MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

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

La MInute Cyber 05

PUBLICATION DU RAPPORT ANNUEL SUR LA CYBERCRIMINALITÉ 2026

C'est en avant-première, lors du Forum INCYBER (FIC) 2026, qui se tenait à Lille des 31 mars au 2 avril derniers, qu'a été présenté le troisième rapport annuel sur la cybercriminalité du ministère de l'Intérieur (2026), rédigé par le Centre d'analyse et de regroupement des Cybermenaces (CECyber) du Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI).

En 2025, 453 200 atteintes numériques ont ainsi été enregistrées, soit une hausse de 87 % sur les cinq dernières années. 61,9 % des faits ont concerné des atteintes numériques aux biens, 33 % des atteintes numériques aux personnes et 17 600 concernaient des atteintes aux systèmes d'information. 100 700 personnes physiques ont été mises en cause pour des atteintes numériques.

Outre les chiffres clés, ce rapport fait le bilan des tendances majeures et de l'évolution de la cybercriminalité. En 2025 le niveau d'activité observé était supérieur à celui observé en 2024. Cela, alors même qu'en 2024, le volume élevé d'attaques s'expliquait en partie par des évènements à forte portée médiatique, tels que les Jeux olympiques et paralympiques de Paris. Cela traduit une pression cyber durable et structurelle. Trois tendances majeures sont observées : les attaques par déni de service distribué (DDoS)[1] s'inscrivent en première place, principalement revendiquées par des groupes se réclamant de l'hacktivisme. Les vols et reventes de données compromises[2] et les attaques par rançongiciel[3] se positionnent respectivement en deuxième et troisième place.

Au-delà des tendances générales de la menace, le rapport dresse le tableau de l'écosystème et des modes opératoires des cybercriminels, leur fine compréhension s'avérant essentielle pour anticiper les attaques et adapter les réponses. La cybercriminalité s'organise désormais selon une logique industrielle, fondée sur la spécialisation des acteurs, la segmentation des tâches et le développement de chaînes de valeur illicites. Services clés en main, modèles d'affiliation et places de marché clandestines permettent à des profils très hétérogènes d'accéder à des capacités d'attaque autrefois réservées à des acteurs experts.

Ce document consacre, également, un chapitre aux évolutions constantes du cadre juridique, à la coopération internationale et aux priorités européennes, ainsi qu'aux réponses judiciaires au travers de l'évocation de plusieurs enquêtes majeures.

Enfin, l'évolution rapide des technologies numériques, conjuguée à l'adaptation constante des usages malveillants couplée à certaines dynamiques, encore émergentes - qui laissent entrevoir des ruptures susceptibles d'affecter durablement les équilibres de sécurité -, rendent impérative une analyse prospective pour lutter contre la cybercriminalité. Ainsi plusieurs points d'attention sont identifiés dans le rapport, tels que le développement de l'intelligence artificielle agentique.

Ce rapport est disponible en téléchargement sur le site internet du ministère de l'Intérieur :

https://www.interieur.gouv.fr/documentation/rapports/rapport-annuel-sur-cybercriminalite-2026.html

1. 53 % des cyberattaques détectées par le CECyber sur l'année 2025
2. 30 % des cyberattaques détectées par le CECyber sur l'année 2025
3. 13 % des cyberattaques détectées par le CECyber sur l'année 2025

Le COMCYBER-MI aux côtés des élus

En 2025, 293 revendications d'attaques cybercriminelles ciblant des collectivités territoriales ont été recensées. Les conséquences peuvent être lourdes : interruption des services publics, captations de données sensibles ou encore pertes financières significatives.

C'est dans ce contexte que l'Association des maires de France et des présidents d'intercommunalité (AMF) et le Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI) ont lancé « CapCyber : crises & collectivités », un exercice de simulation en ligne innovant pour accompagner les élus locaux et leurs agents dans la prévention et la gestion du risque cyber. Hébergé sur le site de l'AMF, ce module est conçu pour anticiper les crises, et propose une immersion pédagogique dans une situation de cyberattaque simulée, afin de mieux comprendre les enjeux et adopter les bons réflexes. Accessible à tous, « CapCyber : crises & collectivités » propose une approche pédagogique et opérationnelle pour sensibiliser et former élus et agents. Le jeu de rôle est également ouvert aux citoyens, qui peuvent ainsi se mettre à la place d'un élu confronté à une crise cyber. Le programme s'articule autour de trois volets complémentaires :

- une formation théorique (gestion de crise) ;
- une formation pratique (jeu de rôle évolutif) ;
- des témoignages de collectivités ayant vécu une crise ;
- une capsule vidéo de prévention par le Centre d'Analyse et de Lutte contre les Atteintes aux Élus (CALAE).

Avec ce dispositif, l'AMF et le ministère de l'Intérieur entendent renforcer la prise de conscience sur le risque cyber et doter les collectivités d'outils concrets pour améliorer leurs actions face à des menaces en constante évolution.

Mobilisation au profit des personnes déficientes visuelles

Dans la lignée de l'article 47 de la loi du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées, la Fédération des Aveugles et Amblyopes de France et le Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI) ont franchi hier une étape majeure.

Dans les locaux parisiens de la Fédération, de riches échanges ont en effet eu lieu afin de définir précisément les attentes mutuelles s'agissant de la lutte contre les cybermenaces. Il s'agissait aussi de comprendre les pratiques numériques des personnes déficientes visuelles, afin d'adapter nos messages de prévention et notre accompagnement, conformément au Référentiel général d'amélioration de l'accessibilité (RGAA).

Ainsi, par le biais de la Lieutenant-colonelle Sophie Lambert, du chef-d'escadron Matthieu Rousseau et l'adjudant Loïc Cartier, ainsi que de Madame Mégane Barreau pour la partie infographie, le COMCYBER-MI a participé aux côtés de M. Fernando pinto da Silva et Denis Boulay, experts en accessibilité et usages numériques de la Fédération des Aveugles de France, à des mises en situation ainsi qu'à des réflexions portant sur les prochaines documentations destinées aux personnes déficientes visuelles.

Ces ateliers, particulièrement instructifs, ont enfin laissé place à un moment important : la signature d'une convention de partenariat par Monsieur Bruno Gendron, Président de la Fédération, et le Général de division Patrick Touak, chef du COMCYBER-MI.

Une signature et un rapprochement important, qui rappelle un de nos objectifs clés : échanger, transmettre, et adapter les messages de prévention à tous les publics.

POUR ALLER + LOIN...

Pilotage de la priorité CYBER du cycle EMPACT par l'OFAC

En mai 2026, l'Office anti-cybercriminalité (OFAC) organisait, en tant que pilote de la priorité CYBER du cycle *EMPACT (European Multidisciplinary Platform Against Criminal Threats)*, les réunions de lancement de deux actions opérationnelles (OA).

La première, l'OA 3.3, consacrée aux partenariats public-privé, pilotée par les Pays-Bas avec l'appui de la France et du Danemark, regroupait une dizaine de pays européens et extra-européens. Cette réunion permettait aux participants d'identifier, d'ores et déjà, les leviers de partenariats à développer pour lutter plus efficacement contre la cybercriminalité à l'échelle européenne et internationale.

La seconde, l'OA 5.3, était consacrée au renforcement des moyens capacitaires dans la lutte contre les rançongiciels. Pilotée par la France avec l'appui de la Commission européenne et du Brésil, et le soutien de CIRCL (Computer Incident Response Center Luxembourg), cette action ambitionne de déployer à l'échelle européenne et internationale une solution technique éprouvée par la France pour contrer plus efficacement les groupes cybercriminels menant des attaques par rançongiciel.

Rapport 2025 de la Cnil

Le 18 mai dernier, la Commission nationale de l'informatique et des libertés (CNIL) a publié son rapport d'activité. Elle indique que l'année 2025 a notamment été marquée par une hausse très importante des plaintes reçues, un montant total d'amendes inédit, mais aussi un record de notifications de violations de données.

Face à ce constat, la CNIL indique poursuivre sa volonté d'accompagner l'entrée en application progressive du règlement sur l'Intelligence artificielle (RIA), et de sensibiliser « les jeunes et les familles », à travers notamment de l'application FantomApp dédiée aux adolescents et financée par la Commission européenne.

Par ailleurs, la Commission constate que ces deux dernières années ont été marquées par de nombreuses violations de données d'ampleur significative, principalement dues à des pratiques insuffisantes en matière de sécurité. En conséquence, la CNIL indique qu'elle consacrera en 2026 la moitié de ses contrôles et de ses actions répressives à la sécurité des données, en vérifiant le strict respect des exigences en matière de sécurité, tout en continuant à diffuser des messages de sensibilisation et des conseils aux particuliers et aux professionnels.

Publication mensuelle éditée par :
Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 05 - MAI 2026
Directeur de la publication : GDI P. TOUAK
Responsable éditorial : CEN D. MALET
Rédacteurs : CEN N. PETITPAS - CEN D. MALET
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