse de la menace 2024

Mai 2023 - Collectivité Territoriale de Martinique

- Cyberattaque par rançongiciel revendiquée par le groupe *Rhysida*.
- Données exfiltrées et diffusées sur le dark web.
- Ralentissement des services administratifs durant plusieurs semaines.

Décembre 2023 - Province des Îles de Nouvelle-Calédonie

- Attaque ayant paralysé plusieurs services publics.
- Réseaux internes coupés pour éviter la propagation.
- Rétablissement progressif avec appui de l'ANSSI locale.

Mai 2024 - Université de Guyane

- Intrusion informatique entraînant une coupure partielle du réseau universitaire.
- Messagerie et portail étudiants temporairement inaccessibles.
- Communication officielle de l'université sur les mesures de protection renforcées.

Juillet 2024 – Villee de Mahina (Polynésie Française)

- Arrêt complet des services de la commune
- Refonte complète de l'infrastructure informatique
- Mise en avant d'une politique de résilience

Novembre 2025 – Conseil Départemental de La Réunion

- Compromission de l'environnement Active Directory
- Exfiltration de données.
- L'ensemble du système d'information a été isolé d'internet, provoquant de forts impacts métiers, notamment du fait de la perte d'accès à la messagerie.

Octobre 2025 – Ville de Saint-Claude (Guadeloupe)

- Cyberattaque paralysant la messagerie et plusieurs services municipaux
- Fermeture temporaire des guichets numériques
- Création d'une cellule de crise locale

Les crises d'origine cyber - quelles spécificités ?

Crise de nature technologique centrée sur l'expertise

Double temporalité (effets immédiats et remédiation longue)

Problème de l'attribution

Adaptation –
une menace intelligente qui s'adapte

Propagation –
Absence d'unicité de lieu

Objectifs de l'atelier

- ✓ **Vivre (de façon fictive !) les enjeux de la gestion d'une crise d'origine cyber**
- ✓ **Se questionner sur les bonnes (et mauvaises) pratiques**

Règles du jeu

- **Diffusion d'un scénario par l'animateur**
- **2 à 3 prises de parole par questions**

Vous représentez les services et les élus de la commune Valfleuri.
La commune est une collectivité de 30 000 habitants. 280 agents travaillent pour cette dernière. Le réseau informatique est géré par la commune et le site et seul le site web est externalisé.

Nous sommes le lundi 6 février 2026.
Il est 9h du matin.
Vous allez débuter la réunion de direction hebdomadaire.

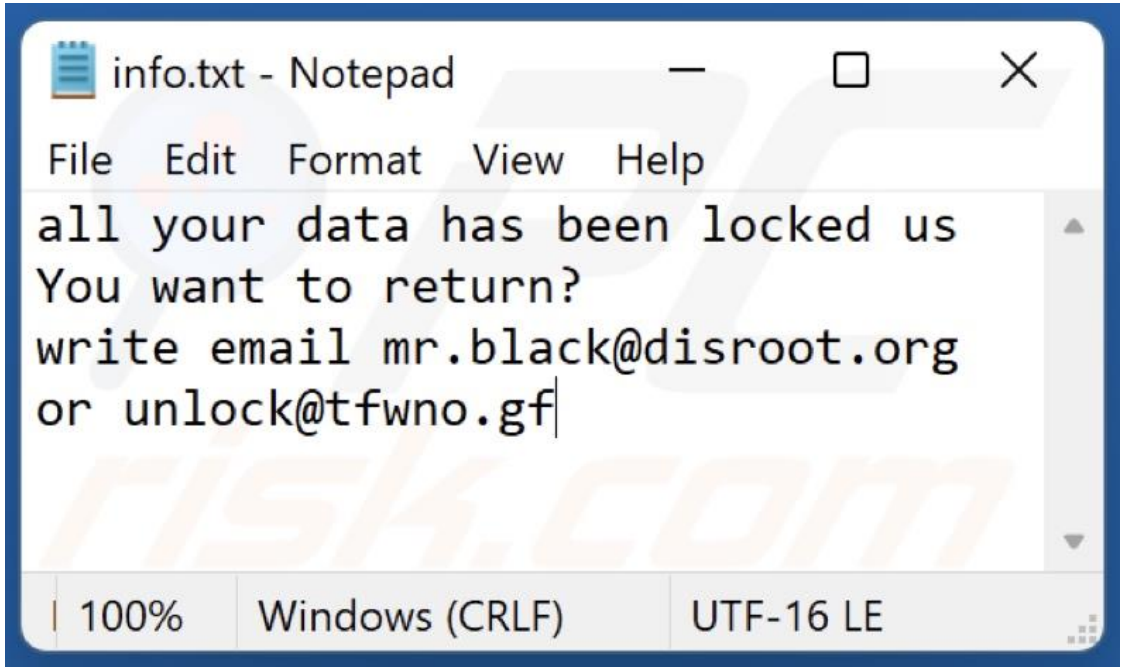
Les agents de l'état-civil appellent l'informatique.
Ils n'arrivent plus à accéder à l'outil de prise de rendez-vous. La gestionnaire de paie n'arrive plus à accéder aux fichiers des contrats passés avec les fournisseurs.

Votre entreprise est victime d'une cyberattaque !

1. Arrêt des activités

Situation :

- **Vous avez un message de rançon**
- **Vos systèmes sont inaccessibles**



1. Arrêt des activités

- **Quelles premières actions prenez-vous face à cette situation ?**
- **Est-il nécessaire d'activer une cellule de crise ?**
- **Qui déclare officiellement la crise ?**
- **Quelles parties prenantes souhaitez-vous mobiliser ?**
- **Comment communiquez-vous si les outils sont hors service ?**

Les rendez-vous à l'accueil s'impatientent pour les demandes de cartes d'identité notamment d'étudiants avant leur examen

La gestion des inscriptions ne peut plus se faire avant les vacances

Les policiers municipaux n'ont plus accès à leurs outils numériques

2. Gestion de la crise

Situation :

- **Le maire demande à sécuriser et relancer au plus vite les activités clés de votre commune**
- **Un point de situation est demandé deux fois par jour**
- **Devant la charge de travail importante, il s'avère nécessaire de prioriser les actions à mener**

2. Gestion de la crise

- Comment doit s'organiser la cellule de crise ?
- De quels outils ai-je besoin ?
- Qui doit définir ces priorités ?
- Quels sont les activités à maintenir ?

3. Pression médiatique

Situation :

- **Le préfet veut se rendre à la mairie pour comprendre la situation**
- **La demande de rançon a été publiée sur les réseaux sociaux**
- **Un journaliste souhaite une interview**
- **Nos administrés veulent savoir si leur données personnelles ont été dérobées**

3. Pression médiatique

- **Qui valide la prise de parole publique ?**
- **Que dire si l'enquête est en cours ?**
- **Comment éviter les erreurs de communication en stress ?**

4. Pression interne

Situation :

- **Les agents ne peuvent plus travailler et s'inquiètent pour leur paye**
- **Les managers intermédiaires manquent d'information et improvisent**
- **Les équipes techniques sont épuisées et subissent la pression de la direction et des agents**

4. Pression interne

- **Comment gérer la communication interne en période de crise ?**
- **Qui soutient les équipes techniques ?**
- **Quel rôle pour la direction RH et les managers de proximité ?**
- **Comment maintenir la confiance et l'engagement des équipes ?**

5. Paiement de la rançon et judiciarisation

Situation :

- **Un collaborateur propose de payer la rançon afin de continuer à travailler**
- **Cela permettra d'éviter aux agents un burnout**
- **Le coût de la rançon est moins élevé que l'arrêt des activités**
- **Aucune assurance de récupération des données de sauvegarde**

5. Paiement de la rançon et judiciarisation

- **En payant la rançon, vais-je arrêter la crise ?**
- **Pourquoi déposer plainte ? Quel est l'apport des forces de l'ordre ?**

Quels enseignements à retenir d'une gestion de crise cyber ?

Il n'y pas de crise « cyber » (mais une crise d'origine cyber)

Je me prépare à gérer la crise (organisation / technique)

Je prends des décisions (parfois incertaines) pour assurer la continuité d'activité

Je communique en interne et avec les parties prenantes

Bien évaluer le besoin et temps de remédiation

Des outils pour s’entrainer

REMPAR 2025

Méthodologie REMPAR25

Guides

Sen Cy-Crise
Initiation à la gestion de crise cyber

MOOC SencyCrise par le COMCYBERMI

Contacts en cas d'incidents cyber

CERT-FR

cert-fr@ssi.gouv.fr / +33 9 70 83 32 18

17 CYBER
Mon assistance en ligne

POLICE NATIONALE

Gendarmerie nationale

CSIRT* Territoriaux ultra-marins

* Computer Security Information Response Team

« L’avenir ne se prévoit pas, il se prépare (Maurice Blondel) »

« Mal communiquer, c’est ajouter une crise à la crise. »

Temps d'échange

ACCD'OM 33ème CONGRÈS

SESSION D'ATELIER - JEUDI 13 NOVEMBRE 2025

MERCI POUR VOTRE ATTENTION

Moïse MOYAL
Délégué à la sécurité numérique aux outre-mer
outre-mer@ssi.gouv.fr

Loic CARTIER – COMCYBER – MI
Département prévention et cyber resilience