MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI
Gendarmerie nationale

# LE MINISTÈRE DE L'INTÉRIEUR FACE AUX CYBERMENACES

## Le COMCYBER-MI

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# La cybercriminalité

## Une ~~proposition de défini~~tion:

« la cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet ».

Rapport ***« Protéger les internautes »***, Bir, Marc Robert, 2014 p.12

MINISTÈRE
DE L'INTÉRIEUR

*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

# RAPPORT ANNUEL SUR LA CYBERCRIMINALITÉ 2024

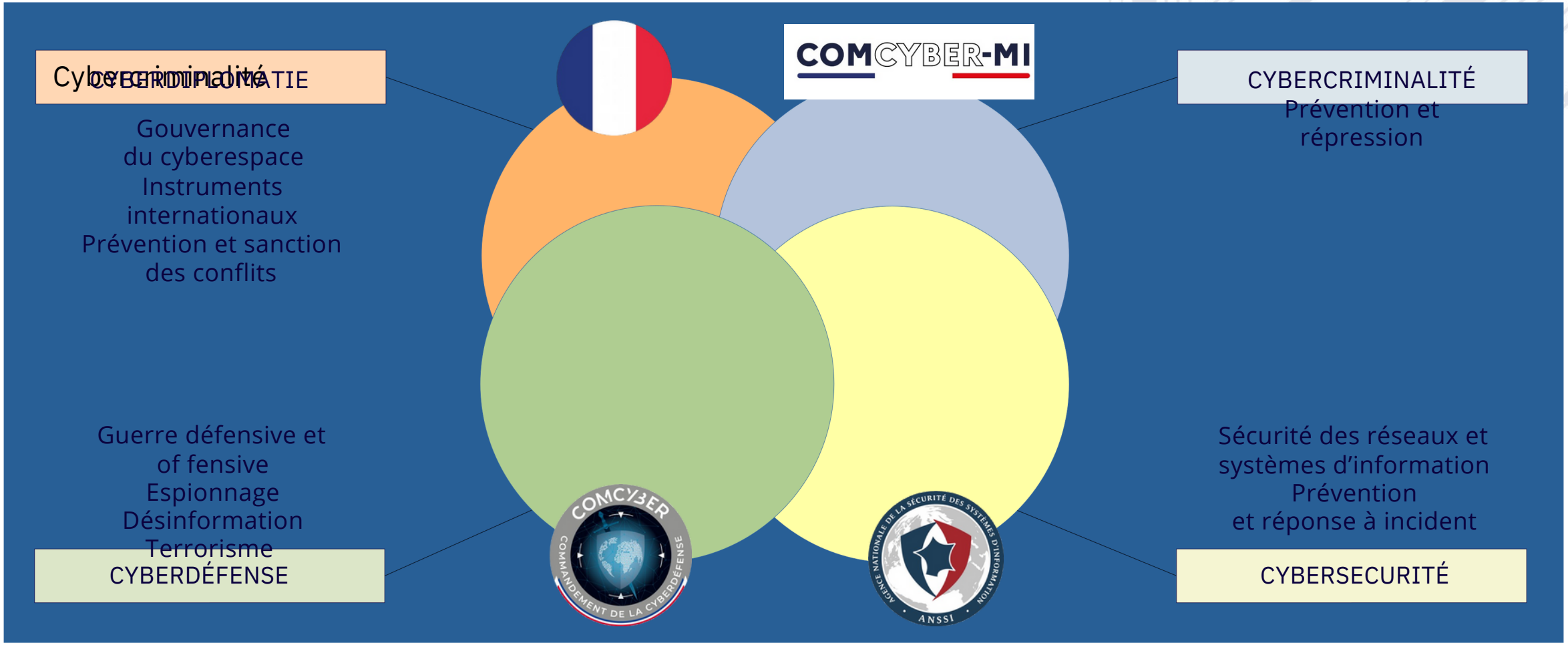
MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# *Les enjeux de la cybercriminalité en 2024*

- *I- État de la menace*
- *II- L'État se structure pour faire face*
- *III- Tous concernés …*

# LES CYBERSPHÈRES

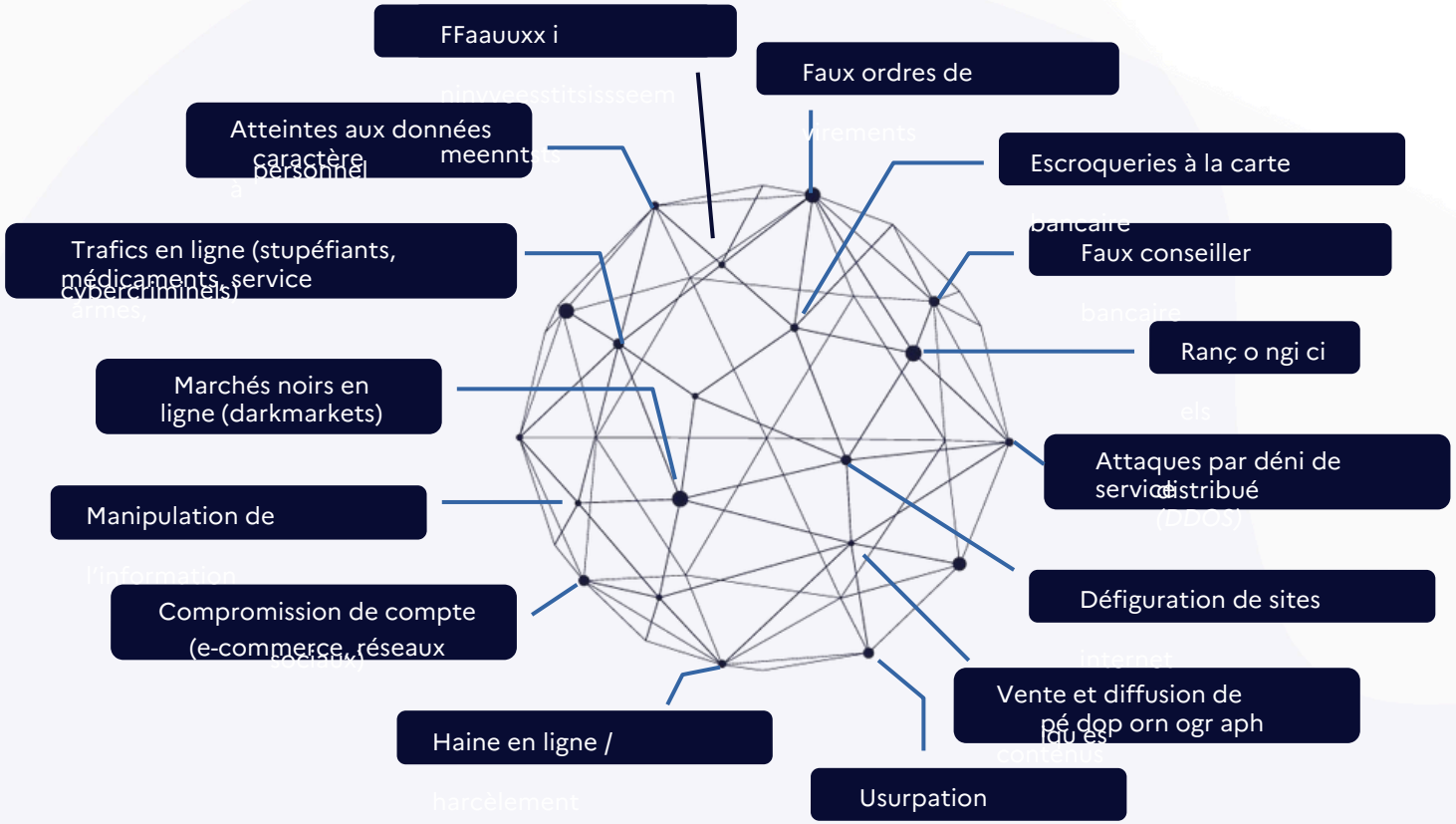


# État de la menace

**278 770**
atteintes numériques enregistrées en 2023

**+ 40%**
d'atteintes numériques en 5 ans

| 2019 | 2020 | 2021 | 2022 | 2023 |
|---|---|---|---|---|
| 199 850 | 233 440 | 279 040 | 255 320 | 278 770 |



MINISTÈRE DE L'INTÉRIEUR
*Liberté Égalité Fraternité*

COMCYBER-MI

# I Répartition des infractions


Atteintes aux biens

59%

Ex : escroqueries, détournement de moyens de paiement, infractions occasionnant un préjudice financier…

Atteintes aux personnes

34,5%

Ex : harcèlement, injures, menaces, discriminations, atteintes aux mineurs…


Atteintes aux législations et réglementations spécifiques numériques

0,5%

~~Ex : infractions au droit d'auteur~~, infractions au RGPD…

Atteintes aux institutions et à l'ordre public

6%

~~Ex : troubles à l'ordre public,~~ atteintes à la sûreté de l'état et aux institutions, trafics, contrefaçon, recel…

## Plateformes en ligne du ministère de l'Intérieur

PERCEV@L

259 094 signalements en 2023.

PHAROS

211 543 signalements en 2023.

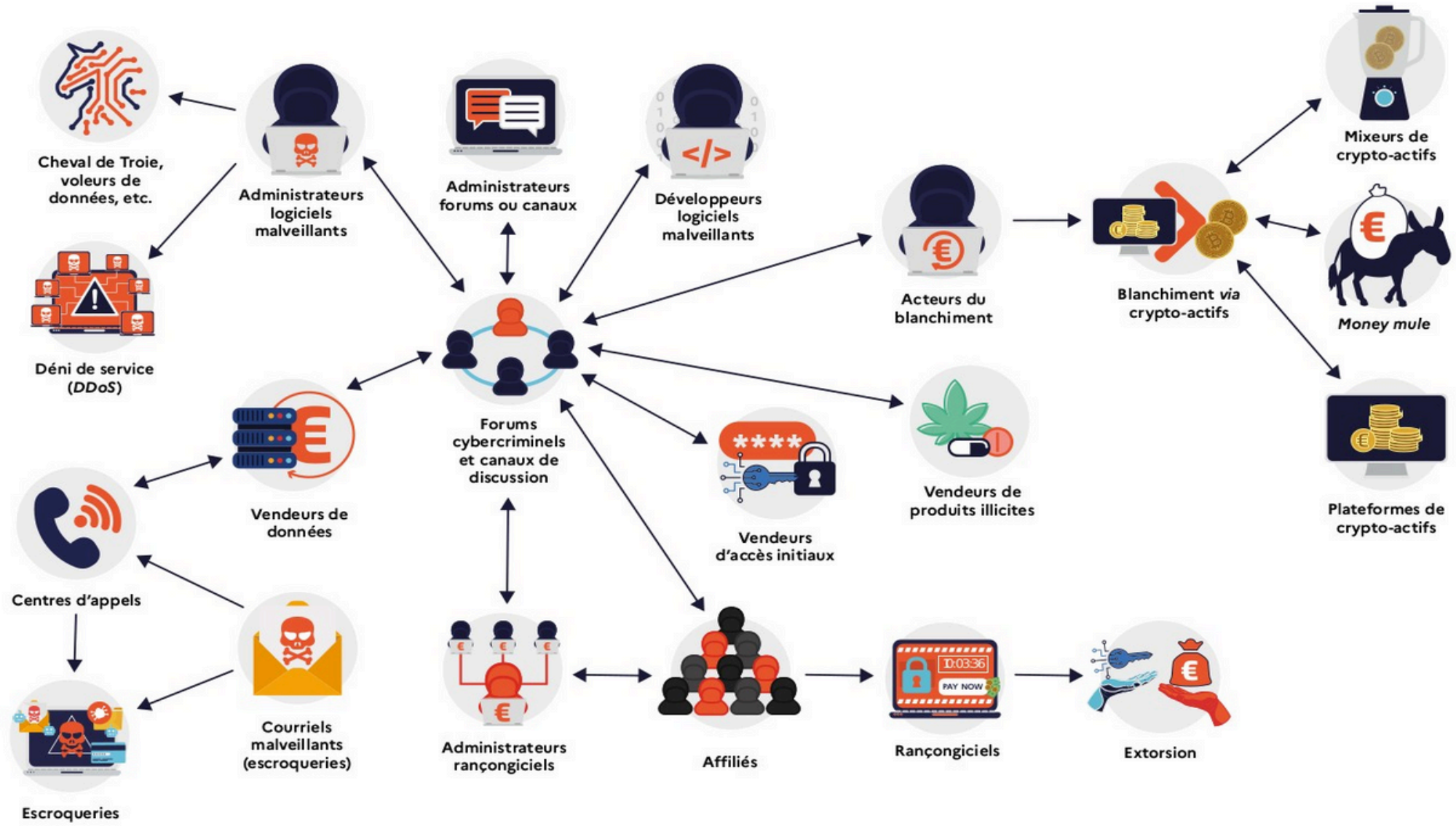
THESEE

104 439 déclaration en 2023.

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# Écosystème de la cybercriminalité



MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# La menace rançongiciel en quelques chiffres

**81%** des attaques sont réalisées par courriel

**5%** des courriels sont des rançongiciels

**450€** coût moyen d'une rançon

**34%** des victimes ont payé la rançon

**20 000** machines infectées en 1 mois

**11s** 1 attaque toutes les 11 secondes


1ère MENACE
Entreprises & Collectivités

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

F / Tech & web

Actualités Start-up Tests Pratique Jeux vidéos

Réservé aux abonnés

# Ciblés par les hackers, les hôpitaux françai malades de leur cybersécurité

Par **Ingrid Vergara**
Publié hier à 22:50, mis à jour hier à 22:50


Pour les pirates, la valeur grandissante des données de santé sur le marché noir du darknet représente u d'échange. *© Tesson / Andia.fr/© Tesson / Andia.fr*

# INFO JDD. Le tribunal de Paris cible d'un vaste pirat

23h00 , le 5 septembre 2020

**ABONNÉS**

**L'intrusion hostile a visé plusieurs magi enquête a été ouverte pour en détermir**

*Le tribunal de Paris, le 2 septembre 2020 (AFP)*

Le tribunal de Paris vient d'être la cible d'u procureur de la République, Rémy Heitz, l sur son propre ordinateur, a ouvert, jeudi, déterminer les auteurs. Celle-ci a été conf sécurité intérieure (DGSI), service chef de sensibilité du dossier. Plusieurs magistrats national financier, et des avocats parisiens effet été touchés.

Société

# Après le piratage informatique de la mairie de Douai, des données personnelles des habitants volées ?

Mercredi 14 avril 2021 à 21:42 - Par **Florent Vautier**, **France Bleu Nord**, **France Bleu**

Douai

**Vendredi dernier, des hackers ont piraté les serveurs de la ville de Douai par le biais d'un rançongiciel, un logiciel malveillant qui bloque les données informatiques en échange d'une rançon. Les services sociaux ont été touchés, faisant craindre la perte de certaines données personnelles.**

Les services municipaux en ligne reviennent progressivement à la normale © Radio France - Odile Senellart

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# *Les enjeux de la cybercriminalité en 2024*

- *I- État de la menace*
- *II- L'État se structure pour faire face*
- *III- Tous concernés …*

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# L'écosystème étatique de lutte contre la cybercriminalité

Service du
Premier ministre

Agence nationale de la sécurité des systèmes d'informations (ANSSI)

Ministère de la justice

Juridiction nationale chargée de la lutte contre la criminalité organisée

Section J3 Cybercriminalité

Ministère de l'Intérieur

COMCYBER-MI

**Compétences rares projetables**
- INVESTIGATIONS SPÉCIALISÉES
- EXPERTISES NUMÉRIQUES
- SCIENCES DE LA DONNÉE

**Centre national de formation cyber**
- INGÉNIERIE DE FORMATION
- PARTENARIATS ACADÉMIQUES

**Stratégie et anticipation**
- ÉTAT DE LA MENACE
- GESTION DE CRISE
- STRATÉGIE MINISTÉRIELLE
- COOPÉRATION INTERNATIONALE

OFAC : Office Anti-Cybercriminalité

UNCyber : Unité Nationale Cyber

BL2C : Brigade de Lutte Contre la Cybercriminalité

DGSI : Direction Générale de la Sécurité Intérieure

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

Décret n° 2023-1084

portant création d'un service à compétence nationale nommé Commandement du ministère de l'Intérieur dans le cyberespace

→ Service à compétence nationale

→ Compétent en matière de prévention et de lutte contre la cybercriminalité

→ Point de contact unique pour les autres ministères dans son domaine de compétence

→ Représente le MININT dans les échanges internationaux et contribue à l'élaboration de la position française dans les instances européennes et internationales

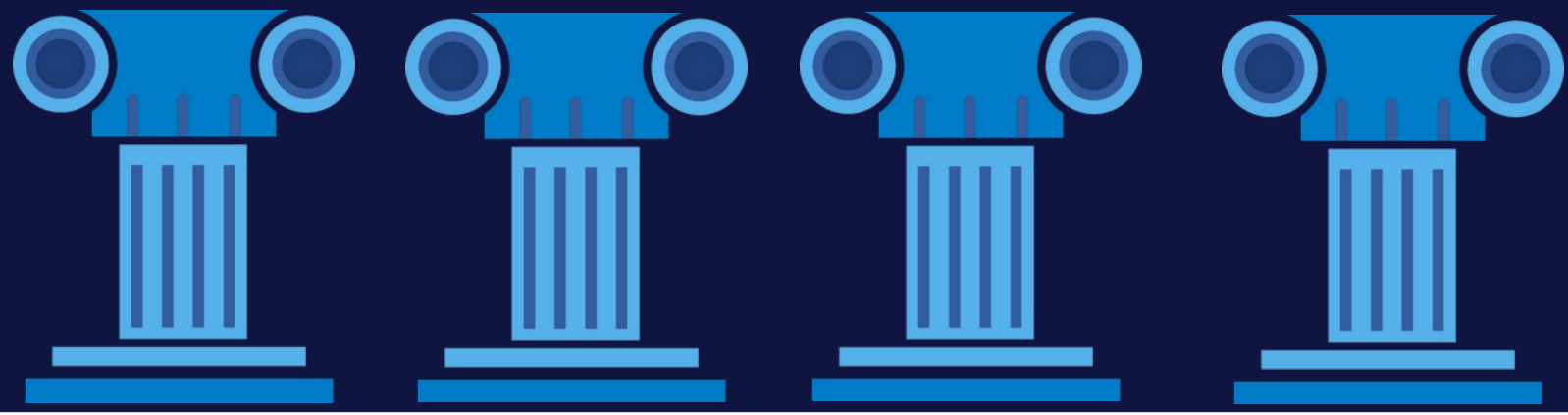
« 4 grands piliers »

ANTICIPATION

STRATÉGIE

OPÉRATIONNEL

FORMATION

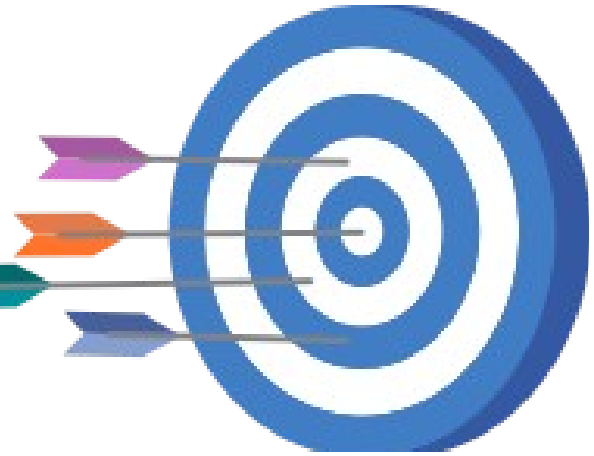


MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# « Objectifs »

Élaborer la stratégie ministérielle de lutte contre la cybercriminalité Mieux anticiper / connaître les cybermenaces (rapport annuel) Coordonner les moyens cybers capacitaires du MIOM Assurer un soutien opérationnel et un appui aux enquêtes judiciaires Élaborer, actualiser et diffuser des contenus de formation destinés aux FSI et agents du MIOM (CNF-Cyber de Lille) Coordonner et assurer le suivi des actions de sensibilisation et de prévention à destination des collectivités et entreprises Coordonner les travaux de recherche, de développement et de prospection liés à la cybercriminalité, aux cybermenaces et à la résilience numérique de la société.

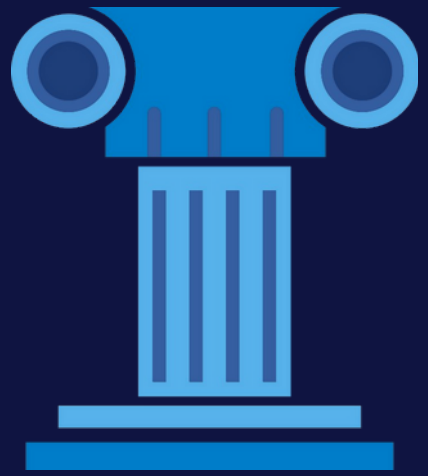


MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

« 4 grands piliers »

## ANTICIPATION



- Renseigner sur les menaces cyber et les modes d'actions des groupes cybercriminels *(rapport annuel / synthèses / flashs d'alertes)*

- Développer les partenariats et les échanges

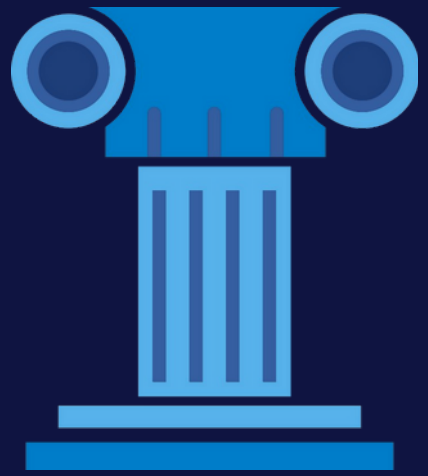
- Mener des actions de sensibilisation à la gestion de crise

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

# COMCYBER-MI

« 4 grands piliers »

## STRATÉGIE



- Élaborer, animer et coordonner la stratégie ministérielle de lutte contre la cybercriminalité

- Coordonner et assurer le suivi des actions de sensibilisation et de prévention à destination des collectivités et entreprises

- Développer les partenariats, coordonner les travaux de recherche et de développement liés à la cybercriminalité, aux cybermenaces et à la résilience de la société

- Développer et coordonner les partenariats à l'international

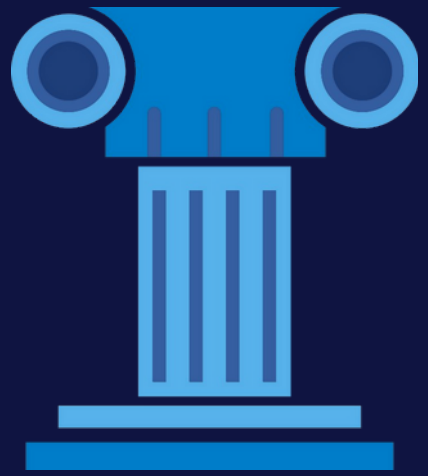
- Anticiper et participer à l'évolution du cadre juridique/réglementaire

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

« 4 grands piliers »

## OPÉRATIONNEL



Assurer un soutien opérationnel et un appui aux enquêtes judiciaires au travers de co-saisines avec des services d'enquête sur des compétences rares :

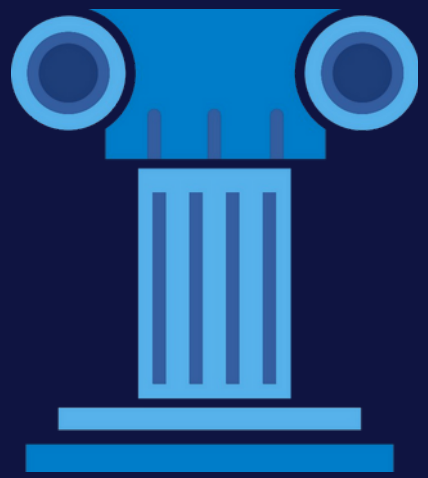
- traçabilité des cryptoactifs
- traitement de la donnée de masse
- expertise technique

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

« 4 grands piliers »

# FORMATION



Le Centre National de Formation Cyber
créé le 1er août 2022 est rattaché au COMCYBER-MI.

Il est chargé d'élaborer , d'actualiser

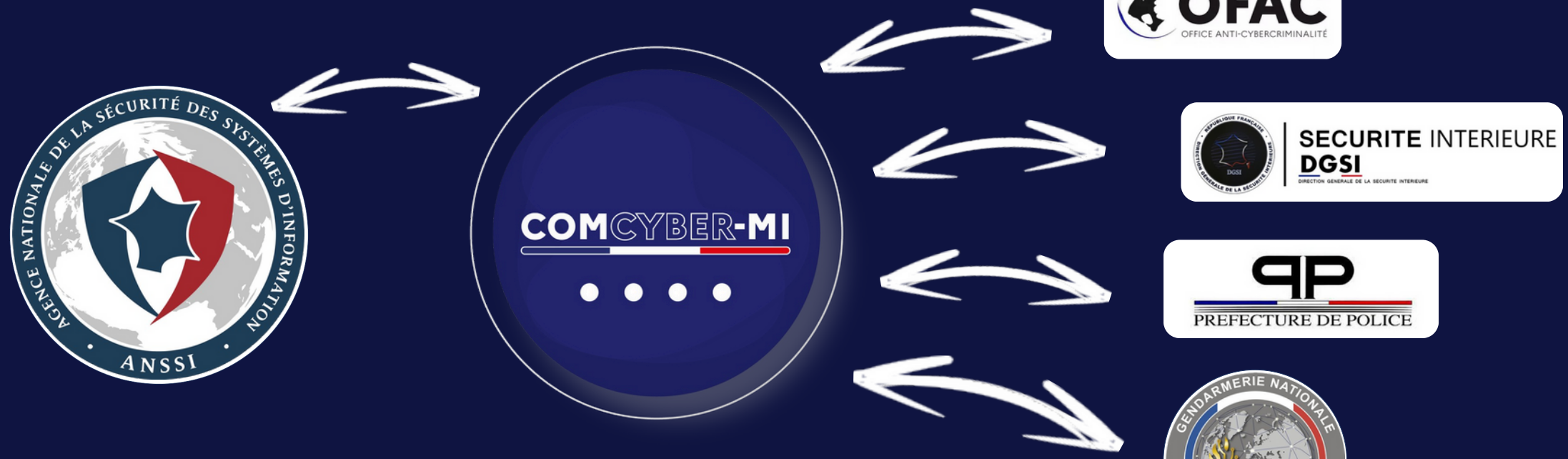
et diffuser des contenus de formation

destinés aux FSI et agents du MIOM

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

# COMCYBER-MI

« Le COMCYBER-MI dans l'écosystème cyber »

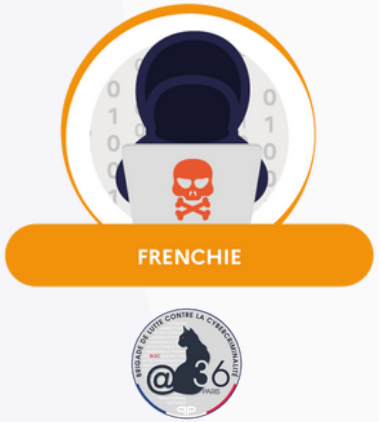


MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

# Les résultats : quelques enquêtes marquantes





MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# *Les enjeux de la cybercriminalité en 2024*

- *I- État de la menace*
- *II- L'État se structure pour faire face*
- *III- Tous concernés …*

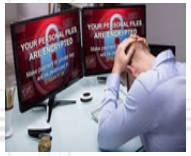
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
*Liberté*
*Égalité*
*Fraternité*

# Tous concernés
...

## UN ÉCOSYSTÈME CYBERCRIMINEL PLUS SOPHISTIQUÉ ET PROFESSIONNEL

### Une menace sérieuse...


- Augmentation de la surface d'attaque
avec une croissance de la digitalisation et de la numérisation
*(facturation, travail à distance, services clients en ligne, utilisation du cloud, automatisation et intelligence artificielle.....)*



- Impacts opérationnels : perturbation voire arrêt de l'activité, retard dans les traitements de commande, perte de revenus, mise en chômage partiel...

- Réputation : perte de confiance du public, dommage à long terme à l'image de l'établissement.

- Coûts financiers : rançons, amendes (RGPD), coûts de réparation et remédiation.


- Conséquences légales : responsabilités légales en cas de fuite de données, potentielles poursuites judiciaires.

### ...trop peu prise en compte

Une menace numérique infinie, rapide, protéiforme, internationale
... et dangereuse pour la stabilité démocratique

1 plainte / 250 faits
tentés ou commis.

6 000 Md€
coût mondial
de la
cyberdélinquance.

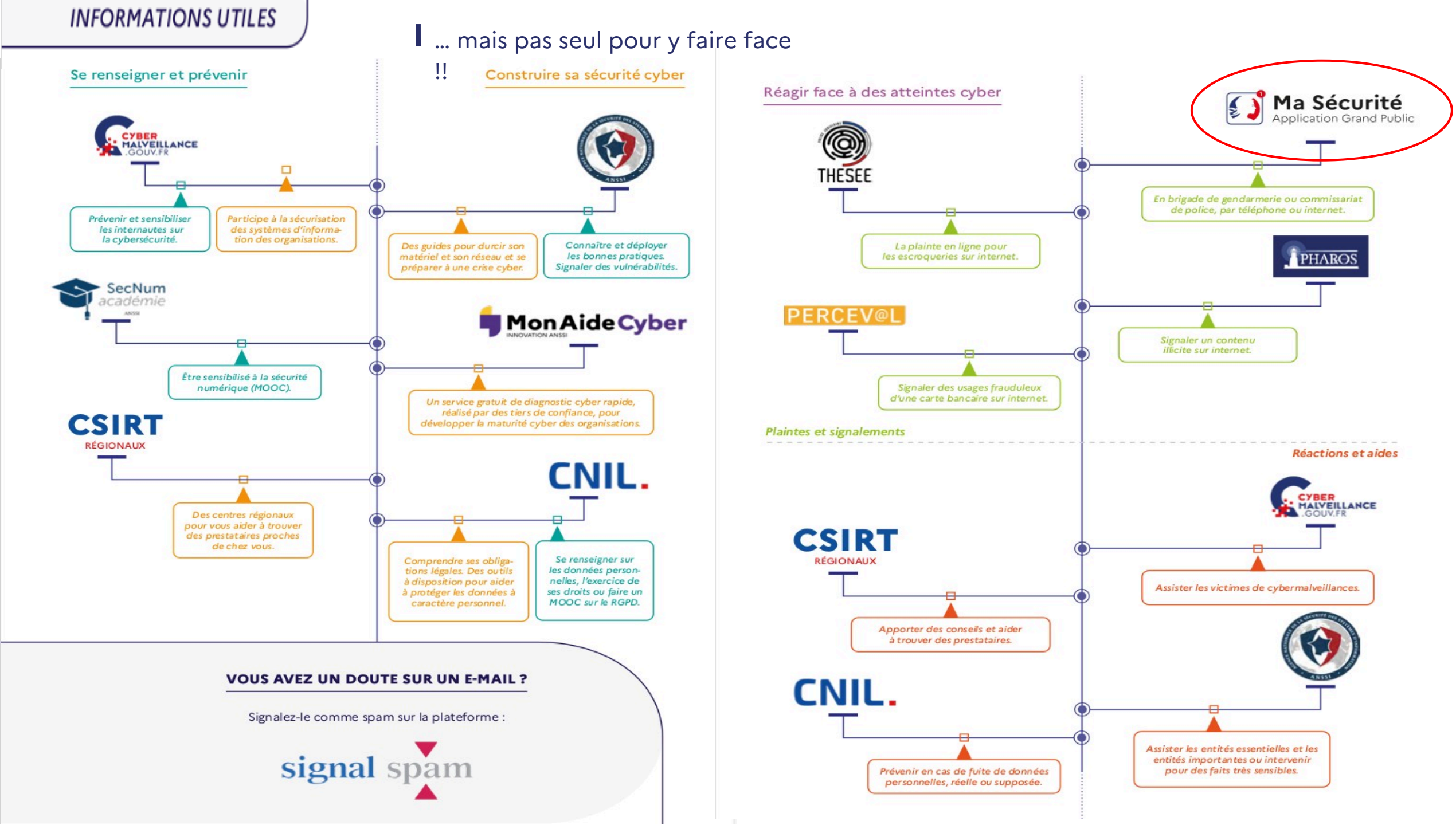
62,5 % de la population mondiale utilise **internet**

58,4 % de la population mondiale utilise les **réseaux sociaux**

**13,5 nouveaux usagers / seconde !**

29 milliards d'**objets connectés** d'ici 2030

# … mais pas seul pour y faire face !!



# CONTACTS UTILES

Ma Sécurité
Application Grand Public

*Le 17 pour contacter les forces de l'ordre par téléphone ou sur le site :*

masecurite.interieur.gouv.fr[1]

THESEE

***THESEE** pour les escroqueries sur internet :*

service-public.fr/particuliers/vosdroits/N31138

PHAROS

***PHAROS** pour signaler des contenus illicites :*

internet-signalement.gouv.fr/PharosS1

PERCEV@L

***PERCEVAL** pour signaler une fraude à la carte bancaire :*

service-public.fr/particuliers/vosdroits/R46526

CYBER MALVEILLANCE .GOUV.FR

***Cybermalveillance** permet de s'informer sur les menaces et trouver de l'assistance en tant que victime :*

cybermalveillance.gouv.fr

CSIRT RÉGIONAUX

*Les **CSIRT régionaux** répondent aux demandes d'assistance et mettent en relation avec des partenaires de proximité :*

cert.ssi.gouv.fr/csirt/csirt-regionaux

ANSSI

***L'ANSSI** assiste les entités essentielles et les entités importantes, fournit des guides et met à disposition un MOOC cyber pour tous :*

cyber.gouv.fr

CNIL.

*La **CNIL** est le régulateur des données personnelles. Elle accompagne les professionnels et aide les particuliers :*

cnil.fr

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# Le rôle de l'équipe juridique

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# Cybersécurité et SI : la nécessité de la conformité

Les systèmes d'information des entreprises, quelle que soit leur taille, sont de plus en plus exposés aux risques de cyberattaques, du vol de données à la

La mise en conformité règlementaire, en matière de cybersécurité, devient un enjeu majeur.
Elle n'est pas sans impact pour les systèmes d'information et doit être prise en compte dès la phase de conception.

loi de programmation militaire

Directive européenne NIS et NIS 2

RGPD

Privacy by design ? Compliance by design

**Version en vigueur au 13 janvier 2025**

# Code des assurances

## Partie législative (Articles L100-1 à L561-1)

### Livre Ier : Le contrat (Articles L100-1 à L195-1)

Article L100-1

#### Titre II : Règles relatives aux assurances de dommages (Articles L121-1 à L12-10-1)

##### Chapitre X : L'assurance des risques de cyberattaques (Article L12-10-1)

Naviguer dans le sommaire du code

### Article L12-10-1

Création LOI n°2023-22 du 24 janvier 2023 - art. 5 (V)

Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime.

Le présent article s'applique uniquement aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle.

*NOTA :*
*Conformément au II de l'article 5 de la loi n° 2023-22 du 24 janvier 2023, ces dispositions entrent en vigueur trois mois après la promulgation de la présente loi.*

Versions | Liens relatifs

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI

# POURQUOI DÉPOSER PLAINTE

## VICTIME D'UNE CYBERATTAQUE

CONTACTER LE 17 OU LA BNUM SUR **Ma Sécurité** Site internet

**DÉPASSEZ VOS CRAINTES**

- Seul face à la crise ?
- Une plainte, est-ce utile pour sortir de la crise ?
- Perdre du temps précieux dans la crise
- Risquer d'entâcher la confiance
- Ralentir les actions de remédiation visant la reprise d'activité
- Préserver l'image de l'entreprise

Le dépôt de plainte permet **L'INTERVENTION D'UN BINÔME ENQUÊTEUR / TECHNICIEN** capable de conseiller sur les investigations numériques et les choix stratégiques à mener.

Des **EXPERTS DE LA GESTION DE CRISE DE LA GENDARMERIE** peuvent prendre en charge les interactions avec le cyberdéliquant.

Alerter au plus tôt c'est **PRÉSERVER LES PREUVES NUMÉRIQUES** pour identifier l'attaquant et bénéficier de conseils pour faire cesser l'attaque.

Anticiper le dépôt de plainte permet de faire gagner du temps.

La **TRANSPARENCE** implique la **CONFIANCE.**

L'intervention de la GN peut **RASSURER** l'écosystème de l'entreprise sur la gestion de l'incident.

L'intervention de la gendarmerie n'a **AUCUN IMPACT** sur la reprise d'activité. Les experts de la gendarmerie recueillent les éléments de preuves en étroite collaboration avec les équipes opérationnelles et les sociétés de remédiation.

La victime conserve à tout instant la maîtrise de sa communication de crise.

**POUR AGIR ENSEMBLE**

- Être reconnu en tant que victime
- Agir en citoyen
- Lutter contre la cyber-criminalité
- S'entourer d'un allié dans la crise
- Se protéger de futures attaques
- Faire valoir ses droits

Victime mais pas coupable !
Le dépôt de plainte permet d'obtenir **RÉPARATION DU PRÉJUDICE.**

Le dépôt de plainte est le seul moyen **D'INFORMER** les forces de sécurité intérieure des menaces qui pèsent sur les citoyens.

Signaler c'est **PROTÉGER ET PARTICIPER À L'EFFORT COLLECTIF.**

Le dépôt de plainte permet de **RECUEILLIR DES ÉLÉMENTS DE PREUVES NUMÉRIQUES** qui permettent d'investiguer et de peser sur les organisations cybercriminelles.

La gendarmerie vous **ACCOMPAGNE DANS LA GESTION DE LA CRISE,** grâce à des équipes projetables aux compétences intégrées, dédiées à l'identification des cybercriminels.

Le dépôt de plainte permet de bénéficier de **L'EXPERTISE DE LA GENDARMERIE** dans la protection de l'entreprise.

La gendarmerie peut détenir des éléments permettant à l'entreprise de récupérer ses données en cas d'attaque par rançongiciel.

**L'ASSURANCE CYBER** permet à l'entreprise de limiter les conséquences économiques d'une cyberattaque.

La LOPMI (Art.5) soumet l'indemnisation des préjudices d'une cyberattaque au **DÉPÔT DE PLAINTE DE L'ENTREPRISE.**

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

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

# La cyber-résilience pour les services juridiques

COMMANDEMENT DU
COM
01000011 0100
01000011 010
01000101 0
0010110
01
DANS LE

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

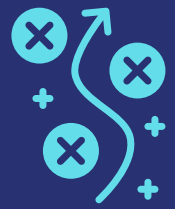
COMCYBER-MI
« Nos forces, pour votre cyber-protection »

# Qu'est-ce que la crise cyber ?

> Déstabilisation immédiate et majeure du fonctionnement courant d'une organisation en raison d'une ou de plusieurs actions malveillantes sur ses services et ses outils numériques - ANSSI

Double temporalité

Lieux multiples



Adaptation de la menace

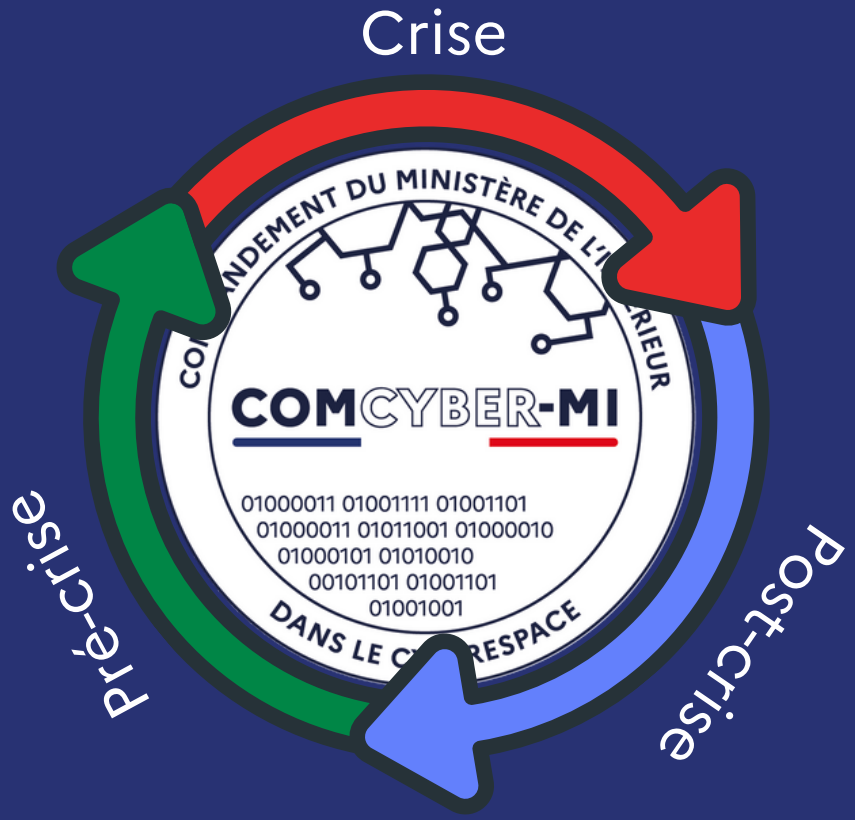
Incertitude

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

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

# Cycle de vie de la gestion de crise

ANTICIPATION
RÉSILIENCE
CAPITALISATION



MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Chef d'escadron Matthieu Rousseau
Département de la gestion des crises cyber



# ANTICIPATION

**1 - S'assurer de la conformité légale et règlementaire** (RGPD, NIS, DORA...)


**2 - S'assurer de la teneur et de la qualité des contrats :**

- assurance pour la couverture du risque cyber
- prestataires informatiques
- partenaires et fournisseurs

**3 - Sensibiliser ses équipes :**

- aux risques juridiques spécifiques
- aux bonnes pratiques numériques

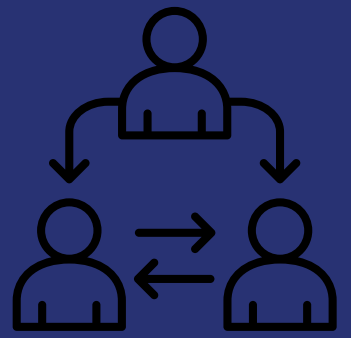
MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Chef d'escadron Matthieu Rousseau
Département de la gestion des crises cyber



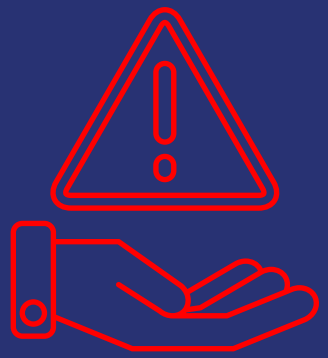
# ANTICIPATION

**4 - Contrôler sa capacité à continuer l'activité**



**5 - Se coordonner avec différents services :**

- DSI / RSSI
- Communication



**6 - Evaluer l'exposition juridique au risque cyber**

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Chef d'escadron Matthieu Rousseau
Département de la gestion des crises cyber

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

# RÉSILIENCE

## 1 - A prévenir :

- Assurances
- Gendarmerie / Police Nationale
- CNIL

## 2 - Fuite de données sensibles et personnelles :

- coordination avec DSI / RSSI
- déclaration CNIL
- notification aux parties prenantes

## 3 - Coordination des équipes :

- internes
- externes

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Chef d'escadron Matthieu Rousseau
Département de la gestion des crises cyber



# RÉSILIENCE

**4 - Préserver les preuves :**

- judiciaires
- légales et règlementaires

**5 - En matière de communication :**

- appliquer la procédure
- contrôler les EDL

MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Chef d'escadron Matthieu Rousseau
Département de la gestion des crises cyber

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

# CAPITALISATION

**1 - Contribuer au Retour d'Expérience :**

- bonnes et mauvaises pratiques
- amélioration des contrats
- humilité et courage intellectuel

**2 - Prise en compte des litiges et conflits :**

- identification des responsabilités
- protection de la propriété intellectuelle
- litiges commerciaux

**3 - Participer aux exercices :**

- tester ses procédures internes
- développer les compétences des collaborateurs

MINISTÈRE
DE L'INTÉRIEUR
*Liberté*
*Égalité*
*Fraternité*

COMCYBER-MI