MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

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

La MInute Cyber 06

PUBLICATION DU RAPPORT ANNUEL SUR LA CYBERCRIMINALITÉ DU COMCYBER-MI

Parmi les missions du COMCYBER-MI, énumérées dans le décret n° 2023-1084 du 23 novembre 2023 portant création de ce service à compétence nationale, figure : « *[la production] chaque année [d'] un rapport d'état de la menace cyber du ministère de l'Intérieur. A cette fin, il centralise, analyse et communique aux services de la gendarmerie et de la police nationales, ainsi qu'aux autres services du ministère de l'Intérieur toutes documentations et données statistiques, en lien avec le service statistique ministériel de la sécurité intérieure, relatives à son domaine de compétence. Les services susceptibles d'apporter leur concours [au COMCYBER-MI] lui adressent, dans les meilleurs délais, les informations utiles à la production du rapport sur l'état de la menace.* »

Le 1er juillet 2025, était ainsi diffusé le second rapport annuel sur la cybercriminalité[1], établi par le Centre d'analyse et de regroupement des Cybermenaces (CECyber) du COMCYBER-MI.

Le rapport présente les chiffres clés de l'année 2024, les tendances majeures et les évolutions attendues. Parmi les constats effectués, celui d'une hausse conséquente des atteintes numériques. En 2024, 348 000 cas ont été enregistrés[2], soit une augmentation de + 74 % en 5 ans. Parmi ces atteintes, 65 % visaient les biens, 29,7 % les personnes, 4,9 % les institutions et l'ordre public. Enfin, 0,4 % étaient spécifiques aux législations et réglementations numériques.

S'agissant de l'analyse de la menace, le rapport signale qu'en 2024, la tendance observée jusqu'alors se poursuit. Les attaques se font plus nombreuses, plus ciblées et davantage difficiles à détecter, notamment *via* l'usage de l'intelligence artificielle ou des crypto-actifs (de nombreuses infractions sont, en effet, commises par le biais de l'utilisation de nouvelles technologies, détournées par les cybercriminels pour perfectionner leurs attaques).

Le COMCYBER-MI souligne, en outre, le fait que, la criminalité numérique n'a cessé d'évoluer dans son organisation, les services spécialisés notant aujourd'hui une « *industrialisation de la cybercriminalité* ». Ainsi, sur le même principe qu'un marché économique légal, une répartition, une automatisation et une rationalisation des tâches entre les acteurs de la cybercriminalité se mettent en place. Pour autant, tous ces acteurs malveillants sont interconnectés entre eux, principalement pour des motifs opportunistes, et sont en mesure de sous-traiter certaines tâches ou de mettre à disposition des compétences, au profit d'autres acteurs, en échange d'une rémunération.

Après un chapitre dévolu à un retour sur des enquêtes majeures et aux évolutions juridiques, l'analyse se fait prospective, le COMCYBER-MI mettant en lumière le rôle central de l'intelligence artificielle dans la prévention et la détection des menaces futures, ainsi que les risques systémiques liés à la généralisation des objets connectés.

Face aux transformations attendues des cybermenaces, doter les services de l'État, les acteurs privés et les citoyens d'une vision éclairée et proactive est un enjeu majeur, pour renforcer collectivement la résilience du pays.

Le rapport est disponible au lien suivant :

Rapport annuel sur la cybercriminalité 2025

1. La cybercriminalité regroupe tous les crimes et délits commis contre ou à l'aide de systèmes informatiques, prenant ainsi des formes très variées comme les vols de données personnelles, les escroqueries, les piratages de comptes, les rançongiciels ou encore l'usurpation d'identité.
2. Les données présentées dans ce rapport proviennent du Service statistique ministériel de la sécurité Intérieure (SSMSI), complétées par d'autres sources institutionnelles : la section J3 du parquet de Paris, l'Office Anti-Cybercriminalité (OFAC) de la Police nationale, l'Unité Nationale Cyber de la Gendarmerie nationale (UNCyber).

INTERVENTION DU COMCYBER-MI LORS DU COMITÉ DE DÉFENSE DE LA ZONE DE DÉFENSE ET DE SÉCURITÉ OUEST

Le 19 juin dernier, à Rennes, le commissaire divisionnaire M. LEVY-VALENSI intervenait, en tant que représentant du général HUSSON, chef du COMCYBER-MI, lors du comité de défense de zone, de la zone de défense et de sécurité ouest, présidé par Monsieur le Préfet de Zone.

Les comités de défense de zone sont prévus par l'article R 1311-25 du Code de la défense. Ils comprennent, les préfets des départements, le préfet délégué pour la défense et la sécurité, et plus généralement les représentants civils et militaires de l'État, occupant des responsabilités à l'échelle zonale.

La présentation du COMCYBER-MI auprès de hauts responsables zonaux, était l'occasion de leur décrire son écosystème, de leur partager une analyse de l'état de la menace, mais aussi d'évoquer les actions initiées pour sensibiliser et accompagner les usagers et organismes.

Le discours de M. LEVY-VALENSI, tourné vers les enjeux territoriaux et les menaces pouvant peser sur les collectivités, introduisait des échanges nourris avec les grands responsables présents, habitués à gérer les crises et à piloter des dispositifs complexes, aux acteurs multiples.

Ce dialogue contribue ainsi à la parfaite connaissance des enjeux et, *in fine*, à améliorer la réponse de l'État.

ACTIONS COMMUNES ENTRE EUROPOL ET LE CENTRE NATIONAL DE FORMATION À LA CYBERSÉCURITÉ DU MINISTÈRE DE L'INTÉRIEUR (CNFCYBER-MI)

Le CNFCYBER-MI du COMCYBER-MI, localisé à Lille, a accueilli à la fin du mois de mai et au début du mois de juin 2025 deux sessions d'envergure dans le domaine cyber.

Ainsi, la 4e session du *Tactical Crypto Workshop* (2025), organisée par la division des enquêtes spécialisées, de la donnée et des investigations techniques du COMCYBER-MI, réunissait 38 participants de 30 pays différents (26 pays de l'Union européenne, mais aussi les États-Unis, le Brésil, la Suisse et la Norvège), aux fins de contribuer à faciliter les interactions entre les services spécialisés des États membres et partenaires d'Europol. Cette session était, en effet, l'opportunité de partager un ensemble de bonnes pratiques techniques en matière d'investigations sur les *blockchains*, issues de l'étude des phénomènes criminels et du retour d'expérience des enquêteurs et analystes présents. Ces échanges sont primordiaux. La connaissance mutuelle et la coopération judiciaire entre les pays étant des facteurs clés de réussite. Cet *axiome* s'applique particulièrement aux investigations relatives à la criminalité usant des crypto-actifs.

La formation *«AI4Executive LEA »* était organisée, également, grâce à l'appui d'Europol. Destinée aux dirigeants des forces de sécurité européenne, elle apportait des réponses à la question majeure : *« Comment construire une stratégie en IA (intelligence artificielle) ? »*. Organisée par le général Patrick Perrot, conseiller IA pour le COMCYBER-MI et co-animée par Ysens de France, docteur en droit, chercheur en droit international et chargée de missions aux côtés du coordinateur IA de la Gendarmerie Nationale, cette formation visait à donner des clés à ses auditeurs afin de comprendre les principes fondamentaux de l'intelligence artificielle, d'identifier les enjeux éthiques, de réglementation et de conformité, mais aussi d'éclairer sur l'exploitation de l'IA dans le cadre de l'expérimentation *« Grands Événements »* et d'informer sur les cas d'usage opérationnels d'une exploitation de l'IA au service de la protection des citoyens. Cette formation n'omettait pas le volet fondamental qu'est la conduite de projet en IA. Forts des connaissances acquises, les dirigeants conviés participaient ensuite à des ateliers de construction d'une stratégie responsable en IA.

POUR ALLER + LOIN...

Interpellation de quatre hackers français

Lundi 23 juin dernier, la Brigade de lutte contre la cybercriminalité (BL2C) de la préfecture de police de Paris a interpellé quatre hackers français dans les Hauts-de-Seine, en Seine-Maritime et à La Réunion. Sous le nom collectif de *« ShinyHunters »*, ils sont suspectés d'être responsables du forum cybercriminel *Breachforums*, mais aussi d'avoir commis des cyberattaques d'un très haut degré de complexité technique, au préjudice de nombreuses victimes en France et à l'étranger.

Breachforums.st, forum anglophone accessible sur le *clearweb*, constituait le plus grand site d'échange et de revente de données informatiques volées et d'accès frauduleux dans des systèmes d'information. Ledit forum, qui comptait plusieurs milliers d'utilisateurs, avait notamment servi à diffuser des données personnelles volées au cours de cyberattaques d'ampleur commises en France.

C'est ainsi que : *« la section de lutte contre la cybercriminalité du parquet de Paris avait ouvert en août 2024 une enquête préliminaire, fondée sur le soupçon que plusieurs administrateurs seraient français »*, indique la procureure de la République de Paris Laure Beccuau dans un communiqué de presse.

Le site *Breachforums.st* avait été visé par deux opérations judiciaires américaines en 2023 et 2024, avant de revenir rapidement en ligne. *« Les interpellations de cette semaine [...] permettent d'espérer sa fermeture totale »*, a ajouté Mme Beccuau. Cette dernière a par ailleurs précisé que *« l'identification des suspects a été rendue possible grâce à la coopération policière et judiciaire avec nos partenaires étrangers, notamment les États-Unis [avec] le Federal Bureau Of Investigation (FBI), [...] traduisant un haut degré de confiance mutuelle »*.

Publication mensuelle éditée par :
Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 06 - JUIN 2025
Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : GBR P. PERROT - CEN D. MALET - CEN N. PETITPAS - LTN J. NACHOUKI - CECyber
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