MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

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

La MInute Cyber 9

LE MENTORAT AU SEIN DU COMCYBER-MI

Le programme de mentorat cyber vise à renforcer les relations entre les militaires et personnels civils récemment affectés au sein du COMCYBER-MI ou de l'UNCyber, et les cyber-réservistes de la Gendarmerie nationale. Élaboré par un groupe de travail de la réserve citoyenne cyber, il favorise un réseau actif et collaboratif en mettant en avant les échanges interprofessionnels et intergénérationnels pour servir l'intérêt général et lutter contre la cybercriminalité. Il associe des mentors expérimentés du domaine cyber à des filleuls (officiers, sous-officiers ou personnels civils) pour un accompagnement personnalisé. Actuellement, la seconde promotion poursuit cet effort en développant les compétences nécessaires pour faire face aux défis croissants des cybermenaces.

Créant une synergie entre les cyber-réservistes et les personnels du COMCYBER-MI ou de l'UNCyber, ce programme facilite les échanges entre ces deux milieux complémentaires permettant aux réservistes chevronnés de transmettre leurs connaissances à des personnels volontaires et engagés, tout en enrichissant leurs perspectives professionnelles. Il renforce en outre les réseaux favorisant la collaboration et la cohésion pour mieux lutter contre la cybercriminalité.

Les filleuls bénéficient de ce mentorat à travers un accompagnement personnalisé. Ils sont guidés par des mentors dont les compétences sont reconnues dans leur milieu professionnel, et reçoivent des conseils adaptés pour surmonter les défis de leur carrière. Ce parcours favorise leur développement, tant sur le plan professionnel qu'académique, notamment dans le domaine de la cybersécurité. Pour les cyber-réservistes, ce programme leur permet de transmettre leur savoir-faire et de découvrir le fonctionnement des unités cyber au sein du ministère de l'Intérieur (MININT).

Le programme de mentorat suit plusieurs étapes clés, avec un appel à candidatures qui permet de sélectionner les mentors et filleuls selon leurs profils et aspirations, puis la formation de binômes pour optimiser les complémentarités et synergies. Des rencontres régulières sont organisées, notamment des immersions métiers où filleuls et mentors découvrent leurs réalités professionnelles respectives. Enfin, les participants sont invités à des événements tels que des conférences ou ateliers pour enrichir leur expérience. Ainsi, le 26 septembre 2024, se sont tenues les premières rencontres, avec notamment une présentation du retour d'expérience (RETEX) sur le travail des personnels du COMCYBER-MI lors des Jeux Olympiques de Paris 2024.

Le mentorat dépasse le simple transfert de connaissances. Il devient un levier de développement personnel et professionnel, créant une communauté cyber plus compétente, solidaire et résiliente. Cette initiative renforce non seulement les compétences individuelles, mais consolide également l'ensemble de l'écosystème cyber du MININT.

BILAN DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ LORS DES JOP PARIS 2024 : LE RÔLE DU COMCYBER-MI

Le COMCYBER-MI (Commandement du ministère de l'Intérieur dans le cyberespace) a joué un rôle clé dans la lutte contre la cybercriminalité pendant les Jeux Olympiques et Paralympiques de Paris 2024. Du 7 mai au 8 septembre 2024, il a déployé un dispositif de grande envergure, mobilisant des équipes spécialisées pour surveiller et analyser les cybermenaces, tout en collectant du renseignement d'intérêt cyber. Ce dispositif a permis d'anticiper et de répondre aux menaces visant à perturber cet événement mondial.

En étroite collaboration avec l'ANSSI, responsable de la cybersécurité des Jeux, et des partenaires publics et privés, tant nationaux qu'internationaux, le COMCYBER-MI a assuré des échanges proactifs avec les Forces de Sécurité Intérieure (FSI) et les autorités militaires, administratives et judiciaires. Un officier de liaison a été intégré au Centre National de Commandement Stratégique (CNCS), assurant la communication continue entre le Campus Cyber et les instances décisionnelles. Ce positionnement stratégique a facilité la remontée des informations en temps réel, permettant une réaction rapide face aux menaces détectées.

Sur le plan opérationnel, les équipes de la Division des Enquêtes spécialisées, de la Donnée et des investigations Techniques (DEDT), basées à Pontoise, ont joué un rôle clé en restant mobilisées pendant toute la durée des Jeux. En mesure d'apporter leur expertise dans le cadre d'enquêtes complexes et de soutenir les FSI dans des opérations nécessitant des compétences de haut niveau, la DEDT s'est mise en ordre de bataille pour garantir que toute menace ou cyberattaque soit traitée rapidement et efficacement.

Pendant la période des Jeux, 481 incidents cyber ont été recensés, dont 104 étaient directement liés à l'événement. Parmi les menaces identifiées, les attaques les plus courantes comprenaient des attaques par déni de service distribué *(DDoS)*, des vols de données, et des défigurations de sites *web*. Plusieurs groupes hacktivistes, notamment Noname057(16), ont cherché à tirer parti de la visibilité mondiale des Jeux pour revendiquer des actions géopolitiques, principalement en lien avec des enjeux internationaux.

La lutte contre la fraude à la billetterie et le typosquattage a également été une priorité du COMCYBER-MI. Grâce à des actions menées conjointement avec l'Unité Nationale Cyber de la Gendarmerie nationale (UNCyber), plusieurs tentatives d'escroquerie ont pu être identifiées et neutralisées, garantissant ainsi une meilleure protection pour les spectateurs et les organisateurs.

L'approche adoptée par le COMCYBER-MI a été progressive et adaptable tout au long de l'événement. Dès l'arrivée de la flamme olympique à Marseille, le dispositif est passé en alerte maximale. Il a été ajusté au fur et à mesure des besoins. Le rythme opérationnel a été modulé en fonction des événements clés des Jeux, tels que la cérémonie d'ouverture ou encore l'arrestation de personnalités influentes dans le cyberespace.

Le bilan des actions menées par le COMCYBER-MI démontre l'efficacité du dispositif mis en place. La collaboration avec des partenaires nationaux et internationaux, ainsi que l'adaptation rapide aux menaces émergentes, ont permis de neutraliser plusieurs tentatives d'attaques tout en assurant une protection renforcée pour les Jeux Olympiques et Paralympiques. Ce travail de coordination et de vigilance constante témoigne de l'importance de la lutte contre la cybercriminalité dans la protection des grands événements mondiaux, en s'appuyant sur un réseau solide d'acteurs publics et privés.

Pour aller + loin...

GOHST

L'expérience acquise grâce au dossier « Encrochat » a amené le C3N à être sollicité par la police suédoise en 2021, afin de collaborer sur Ghost ECC, une nouvelle solution de téléphonie chiffrée utilisée à des fins criminelles. Une enquête est alors ouverte par le C3N, durant laquelle des téléphones équipés de Ghost ECC sont acquis et analysés afin de comprendre leur fonctionnement, et démontrer leur utilisation illicite dans différents pays. Une task force est rapidement créée au sein d'Europol et, fait rarissime, une équipe commune d'enquête entre la France (C3N) et le FBI est mise en place.

Le travail minutieux des enquêteurs de l'UNC, appuyés par le COMCYBER-MI qui a fourni des ressources techniques permettant d'accéder aux communications, ont grandement contribué au déclenchement de l'opération judiciaire internationale menée par Europol le 16 octobre 2024. Au final, plus de 50 personnes ont été interpellées, environ 350 Kg de produits stupéfiants ont été saisis ainsi que plus d'une vingtaine d'armes et plusieurs millions d'euros d'avoirs criminels. L'enquête a également permis de déjouer plus de 50 atteintes graves à la vie et à l'intégrité physique en Australie. Les utilisateurs de cette solution se trouvaient majoritairement en Australie, au Canada, en Suède et en Irlande.

« BILAN CYBER » DE L'ANSSI

L'ANSSI a publié début septembre son « bilan cyber » des JOP de Paris 2024. L'Agence indique que son dispositif, mis en place en étroite collaboration avec les différentes structures impliquées dans l'organisation des Jeux, rassemblait un écosystème cyber de près de 500 entités, dont le ministère de l'Intérieur. Entre le 8 mai et le 8 septembre, ont été recensés 548 événements de cybersécurité, ayant affecté des entités en lien avec l'organisation des Jeux. Caractérisés par « leurs faibles impacts », ils ont donné lieu à une réponse opérationnelle. Aussi, sur les types d'événements de cybersécurité rapportés, près de la moitié correspondent à des indisponibilités, principalement dues à des attaques par *DDoS*. Le reste correspond à des tentatives de compromission ou des compromissions, des divulgations de données ou des signalements de vulnérabilités. Les secteurs d'activité les plus ciblés sont les entités gouvernementales, le sport, les sites de compétitions et les télécommunications, a indiqué l'ANSSI, précisant qu'aucun événement de cybersécurité n'a affecté les cérémonies d'ouverture, de clôture et le bon déroulement des épreuves.

Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 009 - SEPTEMBRE 2024

Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : COL P. PERESSE - LCL S. LAMBERT - CEN D. MALET - CEN R. LE YOUDEC
Conception graphique et maquettage : Mme M. BARREAU

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

*sur **www.gendarmerie.interieur.gouv.fr***

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