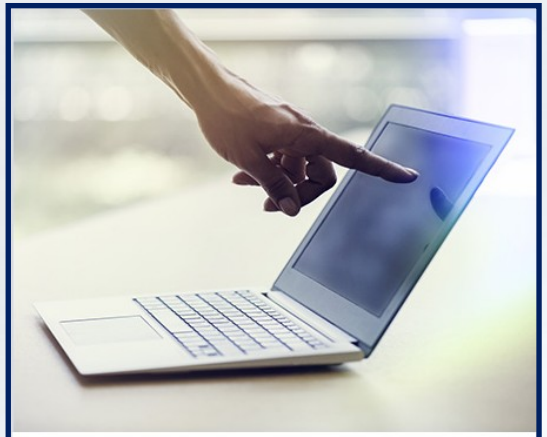
Pourquoi et comment déposer plainte ?

L’état de la menace en région NA

Attaque crapuleuse



Escroquerie financière

Malveillance

Intelligence économique

Rançongiciels DDOS

Faux ordres de virement

Attaques internes

Exfiltration de données Pré-positionnement

Pourquoi déposer plainte ?

Pour la victime :

- comprendre les raisons et/ou le contexte de l'attaque
- identifier les modes opératoires
- identifier ses vulnérabilités
- récupérer les données métiers et limiter leur diffusion
- obtenir le droit à réparation du préjudice subi
- anticiper une nouvelle attaque

Pourquoi déposer plainte ?

Pour l'État :

- identifier et anticiper les évolutions de la menace
- mettre en place une protection adaptée et coordonnée au niveau européen

L’enquête policière

Une attaque informatique a eu lieu, qui va effectuer les 1ères constatations techniques ?

Service de police

Soi-même

Huissier

Prestataire

Quelles sont les 1ères actions à mettre en place ?

Isoler ! ***Ne pas éteindre les postes infectés mais couper tous les accès réseaux***

Confiner - ***Mettre en quarantaine les postes infectés et les supports amovibles***

Sauvegarder ***(journaux d'activité, docs, emails, fichiers, trafic réseau) + copie des supports / acquisition mémoire vive***

Collecter

Communiquer

Comment déposer plainte ?

Services

Personne morale ou physique

1 an
contraventions

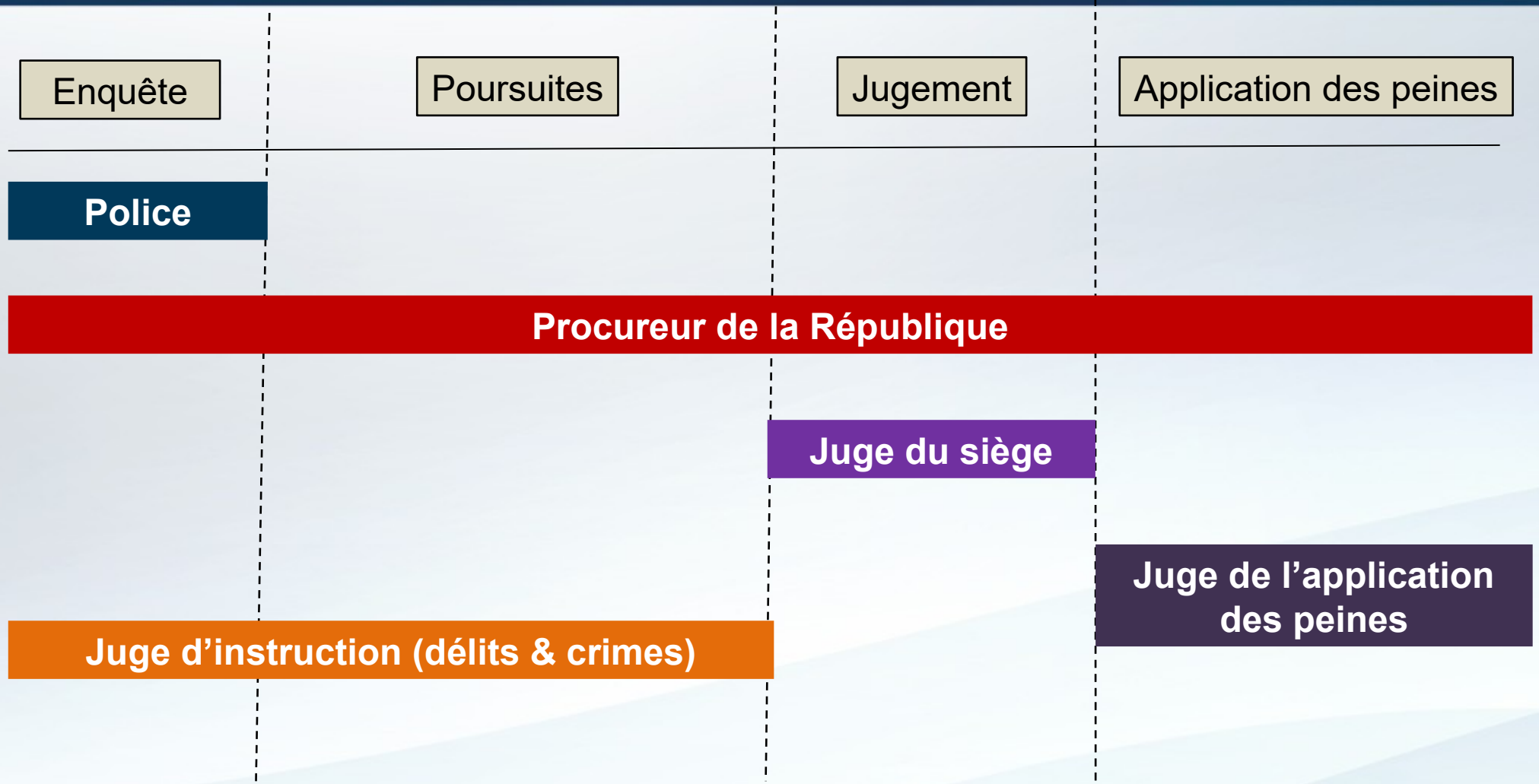
3 ans
délits

10 ans
crimes

Délais pour porter plainte

En Nouvelle Aquitaine : cybermenaces-bordeaux@interieur.gouv.fr

Et aprés ?


Enquête
Poursuites
Jugement
Application des peines
Police
Procureur de la République
Juge du siège
Juge de l'application des peines
Juge d'instruction (délits & crimes)

États membres de l’union européenne et plusieurs pays partenaires non membres de l’union européenne et organisations internationales extérieures à l'UE pour lutter contre la grande criminalité internationale

A notre disposition des canaux de communications internationaux et des procédures bien rodées
SIENA, GEL DE DONNEES (H24/7),
BCN (Interpol)

Le Parquet de Paris avec
la section J3 en charge de la Cybercriminalité sur le plan national et international.

assistance d’EuroJust avec des procédures de coopération internationale

12 TARGETED FOR INVOLVEMENT IN RANSOMWARE ATTACKS AGAINST CRITICAL INFRASTRUCTURE

29 Oct 2021

Press Release

These cyber actors represented a dangerous combination of aggressive disruption and high-stake targets

A total of 12 individuals wreaking havoc across the world with ransomware attacks against critical infrastructure have been targeted as the result of a law enforcement and judicial operation involving eight countries.

These attacks are believed to have affected over 1 800 victims in 71 countries. These cyber actors are known for specifically targeting large corporations, effectively bringing their business to a standstill.

POLICE NATIONALE

EUROPOL

POLICE NATIONALE · DIRECTION CENTRALE DE LA POLICE JUDICIAIRE ·

FIVE AFFILIATES TO SODINOKIBI/REVIL UNPLUGGED

08 Nov 2021

Press Release

Suspected of about 7 000 infections, the arrested affiliates asked for more than 200 million euros in ransom

POLICE NATIONALE

FICHE DE CONTACT
RÉSEAU DES RÉFÉRENTS CYBERMENACES DE LA POLICE NATIONALE

La Police judiciaire vous propose un point de contact unique pour le territoire : **Nouvelle-Aquitaine**

cybermenaces-bordeaux@interieur.gouv.fr

POLICE NATIONALE

Le réseau des référents cybermenaces de la Police nationale est une structure innovante composée de :

- **Réservistes** issus du monde de l'entreprise engagés dans la lutte contre la cybercriminalité
- **Policiers spécialisés**
- **Investigateurs en cybercriminalité**
- **Professionnels et Institutions partenaires**

POLICE NATIONALE · DIRECTION CENTRALE DE LA POLICE JUDICIAIRE