RÉFLEXIONS STRATÉGIQUES

PRÉOCCUPANTS, INSPIRANTS, PASSIONNANTS… DÉCOUVREZ À TRAVERS CES ARTICLES RÉFLEXIONS STRATÉGIQUES, LES SUJETS ET EXTRAITS DE MÉMOIRES RÉALISÉS PAR LES AUDITEURS DU MBA MANAGEMENT DE LA SÉCURITÉ.

#NUMÉRIQUE#MENACE#UE

Les stratégies de l'Union Européenne face aux menaces criminelles à l'ère du numérique

AUTEUR :
LCL CHRISTEL FONTAINE
JUIN 2024

Les stratégies de l'Union Européenne face aux menaces criminelles à l'ère du numérique

Auteur : LCL Christel FONTAINE auditrice de la 10ème promotion

Le 8 novembre 2023, à la tête d'une coalition de six associations françaises et européennes, la Quadrature du Net (association française de défense et de promotion des droits et libertés sur Internet) attaque le décret d'application de la loi appliquant le règlement européen relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne (TCO, Terrorist Content Online Regulation). Le but est de questionner la validité du règlement européen au regard des textes qui garantissent les droits fondamentaux au sein de l'Union. La coalition relève que le décret d'application de la loi du 16 août 2022, qui adapte le droit de l'UE, « participe à la surveillance des contenus en ligne et porte atteinte à la liberté d'expression en ligne ». Mais si c'est le décret français qui est attaqué, c'est le niveau européen que la coalition vise, via une question préjudicielle posée au Conseil d'État et qui devrait alors être transmise à la Cour de justice de l'Union européenne (CJUE).

Le TCO1, adopté en 2021 établit « des règles uniformes pour lutter contre l'utilisation abusive de services d'hébergement pour diffuser au public des contenus à caractère terroriste en ligne ». Il prévoit, entre autres, une logique de censure administrative qui permet à chaque État membre d'accorder à une autorité publique nationale le pouvoir « d'émettre des injonctions de retrait de contenus qui lui paraîtraient être à caractère terroriste » à destination des fournisseurs de services d'hébergement. En France, ces autorités sont l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM).

Ce recours illustre toute la difficulté à trouver un juste équilibre dans la mise en œuvre des stratégies envisagées, autant au niveau européen qu'au niveau national, face à la menace criminelle dans l'espace numérique.

(1) Les termes « sécurité informatique » et « cybersécurité » seront utilisés comme synonymes dans ce document.
(2) En partant des règles et en jouant contre elle-même tout en faisant preuve de créativité dans des échelles de temps inhumaines (« quatre heures de pratique et 44 millions de parties [d'entraînement] pour vaincre Stockfish ») idem sur StarCraft avec la création d'une ligue composée de joueurs uniquement IA (cf. [20]).
(3) Un botnet est un ensemble de machines informatiques (caméras, ordinateurs, etc.) qui sont contrôlées de manière visible ou non par un cybercriminel pour son profit.

Les stratégies de l'Union Européenne face aux menaces criminelles à l'ère du numérique

Auteur : LCL Christel FONTAINE auditrice de la 10ème promotion

Cette libre circulation de l'information, revendiquée également par les hackers, prend naissance dans la contre-culture des années 1960. L'architecture même de l'espace numérique est alors conçu dans un esprit d'ouverture, d'autogestion, de liberté des échanges et de l'expression. Créé pour que l'information puisse toujours circuler sans entrave, c'est un espace fortement décentralisé et surtout dénué de centre.
En parallèle, depuis plusieurs années, le développement extrêmement rapide de l'espace numérique a entraîné l'éclosion de nouvelles menaces criminelles auxquelles il est nécessaire de s'adapter tout aussi rapidement. En effet, « si la technologie offre de nouvelles opportunités à la société ainsi que de nouveaux outils aux juges et aux services répressifs, elle ouvre aussi des perspectives aux criminels » (3).

Phénomène mondial, sans frontières et sans définition unanimement admise, la cybercriminalité implique une coopération internationale accrue. Le 27 décembre 2019, l'Assemblée générale des Nations Unies adopte une résolution sur la « lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles » (4). Mais la convention du Conseil de l'Europe de 2001 sur la cybercriminalité (dite «convention de Budapest») est le premier traité international sur la question (5).
Au niveau de l'Union européenne (UE), la Commission européenne fait de la question de l'évolution des menaces criminelles l'un des piliers d'une stratégie de l'UE pour l'Union de la sécurité sur la période 2020-2025. La question de l'évolution des menaces criminelles y est déclinée en quatre priorités :

- la mise en œuvre de la législation en matière de cybercriminalité ;
- la lutte contre les contenus illicites en ligne ;
- la lutte contre les menaces hybrides ;
- l'évaluation des moyens de renforcer les capacités des services répressifs en matière d'enquêtes numériques.

Parallèlement, la mise en place de ces différentes stratégies de l'Union européenne pour lutter contre ces nouvelles menaces se traduit par des réalisations concrètes sur le plan législatif. Les États font face à de nouveaux défis technologiques et politiques. Leur résilience est quotidiennement éprouvée, nécessitant de nouvelles ressources humaines et scientifiques, mais aussi, juridiquement et politiquement, une constante adaptation. Interdire de faire dans le monde virtuel ce qu'il est interdit de faire dans le monde réel semble être un axiome simple et indiscutable.

(3) Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité COM(2020) 605 final
(4)https://digitallibrary.un.org/nanna/record/3847855/files/A_RES_74_247-FR.pdf withWatermark=0&withMetadata=0&version=1®isterDownload=1 .
(5) https://www.coe.int/fr/web/cybercrime/the-budapest-convention

Les stratégies de l'Union Européenne face aux menaces criminelles à l'ère du numérique

Auteur : LCL Christel FONTAINE auditrice de la 10ème promotion

Mais comme pour toutes libertés individuelles, parfois limitées au nom du bien commun, cette interdiction suscite une certaine méfiance, voire une défiance.
Les menaces criminelles, circonscrites ici aux crimes et délits commis dans et grâce à l'espace numérique (6), engendre un nouveau paradigme, une nouvelle manière de penser la prévention et la répression. Dans ce nouvel espace de délinquance (27 États représentant plus de 4 000 000 km² et plus de 425 millions de personnes), le caractère polymorphique des cyber menaces se fonde à la fois sur la complexité des cyberattaques et sur la professionnalisation des cybercriminels. Territoire à part entière, le cyberespace n'est plus physique mais numérique. Il en découle des particularités, abolissant les distances et les frontières, avec des enjeux inédits en termes de sécurité intérieure.

Les phénomènes criminels sont regroupés en plusieurs catégories : les atteintes aux personnes (atteinte à la vie privée, chantage, harcèlement…), les escroqueries (virement frauduleux, récupération de données bancaires, médicales…), les atteintes aux systèmes de traitement de données automatisés (connexion illicite à un compte client en ligne), l'intelligence économique et les atteintes à la sécurité nationale (collecte et diffusion de données piratées). De manière générale, les atteintes à l'encontre des systèmes d'information sont écartées du mémoire au profit des crimes et délits traditionnels commis par des individus malveillants au moyen d'un usage de technologies numériques.toutes les catégories d'infractions liées au numérique ont augmenté entre 2016 et 2023, selon la dernière note du service statistique ministériel de la sécurité intérieure (SSMSI) (7).
Les atteintes aux biens, majoritaires, ont augmenté de 8 % en moyenne par an sur la période, et les atteintes aux personnes de 9 %. La note relève l'hétérogénéité de cette criminalité : escroqueries, atteintes morales, atteintes à l'autorité de l'État, fraudes à l'identité. La criminalité numérique s'est diversifiée et s'étend à quasiment l'intégralité du champ des crimes et délits. Parallèlement, les auteurs ont des profils variés, auxquels les forces de sécurité intérieure doivent s'adapter et intégrer les modes opératoires. Leurs motivations sont tout aussi diverses. Délinquant indépendant, groupe structuré et autonome, réseau soutenu par des gouvernements, « hackiviste », tous ont en commun la capacité de suivre et de s'adapter aux évolutions de la société (en 2022, le chiffre d'affaires du commerce en ligne européen était de 899 milliards d'euros) et de l'actualité (hameçonnage lié aux dispositifs gouvernementaux de formation ou de transition énergétique, par exemple). Comprendre les motivations des hackers, en déduire la portée des risques puis investir avec discernement dans la cybersécurité est l'unique ligne de conduite à tenir face à cette menace en pleine expansion.

(7)Analyse InterStats du SSMSI n° 67 – Avril 2024 – voir Annexe 1

Les stratégies de l'Union Européenne face aux menaces criminelles à l'ère du numérique

Auteur : LCL Christel FONTAINE auditrice de la 10ème promotion

Acteur central, le hacker est chargé de la mission cruciale de parvenir à pénétrer les systèmes d'information. Les objectifs multiples de son organisation criminelle incluent l'obtention de rançons, la revente de données à des tiers, voire le détournement direct de fonds. Dans cet univers cybercriminel, la fiche de mission est réduite à infiltrer, corrompre et exploiter.

Le mode opératoire du hacker ressemble à celui d'un cambrioleur expérimenté. En disséquant l'infrastructure, il cherche la faiblesse. Si l'architecture est trop robuste pour une compromission directe, il se tourne alors vers une autre cible : les collaborateurs ou les usagers. Les êtres humains, souvent la partie fragile du système, deviennent alors une porte d'entrée potentielle.
Ensuite, deux types d'attaque coexistent. Dans un premier cas, des bots automatiques explorent les systèmes pour dénicher des failles de sécurité, exploitées ensuite par les hackers. Dans un second cas, les cybercriminels mènent une analyse ciblée sur un compte présentant un potentiel exploitable.
Une fois la brèche trouvée, l'intrusion dans le système d'information de la victime peut commencer.
Quelle que soit la motivation (détournement de fonds, revente d'informations sensibles sur le Dark Web, rançongiciel), le cybercriminel tire très souvent parti de ses efforts, notamment quand il monétise ses méfaits. Il opte alors souvent pour le blanchiment de fonds via le darkweb. Les paiements en cryptomonnaies, en particulier le Bitcoin, sont privilégiés pour leur anonymat, la rapidité et la facilité d'utilisation. Cette méthode rend pratiquement impossible le suivi des transactions pour les autorités, représentant ainsi le moyen de paiement préféré des cybercriminels.
Il est devenu impératif pour les particuliers, les entreprises et les organisations de renforcer leur vigilance et leur cybersécurité. Comprendre les motivations, les méthodes et les objectifs des cybercriminels est essentiel pour contrer cette inquiétante menace aux contours flous mais bien réelle. Dans ce contexte, la Gendarmerie nationale a amorcé un virage « numérique ». Forte de sa gestion décentralisée et de son adaptation aux problématiques liés au territoire (elle est compétente sur 95 % du territoire français), elle a su s'imposer au sein du Ministère de l'Intérieur et des outre-mer comme un acteur central dans la définition de la stratégie nationale. À l'ère du numérique, les gendarmes œuvrent sur un nouveau territoire, insaisissable, dont les contours sont fluctuants mais dont les usages peuvent entraîner des dommages irréversibles. Nouveau terrain d'affrontement, l'espace numérique pousse les praticiens à constamment se renouveler, à affronter une «datasphère », produisant de nouveaux rapports avec des territoires à découvrir au quotidien. Il s'agit même parfois de redécouvrir certains territoires.

Les stratégies de l'Union Européenne face aux menaces criminelles à l'ère du numérique

Auteur : LCL Christel FONTAINE auditrice de la 10ème promotion

En effet, la révolution numérique s'est emparée des villes (les « smart cities 8»), des champs agricoles (grâce aux tracteurs connectés), des routes (et le contrôle des flux par les voitures autonomes), défiant les forces de sécurité intérieure
dans leur façon de se représenter des phénomènes criminels le plus souvent intangibles.
Fortement intégrée aux forces de sécurité intérieure européennes, de par son histoire et sa faculté d'adaptation, comment la Gendarmerie nationale s'approprie-t-elle cette nouvelle délinquance pour protéger les citoyens ? Comment s'insère-t-elle dans une dynamique de nécessaire coopération ?

La sphère des données est ancrée dans le monde physique, humain et politique qui doit être appréhendée de manière globale et interdisciplinaire.

Littéralement, la « ville intelligente » qui, grâce au recueil de différentes données, adapte leurs politiques publiques dans les domaines de la consommation d'eau, d'énergie, de traitement des déchets, etc.
Parallèlement, comment l'Union européenne prend-elle suffisamment en compte ces nouvelles contraintes ? Quels sont ses impératifs ? Saura-t-elle se donner les moyens de ses ambitions ?

Si l'union fait la force, quelle est la force de l'Union, pour paraphraser les propos empruntés au général d'armée (2S) Marc Watin-Augouard (9), précurseur au sein de la Gendarmerie Nationale des questions liées au cyber ? Alors que les États membres transforment continuellement leur organisation nationale pour répondre à ces menaces, comment faire en sorte qu'une seule et même
voix, européenne, porte suffisamment pour lutter contre les cyber délinquants, tout en préservant les droits et libertés des utilisateurs ?

Afin de dresser un constat lucide, il conviendra d'abord de faire un point de situation sur les stratégies de l'UE et leurs déclinaisons, notamment au niveau national, qui se sont développées ces dernières années (1re partie), puis de s'interroger sur les défaillances de la mise en œuvre, tant du point de vue politique que technologiques (2de partie).

(8)DOUZET Frédérick, « Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique », Hérodote, 2020/2-3 (N° 177-178), p. 5.
(9)« L'union fait la force, c'est la force de l'Union », Revue du Trèfle n°166, p.31