MINISTÈRE
DE L'INTÉRIEUR
*Liberté
Égalité
Fraternité*

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

# La MInute Cyber 03


## *LA CYBERCRIMINALITÉ DANS LE SOCTA 2025*

Le 18 mars dernier, la directrice exécutive d'Europol Catherine De Bolle a présenté à la presse le nouveau rapport « SOCTA » *(Serious and Organised Crime Threat Assessment)*. Ce rapport constitue la publication majeure de l'agence Europol, fournissant une vue d'ensemble des menaces générées par la criminalité grave et organisée en Europe. Publié tous les quatre ans, il identifie les principales activités criminelles, la dynamique des réseaux criminels et les tendances émergentes.

Dans sa dernière édition, le SOCTA met en évidence le caractère transversal de la dimension cyber et technologique du crime organisé en Europe, engendrant des transformations durables et structurelles.

Ainsi, il souligne le fait que le crime organisé se « nourrit » du cyber-espace. Les infrastructures numériques constituent le moteur des actions criminelles, en permettant aux activités illicites de se développer et de s'adapter à une vitesse sans précédent. Presque toutes les formes de criminalité grave et organisée ont une empreinte numérique, que ce soit en tant qu'outil, cible ou facilitateur. De l'escroquerie en ligne au rançongiciel, en passant par le trafic de drogue et le blanchiment d'argent, Internet est devenu le principal lieu d'exercice de la criminalité organisée. Les réseaux criminels exploitent de plus en plus l'infrastructure numérique pour dissimuler leurs activités aux forces de l'ordre, tandis que les données apparaissent comme la nouvelle monnaie du pouvoir – volée, échangée et exploitée par les acteurs criminels.

De même, le SOCTA insiste sur le facteur accélérateur que constituent l'IA et les technologies émergentes dans l'expansion du crime organisé. Et donc, les mêmes qualités qui rendent l'IA révolutionnaire – accessibilité, adaptabilité et sophistication – en font également un outil puissant pour les réseaux criminels. Ces technologies automatisent et élargissent les actions criminelles, les rendant plus évolutives et plus difficiles à détecter.

De manière plus détaillée, le SOCTA identifie sept menaces criminelles dont l'expansion est la plus rapide en Europe. Il s'agit des cyberattaques, des escroqueries en ligne, de l'exploitation sexuelle des mineurs en ligne, du trafic de migrants, du trafic de drogue, du trafic d'armes à feu, ainsi que du trafic de déchets.

Le rapport s'appuie sur les contributions des États membres de l'UE et de plusieurs États tiers, le tout, enrichi grâce à l'expertise d'Europol en matière de renseignement criminel. Il offre des perspectives stratégiques qui permettent d'orienter les politiques de l'UE et l'action des forces de sécurité intérieure de l'UE. C'est effectivement sur la base du rapport SOCTA que les États membres fixeront des priorités en matière de lutte contre la criminalité organisée pour les quatre prochaines années (2026-2029), lesquelles seront déclinées en plans d'action opérationnels dans le cadre du programme EMPACT *(European Multidisciplinary Platform Against Criminal Threats)*, le vaisseau amiral de l'UE en matière de lutte contre la criminalité organisée[1].

1. Pour l'actuel cycle EMPACT 2022-2025, la France dirige quatre plans d'action opérationnels, dont deux relèvent du domaine de la cybercriminalité : les cyber-attaques et les escroqueries en ligne.

## *LES LOGICIELS ESPIONS : UNE MENACE SILENCIEUSE*

Les logiciels espions (« *spywares* ») se multiplient et deviennent l'une des cybermenaces les plus redoutables, leur objectif étant de collecter, sans que les utilisateurs ne s'en aperçoivent, des données sensibles sur les appareils des victimes, comme les identifiants, les coordonnées bancaires, les données de géolocalisation, ou encore les historiques de navigation.

À l'origine ciblant principalement les ordinateurs sous Windows, les *spywares* ont rapidement étendu leur menace aux ordinateurs Mac et vers les *smartphones*, devenus la cible privilégiée en raison de leur utilisation intensive et constante des connexions à Internet. L'infection se produit généralement *via* l'exploitation de vulnérabilités logicielles, le téléchargement d'applications malveillantes déguisées en programmes légitimes, ou encore *via* des réseaux *Wi-Fi* publics non sécurisés.

Le marché des logiciels espions s'est considérablement développé, porté par des entreprises spécialisées telles que NSO Group ou Intellexa. Bien que ces solutions soient destinées officiellement à la lutte contre la criminalité et le terrorisme, elles restent controversées en raison de leur utilisation potentielle contre des opposants politiques, journalistes, ou activistes. Le scandale lié au logiciel Pegasus, capable d'espionner entièrement des *smartphones*, illustre ces dérives.

Les conséquences pour les victimes peuvent être graves. Citons, à titre d'exemple, les atteintes profondes à la vie privée. Dans certains cas extrêmes, la sécurité nationale peut être menacée. Aux vues de ces menaces, le cadre juridique français est clair, et les articles 323-1 à 323-3 du Code pénal répriment sévèrement l'utilisation et la diffusion illégales de ces outils.

Pour prévenir ces risques, plusieurs bonnes pratiques sont recommandées. Ainsi, maintenir ses systèmes à jour, utiliser un antivirus performant, activer l'authentification multifactorielle, éviter les réseaux *Wi-Fi* non sécurisés et être vigilant face aux téléchargements ou pièces jointes suspects sont à mettre en œuvre.

Détecter un *spyware* est possible en surveillant certains signaux inhabituels comme des ralentissements inexpliqués des appareils, des transactions bancaires suspectes, ou encore des comportements anormaux de navigation Internet.

En cas d'infection avérée, des outils spécifiques existent pour supprimer ces menaces, et dans les cas les plus graves, une réinitialisation complète des appareils est nécessaire.

Vigilance et prévention restent donc les maîtres mots pour se protéger.

## *SENSIBILISATION AUX RISQUES CYBER CHEZ LES PLUS JEUNES : L'OPÉRATION CACTUS*

Suite à son expérimentation réussie en 2024, l'opération CACTUS a été étendue du 19 au 21 mars 2025 à tout le territoire national, incluant les Outre-mer. Cette action de sensibilisation aux risques liés aux cybermenaces à destination des 11/18 ans, mobilisait, à nouveau, et de concert, le ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche, le ministère de l'Intérieur (COMCYBER-MI), Cybermalveillance.gouv.fr (GIP ACYMA), les magistrats de la section de lutte contre la cybercriminalité et la Commission nationale de l'informatique et des libertés (CNIL).

Ainsi, plus de 2,5 millions d'élèves, au sein de plus de 4 700 collèges et lycées, ont reçu, *via* les espaces numériques de travail (ENT), un message les incitant à cliquer sur un lien pour se procurer gratuitement des jeux vidéos piratés. Parmi ces élèves, près d'1 sur 12 ont cliqué sur le lien, redirigeant vers un message de sensibilisation contenant une vidéo.

Cette action de sensibilisation aux risques d'hameçonnage s'est accompagnée de séances de sensibilisation pédagogiques, menées à plusieurs voix dans des établissements volontaires.

Conçue de manière collaborative, l'opération CACTUS s'inscrit, enfin, dans une démarche de plus long terme, les partenaires précédemment cités ayant travaillé à l'élaboration de *kits* de sensibilisation destinés aux équipes pédagogiques.

## *Pour aller + loin...*

### *L'exercice DEFNET 2025 : une mobilisation des Armées, mais aussi de services de l'État, dont le COMCYBER-MI*

Conduit depuis 2014, sous l'autorité du Commandement de la cyberdéfense (COMCYBER), DEFNET est un exercice majeur annuel de la cyberdéfense militaire.

Durant deux semaines, du 17 au 28 mars 2025, toute la chaîne de cyberdéfense du ministère des Armées s'est entraînée à réagir à différents incidents de grande ampleur, sur les réseaux déployés en opérations, mais aussi sur le territoire national. L'objectif de cet exercice est de savoir faire face, en cas de combat cyber de haute intensité, à des attaques multiples, sophistiquées et simultanées, renforçant ainsi la préparation opérationnelle en matière de lutte informatique défensive (LID) et de lutte informatique d'influence (L2I).

Le scénario de l'exercice mêlait des enjeux multiples. Les cybercombattants des armées ont été immergés dans un conflit de haute intensité entre deux pays fictifs. L'un deux, membre de l'OTAN, bénéficiait du soutien de la France pour protéger ses frontières. En parallèle du mouvement de troupes à terre, en mer et dans les airs, plusieurs cyberattaques étaient recensées sur les systèmes d'information et systèmes d'armes, dont certains se retrouvaient paralysés. Cette situation, déjà complexe, se dégradait, en outre, par des campagnes de désinformation se multipliant afin de jeter le discrédit sur les actions de l'armée française. Ces dernières attaques mobilisaient les cybercombattants spécialisés en lutte informatique d'influence (L2I).

DEFNET est conçu pour construire et tester une chaîne cyber de bout en bout et fait donc intervenir les acteurs industriels, de même que les partenaires étatiques.

À ce titre, le Commandement du ministère de l'Intérieur dans le cyberespace prêtait son concours dans le champ de l'appui opérationnel et du partage de renseignements issus des investigations. Cela, dans le respect des prérogatives de chacun et du secret de l'enquête.

Ce partage d'expérience dans l'entraînement cyber concourt, *in fine*, au développement d'une coopération opérationnelle éprouvée.

Publication mensuelle éditée par :
Commandement du ministère de l'Intérieur dans le cyberespace
**#LaMInuteCyber n° 03 - MARS 2025**
Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : LCL S. LAMBERT - LCL M. TETU - CEN N. PETITPAS
Conception graphique et maquettage : Mme M. BARREAU

**En attendant le prochain numéro de La MInute cyber, suivez notre actualité :**

*sur LinkedIn et sur X (ex-Twitter) :* ***@ComCyberMI***