Le Centre européen de lutte contre la cybercriminalité (EC3): état des lieux et rapport d'activité, y compris le support pour la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, la surveillance et la lutte contre les crimes liés à l'Internet clandestin

Europol a mis en place en 2013 le Centre européen de la cybercriminalité (EC3) afin de renforcer l'application de la loi contre la cybercriminalité dans l'UE et de contribuer ainsi à la protection des citoyens, des entreprises et des gouvernements européens contre la criminalité en ligne. Depuis sa création, l'EC3 a contribué de manière significative à la lutte contre la cybercriminalité, en participant à des dizaines d'opérations médiatisées et à des centaines de déploiements de soutien opérationnel sur le terrain ayant entraîné des centaines d'arrestations. De même, l'EC3 a contribué à l'analyse de centaines de milliers de dossiers, dont la grande majorité se sont avérés difficiles. Bien qu'il soit difficile de fournir des estimations fiables, certains rapports dans ce milieu suggèrent que les coûts de la cybercriminalité dans le monde s'élèvent à des centaines de milliards d'euros par an [1].

Chaque année, l'EC3 publie des évaluations de la criminalité organisée sur Internet (IOCTA), son rapport stratégique phare sur les principales constatations, les menaces émergentes et l'évolution de la cybercriminalité.

La lutte contre la cybercriminalité est la première des dix priorités d'Europol dans le cadre du cycle politique quadriennal pour la période 2018-2021. Cette priorité est réalisée par :

1. Le démantèlement des activités criminelles liées aux attaques contre les systèmes d'information ;
2. La lutte contre les abus et l'exploitation sexuelle des enfants, y compris la production et la diffusion de matériel pédopornographique ; et
3. Le ciblage des infracteurs impliqués dans la fraude et la contrefaçon des moyens de paiement autres que les espèces, y compris la fraude à grande échelle par carte de paiement (en particulier la fraude carte inexistante), dans les menaces émergentes pour d'autres moyens de paiement autres que les espèces et dans l'activation des activités criminelles.

Les différences dans les juridictions nationales distinctes et définies sur le plan territorial dans le domaine de la lutte contre la cybercriminalité posent des difficultés pour déterminer le droit applicable en matière d'interactions transnationales et créent une incertitude juridique, empêchant ainsi la coopération policière et judiciaire transfrontalière, nécessaire pour lutter efficacement contre la cybercriminalité.

1 Source:https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

En septembre 2017, la Commission a adopté un nouveau paquet sur la cyber-sécurité comprenant un large éventail de mesures visant à renforcer la résilience de l'UE et sa réaction aux cyber-attaques. Le paquet comprend plusieurs éléments qui intéressent directement Europol, tels que stipulés dans la Communication "Résilience, dissuasion et défense: renforcer la cybersécurité pour l'UE",[2] la proposition de Directive sur la fraude en matière de paiement sans espèces[3] et la Recommandation "sur une Réponse coordonné concernant les incidents et les crises de cybersécurité à grande échelle"[4].

21/02/2019

[2] Proposition de Directive du Parlement européen et du Conseil concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil COM/2017/0489 final - 2017/0226 (COD) Recommandation de la Commission du 13.9.2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (C(2017) 6100 final)

[3] Feuille de route en vue de renforcer l'échange d'informations et la gestion de l'information, y compris des solutions d'interopérabilité, dans le domaine de la justice et des affaires intérieures, le 6 juin 2016, Secrétariat du Conseil, dossier no. 9368/1/16

[4] JOIN(2017) 450 final