LES PUBLICATIONS

[EN CLAIR]

COMBAT CONTRE LA CYBERCRIMINALITÉ : COMMENT ENISA ET EUROPOL COLLABORENT-ELLES ?

Par Lou-Anne DUCOS

LES JEUNES IHEDN

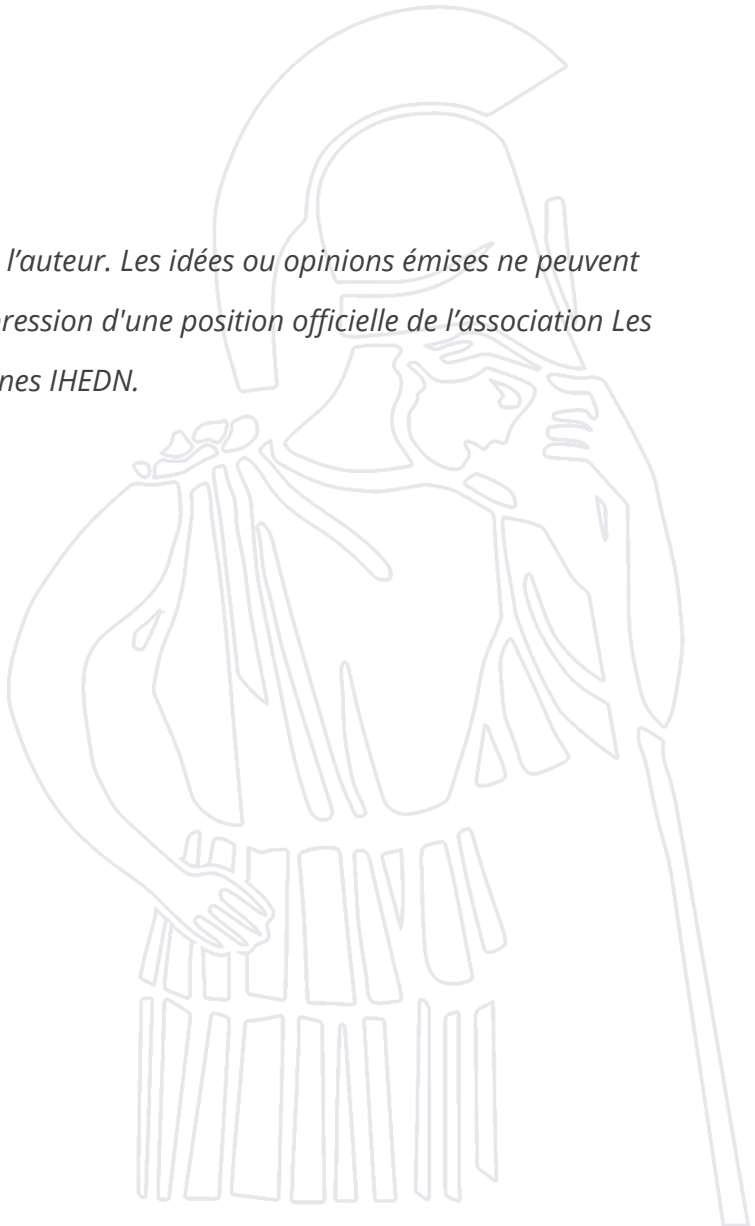
À PROPOS DE L'ARTICLE

À l'occasion du #Cybermois, Les Jeunes IHEDN vous ont préparé une série d'articles thématiques sur les enjeux de cybersécurité et de cyberdéfense. Découvrez dans cet article comment l'Union européenne contribue à lutter contre la hausse de la cybercriminalité en Europe en créant de nouvelles opportunités de collaboration entre ses agences, en l'occurrence ENISA et EUROPOL.

À PROPOS DE L'AUTEUR

Lou-Anne DUCOS est responsable des Publications pour le Comité directeur et membre du Comité Europe de l'association depuis deux ans. Elle est actuellement en Master 2 à Sciences Po Saint-Germain-en-Laye et travaille en parallèle au sein de l'Agence Européenne de Défense.

Ce texte n'engage que la responsabilité de l'auteur. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle de l'association Les Jeunes IHEDN.



Combat contre la cybercriminalité : comment ENISA et EUROPOL collaborent-elles ?

Février 2021, EUROPOL dévoile le succès de son « Opération SECRETO » conduisant au démantèlement d'un groupe de cybercriminels recherché pour avoir dérobé plus de 14 millions de dollars à des banques américaines[1]. Ce succès, engendré par la coopération permise par EUROPOL entre les autorités américaines et les forces de l'ordre des États-membres (EM) de l'Union européenne (UE), a également été permis par des échanges accrus avec l'ENISA, l'agence européenne chargée de la sécurité des réseaux et de l'information. Les deux organisations, disposant pourtant de mandats très différents, ont vite compris l'intérêt de coopérer pour mener à bien leurs missions. En effet, le crime cyber occupe désormais une place prépondérante dans le paysage sécuritaire européen. Pour preuve, le programme stratégique pour l'UE 2019-2024 défini par le Conseil européen place la cybercriminalité au sein de sa première priorité : protéger les citoyens et les libertés. De ce fait, il est apparu nécessaire que les agences de l'UE combinent leurs différentes expertises pour protéger au mieux les intérêts des membres de l'Union. Cet article reviendra ainsi sur l'enjeu grandissant de la cybercriminalité pour l'Union européenne ainsi que sur les mécanismes de coopération développés par EUROPOL et ENISA pour répondre à ce défi.

[1] EUROPOL. « Internet Organised Crime Threat Assessment 2021 ». Décembre 2021, Publication Office of the European Union. Disponible sur : https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf.

Deux agences européennes aux rôles bien définis

ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information)	
BUT	Garantir un niveau élevé commun de cybersécurité dans toute l'Europe
DATE DE CRÉATION	2004
QUARTIER GÉNÉRAL	Héraklion (et un bureau à Athènes)
MISSIONS	• Promotion d'une coopération active entre les acteurs de la cybersécurité au sein des États membres et des institutions et agences de l'Union • Mise en place d'une approche cohérente de la cybersécurité = pas de fragmentation, la cyber doit être pensée dans chaque politique • Anticipation et partage du savoir
MÉTHODE	• Appui à la mise en place d'un cadre juridique et réglementaire adapté • Activités de sensibilisation • Organisation d'exercices cyber • Centralisation et partage des informations relatives aux menaces cyber (*CERTs* européen et nationaux) = activités d'intelligence
BUDGET	24 millions d'euros envisagés pour 2022

EUROPOL (Agence de police européenne)	
BUT	Aider les États membres à combattre la délinquance grave et organisée
DATE DE CRÉATION	1998
QUARTIER GÉNÉRAL	La Haye
MISSIONS	• Lutte contre le trafic de drogues • Lutte contre le trafic d'êtres humains • Lutte contre l'aide à l'immigration illégale • Lutte contre la contrefaçon de l'euro • Lutte contre les attaques cyber, terroristes et les groupes de criminels organisés
MÉTHODE	• Mise en place de différents centres spécialisés (centre contre le crime cyber, centre pour le contre-terrorisme) • Échange d'informations sur les activités criminelles entre EM • Rapports d'anticipation sur les menaces • 40 000 enquêtes par an grâce à 220 officiers de liaison, une centaine d'analystes, un effectif total de plus de 1000 personnes
BUDGET	192,4 millions d'euros pour 2022

Un objectif commun : la lutte contre la cybercriminalité

Loin d'être une menace nouvelle, la cybercriminalité atteint toutefois des sommes records, faisant de ce défi sécuritaire une préoccupation pour l'ensemble des États européens. En effet, si le crime cyber était un pays, il s'agirait du troisième pays le plus riche après les États-Unis et la Chine. Le coût du crime cyber a été évalué à environ 7000 milliards de dollars en 2022[2], un coût qui devrait augmenter de 15% par an pendant les 5 prochaines années lui permettant ainsi d'atteindre 10,5 mille milliards de dollars en 2025 (contre 3 mille milliards en 2015)[3]. De plus, le cliché du *hacker* seul dans sa chambre a laissé place à des réseaux de cybercriminels organisés agissant selon un modèle économique très développé. Des méthodes de rendement bien rôdées ont été mises au point tout en travaillant à rendre ces actions illégales invisibles aux yeux des autorités. En parallèle de cette professionnalisation de la cybercriminalité, un véritable commerce a été créé engendrant des impacts directs sur l'ensemble de l'écosystème privé et public des EM. Il n'est désormais plus nécessaire d'avoir des compétences informatiques poussées pour lancer des attaques, chaque individu peut simplement acheter ou louer des kits sur internet leur permettant de lancer des attaques élaborées sans avoir la moindre compétence technique. C'est par exemple le cas des *ransomware-as-a-service* ou des attaques *DDoS-as-a-service* qui sont de plus en plus présentes sur le net. En conséquence, chacun peut devenir un criminel en ligne et nuire à la population ce qui rend le travail des autorités d'autant plus complexe. Pour ne rien faciliter à la situation, il est très difficile d'attribuer les crimes cyber et donc de punir les responsables. L'utilisation de *proxys*, *VPNs*, des réseaux décentralisés comme *TOR*, ou encore d'ordinateurs de victimes précédentes pour initier l'attaque permet en effet de rendre particulièrement complexe l'identification des auteurs. Quand bien même une personne ou un pays serait suspecté d'être à l'origine

[2] MALCOMB, Farber. « Cybercrime Damages To Cost The World $7 Trillion USD in 2022 ». *Cybersecurity Ventures* [en ligne], Août 2022 [Consulté le 3 octobre 2022]. Disponible sur : https://www.einpresswire.com/article/585389499/cybercrime-damages-to-cost-the-world-7-trillion-usd-in-2022.

[3] MORGAN, Steve. « Cybercrime to cost the world $10.5 trillion annually by 2025 ». *Cybersecurity Ventures* [en ligne], Novembre 2020 [Consulté le 6 mars 2021]. Disponible sur : https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

de l'attaque, il reste très coûteux de le prouver et attribuer une cyberattaque est un acte politique lourd de conséquences. Enfin, la cybercriminalité, avant tout vue comme une menace économique, a pris une ampleur inédite en 2020 lorsqu'une attaque *ransomware* contre un hôpital allemand a conduit au premier mort lié à une attaque informatique[4]. La patiente, devant être opérée au moment de l'attaque, a été transférée d'urgence lorsqu'il s'est avéré que l'attaque empêchait l'hôpital de mener à bien les interventions prévues. Dans un état critique, elle est morte au cours du transfert. Les attaques répétées contre les hôpitaux, phénomène amplifié durant la crise de la Covid-19, et encore récemment avec l'attaque sur l'Hôpital de Corbeil-Essonnes, mettent ainsi en lumière la possibilité de voir des attaques cyber devenir mortelles. Les gouvernements craignent également de plus en plus les attaques contre leurs infrastructures critiques (services financiers, systèmes de transport, santé publique, services de sécurité, plus généralement les opérateurs de services essentiels et opérateurs d'importance vitale) qui, comme les attaques répétées de la Russie contre l'Ukraine l'ont montrées, peuvent grandement déstabiliser un pays.

Pour lutter contre cette cybercriminalité, l'UE a multiplié les initiatives et la création d'agences spécialisées. Pour autant, certaines dont l'ENISA restent encore méconnues du grand public.

Une coopération entre EUROPOL et l'ENISA accrue

La coopération entre EUROPOL et ENISA a débuté en 2011 avec un premier atelier commun tenu à Prague sur le thème de la lutte contre la cybercriminalité. ENISA a permis d'apporter une composante plus technique aux discussions avec EUROPOL, impliquant aussi les *CERTs* européens (*Computer Emergency Response Team*). Cette coopération s'est institutionnalisée en 2014 avec la signature d'un accord de coopération stratégique entre

[4] LE MONDE AVEC AP. « En Allemagne, une attaque informatique contre une Clinique provoque un mort ». *Le Monde* [en ligne], Septembre 2020 [Consulté le 6 mars 2021]. Disponible sur : https://www.lemonde.fr/pixels/article/2020/09/17/en-allemagne-une-attaque-informatique-contre-une-clinique-provoque-une-mort_6052638_4408996.html.

les deux agences. L'objectif affiché était de faciliter la collaboration et les échanges d'expertise dans le domaine de la lutte contre la cybercriminalité en produisant des rapports conjoints de situation d'ordre général et en mettant en place des formations communes pour garantir un niveau d'expertise élevé. Les deux agences ont également décider de créer un lien plus étroit entre elles en invitant leurs homologues à prendre part à leurs activités. Ainsi, l'ENISA fait partie du comité du centre EC3, le Centre européen de lutte contre la cybercriminalité au sein d'EUROPOL. En contrepartie, le centre EC3 d'EUROPOL fait partie du groupe permanent des parties prenantes de l'ENISA, un organe consultatif qui a pour rôle de conseiller le directeur de l'Agence sur ses priorités de l'année. Chaque entité est alors capable de contribuer au travail de l'autre, de connaître les priorités fixées pour l'année et de prendre part aux discussions.

En 2016, les deux agences publient un communiqué conjoint sur la protection des données en matière d'investigations policières. Le débat est alors de savoir comment décrypter et accéder aux informations obtenues au cours des investigations tout en respectant le mécanisme de protection des données. La question de la protection de l'intégrité de nos informations sensibles par le biais de la cryptographie est également évoquée, conduisant EUROPOL et ENISA à développer une nouvelle plateforme de décryptage en 2020[5]. Les deux agences, sous l'égide de la Commission européenne, ont travaillé sur cette plateforme dans l'objectif de décrypter les données perquisitionnées dans le cadre d'investigations criminelles. Ce nouvel outil a grandement aidé à l'arrestation spectaculaire des 104 individus recherchés au cours de « l'Opération SECRETO »[6].

[5] CISOMAG. « Europol and European Commission launch new decryption platform to combat encryption misuse ». *Ciso Mag* [en ligne], 21 décembre 2020 [Consulté le 6 mars 2021]. Disponible sur : https://cisomag.eccouncil.org/europol-and-european-commission-launch-new-decryption-platform-to-combat-encryption-misuse/.

[6] EUROPOL. « Internet Organised Crime Threat Assessment 2021 ». Décembre 2021, Publication Office of the European Union. Disponible sur : https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf.

Le 29 septembre 2017, lors du Sommet de Tallinn et dans un contexte de recrudescence des attaques au moyen des *ransomwares Wannacry* et *Notpetya,* les États-membres de l'UE décident de renforcer leur outillage en matière de lutte contre la cybercriminalité. EUROPOL obtient ainsi l'opportunité d'agir en partenariat avec l'ensemble des États-membres lors d'attaques cybers pour aider les victimes et maintenir des points permanents d'échanges d'informations entre les pays. Le mandat d'ENISA sera également renforcé en 2021 lorsque la Commission décide de la création d'une nouvelle structure : la *Joint Cyber Unit*. Celle-ci devrait être opérationnelle d'ici le 31 décembre 2022 et finalisée pour juin 2023. Elle sera pilotée par l'ENISA dans l'objectif d'assurer une réponse coordonnée de l'UE aux incidents et crises cybernétiques à grande échelle. Le renforcement de ces deux institutions permettra dans le futur une coopération encore plus effective, chaque agence développant ses propres outils et élargissant son mandat initial.

Il est toutefois important de noter que les deux agences fonctionnent avec des moyens très différents. Qu'ils s'agissent de moyens humains ou financiers, ENISA est pour l'instant très loin d'avoir les ressources dont dispose EUROPOL. ENISA joue ainsi un rôle d'appui et d'échange d'information avant d'être un véritable centre opérationnel capable de lutter directement contre la cybercriminalité. Néanmoins, la coopération accrue entre les deux agences demeure un signe positif pour la lutte contre la cybercriminalité au sein de l'Union. Elle marque également un changement de paradigme européen avec une stratégie européenne qui vise tout autant à atténuer les risques de cyberattaques en consacrant davantage d'efforts sur la sensibilisation des acteurs et la détection des attaques qu'à arrêter les réseaux de cybercriminels.






publication@jeunes-ihedn.org