AUDITION COMMISSION DE SÉCURITÉ AFE
JÉRÔME NOTIN – 17CYBER

Préambule

La plateforme cybermalveillance.gouv.fr, lancée en 2017, a été conçue afin d'accompagner particuliers, entreprises et collectivités confrontés à des incidents numériques en proposant un diagnostic, des recommandations techniques adaptées et une mise en relation avec des prestataires de proximité pour une intervention rapide et efficace. Depuis le 17 décembre dernier, cette plateforme porte également le nouveau dispositif « 17cyber.fr », destiné à renforcer l'assistance judiciaire et technique des victimes, en permettant notamment un échange direct avec des policiers ou des gendarmes pour faciliter la judiciarisation des faits.

Comme l'a souligné le Sénateur Olivier Cadic, plus nous dématérialisons et modernisons les services consulaires, plus nous devenons exposés à des risques croissants et donc aux cyberattaques comme l'usurpation d'identité. En effet, cette évolution numérique, si nécessaire et attendue par nos concitoyens à travers le monde, comporte son lot de risques. La dématérialisation impose une responsabilité accrue en matière de cybersécurité, car la vulnérabilité de nos systèmes numériques expose chacun d'entre nous à des risques sérieux avec parfois des conséquence dramatiques en particulier pour nos concitoyens qui auront plus de difficultés à réaliser des démarches administratives depuis l'étranger. C'est pourquoi l'intégration et l'accessibilité de services dédiés comme le « 17cyber.fr » pour les Français à l'étranger doivent être soutenues et promues activement.

I. Historique et contexte de création des plateformes

1. Cybermalveillance.gouv.fr (2017)

- Créée dans le cadre de la stratégie nationale de sécurité du numérique (2015).
- Objectif : Assistance aux victimes de cyberattaques (particuliers, entreprises, collectivités).
- Statut : Groupement d'intérêt public (GIP) réunissant acteurs publics et privés.

2. 17cyber.gouv.fr (2024)

- Lancée le 17 décembre 2024, après plusieurs reports.
- Initiative portée par le sénateur Olivier Cadic (2019) et proposée par le Président de la République en janvier 2022.
- Objectif : Guichet unique numérique pour la cybercriminalité, équivalent du « 17 » en ligne.
- Collaboration entre ANSSI, ministère de l'Intérieur, police, gendarmerie et justice.
- Développé après des échanges avec les forces de l'ordre et un projet pilote étendu progressivement.

II. Missions et fonctionnement des plateformes

1. Cybermalveillance.gouv.fr

- **Assistance aux victimes** : Diagnostic, conseils pratiques, orientation vers des prestataires labellisés.
- **Prévention** : Production et diffusion de contenus pédagogiques.
- **Veille et alerte** : Remontée d'informations aux autorités judiciaires.

2. 17cyber.gouv.fr

- **Interface 24/7 avec policiers et gendarmes** :
  - Aide à la judiciarisation des faits cyber via échanges par messagerie instantanée 24/7 avec des policiers et des gendarmes sur 11 des 52 cybermalveillances traitées par Cybermalveillance.gouv.fr
  - Pas de possibilité à date de dépôt de plainte dématérialisé (actuellement limité à certaines infractions à des infractions aux biens contre un auteur inconnu : vol de téléphone, dégradation de véhicule, etc.).
- **Évolution** : Passage de 11 à 52 catégories de menaces cyber prises en charge.

III. Limites actuelles et problématique des Français de l'étranger

1. Accès restreint aux plaintes en ligne

- Les expatriés peuvent consulter 17Cyber..gouv.fr, mais ne peuvent pas déposer plainte en ligne
- Les plaintes en ligne sont limitées aux infractions traditionnelles (vols, atteintes aux biens physiques, contre X).
- Détournement du système : Certains Français de l'étranger renseignent une fausse adresse en France pour déposer plainte.

2. Conséquences

- Obligation de déplacement en France pour porter plainte.
- Absence de cartographie de prestataires de cybersécurité à l'étranger.
- Chiffre noir élevé : Beaucoup de victimes renoncent à porter plainte faute de solution adaptée.

3. Objectif clé

- Élargir la plainte en ligne aux infractions cyber pour permettre aux Français de l'étranger et du territoire national de porter plainte à distance.

IV. Statistiques et impact des plateformes

Fréquentation de Cybermalveillance.gouv.fr :

- 3,8 millions de visiteurs en 2023 → 5,4 millions en 2024.
- Pic d'usage lors de fuites de données massives (mutuelles de santé, France Travail, Free).

Bénéfices attendus du dépôt de plainte en ligne :

- Désengorgement des commissariats et gendarmeries lors de cyberattaques massives.

- Optimisation des enquêtes judiciaires grâce à la collecte d'éléments techniques (adresses IP, transactions en bitcoin, etc.).

V. Enjeux à résoudre

- **Cadre législatif inadapté** : Le champ infractionnel cyber n'est pas encore de la compétence de plainte en ligne

  https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049607599
- **Accès impossible aux plaintes cyber pour les expatriés** :
  - Aucun dispositif de plainte en ligne depuis l'étranger.
  - Risque accru pour les Français à l'étranger, souvent isolés face à la cybercriminalité.
- **Écart entre les victimes réelles et celles qui déposent plainte** : Dispositifs trop complexes, manque de lisibilité, impossibilité de déposer plante dans un commissariat de police pour les Français de l'étranger.

VI. Propositions et attentes vis-à-vis de l'AFE

1. Demande principale : élargir le champ infractionnel des plaintes en ligne

- Intégrer explicitement les infractions cyber au dispositif de plainte en ligne.
- Adapter le décret **n°2024-478 du 27 mai 2024** pour inclure les cyberinfractions.

2. Actions concrètes pour l'AFE

- **Adoption d'une résolution officielle** demandant au gouvernement l'extension du champ infractionnel aux délits cyber afin de leur permettre de porter plainte depuis l'étranger.
- **Renforcement de la visibilité des plateformes** :
  - Intégration d'un lien ou widget vers Cybermalveillance et 17Cyber sur les sites des consulats et ambassades.
  - Diffusion de ces outils par le réseau diplomatique français.
- **Campagne nationale de sensibilisation** sur la cybercriminalité, calquée sur le modèle de la sécurité routière. *(Suggestion J. Notin)*

VII. Problème actuel : Complexité des dispositifs cyber

- Multiplication des plateformes (Pharos, Perceval, Thésée, Cybermalveillance, 17Cyber) rendant difficile l'orientation des victimes.
- Même les forces de l'ordre peinent à identifier le bon service à mobiliser.

Objectifs du 17 Cyber

- **Simplifier l'accès aux victimes** via une porte d'entrée unique.
- **Automatiser l'orientation** :
  - Conseils préventifs immédiats.
  - Accès direct au dépôt de plainte en ligne.

Menaces cyber les plus fréquentes

- **Phishing (hameçonnage)** : faux SMS/emails frauduleux.
- **Fraude à la réparation informatique** : faux techniciens extorquant des victimes (140 000 cas estimés en 2024).
- **Arnaques bancaires** : escroqueries de faux conseillers.

VIII. Illustration concrète : impact des cyberattaques et solutions judiciaires

- **Succès judiciaires grâce aux plateformes** :
  - Exemples de cybercriminels condamnés à 5-8 ans de prison grâce aux signalements centralisés.
  - Affaire "cryptoporno" : identification et arrestation des auteurs grâce aux plaintes collectées.
- **Blocage d'accès depuis l'étranger** :
  - Certains sites officiels français (ex : Ameli.fr) inaccessibles temporairement pour des raisons de sécurité.
  - Urgence d'un accès garanti aux expatriés aux services de cybersécurité.

IX. Anticipation des enjeux futurs et nécessité d'agir rapidement

- **Contexte de digitalisation croissante** (vote électronique, démarches en ligne) → nécessité de garantir la cybersécurité des expatriés.
- **Risque majeur en cas de cyberattaque massive** :
  - Exposition accrue des Français de l'étranger.
  - Incapacité actuelle à déposer plainte à distance = vulnérabilité renforcée.