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

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

# La MInute Cyber 03


©COMCYBER-MI

## EMPACT : UN MÉCANISME EUROPÉEN DE PREMIER PLAN EN MATIÈRE DE LUTTE CONTRE LA CRIMINALITÉ ORGANISÉE

Dans un contexte où le crime organisé est en perpétuelle évolution, notamment grâce aux nouvelles technologies, le nouveau cycle EMPACT 2026-2029 réaffirme l'importance de la coopération internationale pour lutter efficacement contre ces menaces. Créé en 2010, la *« European Multidisciplinary Platform Against Criminal Threats »* constitue le cadre stratégique européen pour coordonner les actions des États membres et des institutions européennes contre la grande criminalité organisée.

Première étape du cycle, Europol publie tous les quatre ans son rapport *SOCTA (Serious Organised Crime Threat Assessment)*, qui identifie les principales tendances criminelles. Le dernier rapport, publié le 18 mars 2025, souligne l'impact croissant de l'intelligence artificielle et des technologies émergentes dans l'expansion du crime organisé. Ces outils permettent aux réseaux criminels d'automatiser leurs activités, de se masquer plus facilement et de se développer à une vitesse sans précédent. Sur la base de ce diagnostic, les pays membres de l'Union européenne ont défini dix-sept priorités politiques, regroupées en treize plans d'action opérationnels (OAP).

Le ministère de l'Intérieur joue en ce sens un rôle central dans le pilotage des OAP liés à la cybercriminalité au sein du cycle EMPACT 2026-2029. Il pilote ainsi trois des treize OAP, tous liés à la cybercriminalité : un premier touchant aux cyberattaques, piloté par l'OFAC, un second aux escroqueries en ligne, piloté par l'UNCyber, et un troisième relatif aux abus sexuels sur mineurs en ligne, piloté par l'OFMIN.

En plus de piloter ces OAP, le ministère de l'Intérieur participe à différentes actions opérationnelles (OA) dans le cadre de ces plans, notamment en assumant des rôles de chef de file ou de co-chef de file. Par exemple, les composantes du COMCYBER-MI sont impliquées dans des actions telles que la lutte contre les escroqueries en ligne en Afrique, et les travaux du réseau *« InterCOP »* relatif à la prévention de la cyberdélinquance juvénile.

A noter également que la France pilote ou co-pilote d'autres OAP en matière de trafic de stupéfiants de migrants, d'armes, ou encore de criminalité environnementale.

Ces différents OAP bénéficient de fonds européens dédiés, dont l'enveloppe a été substantiellement augmentée pour le nouveau cycle.

Le mécanisme EMPACT est donc bien plus qu'un simple outil opérationnel : c'est une réponse globale, structurée et coordonnée, à la main des Etats-membres de l'UE pour lutter contre la criminalité organisée qui affecte la sécurité des citoyens européens, dans ses dimensions stratégique et opérationnelle.

## Le COMCYBER-MI récompensé !

Mardi 17 mars dernier, à l'occasion de la 15ème édition du Gala des directeurs sécurité au Pavillon Cambon Capucines, le commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI) a eu l'honneur d'être primé.

Après une allocution d'ouverture prononcée par M. le ministre de l'Intérieur Laurent NUÑEZ, la soirée, qui avait pour thème « Souveraineté & Sécurité : Construire une Résilience Collective Public-Privé », a laissé place à une table-ronde, modérée par Mme Virginie CADIEU, ayant réuni de hautes autorités. Étaient en effet présents le général de corps d'armée Aymeric BONNEMAISON, Direction du renseignement et de la sécurité de la défense (DRSD), M. le Préfet Xavier Brunetiere, Directeur de la Protection et de la Sécurité de l'État (SGDSN), et M. Olivier de PAILLERETS, *EVP Strategy, Transformation & Security* (Orange Cyber Défense). À l'issue, devant plusieurs centaines de personnes et par l'intermédiaire du Général de division Patrick TOUAK, le COMCYBER-MI a donc remporté le prix « Coup-de-cœur » du jury, remis par M. Pierre BRAJEUX, Président de TORANN-FRANCE, pour son engagement dans la lutte contre les cybermenaces, au sein de laquelle résilience et coopération demeurent étroitement liées.

Le GDI TOUAK, à l'occasion des traditionnels remerciements, a tenu à souligner le travail au quotidien des personnels du COMCYBER-MI, tout en rappelant que ce prix encourageait *« à poursuivre notre engagement avec les mêmes valeurs, les mêmes principes : humilité, sens du collectif, et partage des informations et des expériences »*.

## Coopération avec le monde universitaire

Du 12 au 14 mars dernier, *Guardia Cybersecurity School*, école parisienne de cybersécurité, organisait son *« GuardiHack »*. Il s'agit d'un challenge de type *« Capture The Flag » (CTF)* d'une durée de 72 heures (non stop), comprenant des épreuves portant sur différents domaines (Crypto, Forensic, Reverse Engineering, Pwn, Web, OSINT, etc.), avec un fil conducteur axé sur la thématique du vol de données. Au total, vingt équipes de cinq joueurs chacune y participaient.

À cette occasion, M. le Commissaire divisionnaire Eric LEVY-VALENSI, adjoint du général de division Patrick TOUAK, chef du COMCYBER-MI, a prononcé un discours d'ouverture. Après être revenu sur les cybermenaces dans leur ensemble, M. LEVY-VALENSI s'est plus particulièrement arrêté sur les vols de données et sur la nécessité d'apporter une réponse adaptée à cette menace hybride. En outre, M. le Commissaire divisionnaire a rappelé l'importance de la coopération de manière générale, à l'image de celle associant le COMCYBER-MI et *Guardia Cybersecurity School*, qui contribue au renforcement de la lutte contre la cybercriminalité.

Aussi, par l'intermédiaire du Capitaine Michaël TOURBIER et de l'Adjudant Loïc CARTIER, la Division de la connaissance, de l'anticipation et de la gestion de crise (DCAGC) du COMCYBER-MI animait un atelier de gestion de crise. Se présentant sous forme de questions auprès des étudiant(e)s de deuxième année, il visait à former ces derniers aux bonnes pratiques à mettre en place durant une crise cyber. Cet exercice, venu compléter le challenge *« GuardiHack »*, a ainsi permis de renforcer la sensibilisation des étudiants sur des sujets d'importance capitale.

## POUR ALLER + LOIN…

### *La cybermenace en France*

Le 11 mars dernier, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié son Panorama de la cybermenace 2025.

Après un pic de signalements observés lors des Jeux olympiques et paralympiques de Paris 2024, l'ANSSI a traité l'an passé 3 586 événements de sécurité (- 18 %). Aussi, elle constate à nouveau que les modes opératoires attaquants (MOA) ciblant les intérêts français sont liés à la Russie et à la Chine, principalement à des fins d'espionnage ou de pré-positionnement, dans un contexte mondial où les tensions géopolitiques se renforcent chaque jour. Au même moment, l'Agence observe que le ciblage d'infrastructures critiques (télécommunications et énergie), *via* des tentatives de sabotage, reste très prisé de ces acteurs.

L'année qui vient de s'écouler a également vu une recrudescence significative d'incidents en lien avec la cybercriminalité, tels ceux liés aux exfiltrations de données. Enfin, l'Agence observe un niveau de cybermenaces élevé, qui n'épargne personne et qui est le fait d'attaquants toujours plus spécialisés, alors que les frontières entre acteurs étatiques et cybercriminels s'érodent.

En somme, *« ce panorama 2025 permet de mieux comprendre et d'anticiper ces cybermenaces, [afin] de contrer, décourager ou au moins complexifier grandement la vie des attaquants »*, selon Vincent STRUBEL, Directeur général de l'ANSSI.

### *Une action judiciaire internationale décisive en matière de lutte contre la cybrecriminalité*

Le 11 mars 2026, les autorités judiciaires de France, des États-Unis et des Pays-Bas, avec le soutien d'Europol et d'Eurojust, ont permis de mettre hors ligne l'infrastructure du groupe Socks escort.com et de la solution de paiement *Bitsidy.com*. L'Allemagne, l'Autriche, la Bulgarie, la Hongrie et la Roumanie étaient associées à l'opération.

En juin 2024, sur un renseignement émanant des autorités américaines signalant qu'une partie de l'infrastructure des serveurs de *Bitsidy.com* se trouvait en France, la section de lutte contre la cybercriminalité du parquet de Paris avait ouvert une enquête préliminaire, confiée à l'Office anti-cybercriminalité (OFAC).

Les investigations initiées ont alors démontré que les cybercriminels exploitaient des failles de sécurité dans des routeurs résidentiels, et des objets connectés pour y injecter un virus. Une fois ces appareils compromis, leurs adresses IP étaient mises à la location. Les clients de *socks escort.com* les utilisaient ensuite pour dissimuler leurs propres adresses IP d'origine et mener des activités criminelles en toute impunité, notamment des attaques *DDoS*. Ce réseau était tentaculaire : le 4 mars 2026, la société *socks escort.com* indiquait sur son site web disposer de 35 915 proxys dans 102 pays, dont 454 en France, 14 720 aux USA, 5 317 au Royaume-Unis et 695 en Italie.

Le démantèlement de ce réseau criminel souligne l'importance de la mise en œuvre d'une coopération internationale dans la lutte contre la cybercriminalité.

Publication mensuelle éditée par :
Commandement du ministère de l'Intérieur dans le cyberespace
**#LaMInuteCyber n° 03 - MARS 2026**
Directeur de la publication : GDI P. TOUAK
Responsable éditorial : CEN D. MALET
Rédacteurs : LCL M. TÉTU - CEN M. MALET - 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